CONCEPTRONIC C54BRS4A
802.11g Wireless Broadband Router

User Manual

About This Manual

This manual provides descriptions of the Conceptronic C54BRS4A 802.11g Wireless Broadband Router, its hardware and software features, and how to set up and use the device on your small office or home network.

Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Wireless Broadband Router. Have all the necessary information and equipment on hand before beginning the installation. A packing list is included at the end of this section.

Installation Overview

The procedure to install the Wireless Broadband Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Check the contents of the package to be certain that everything listed on the packing list is included. A packing list is included at the end of this section. The information you will need includes the account name or number and the password used to gain access to your service provider's network, and ultimately to the Internet.
2. Install the hardware, that is, connect the Ethernet cables to the device to establish the necessary network links to your computer and connect the power adapter to power on the Wireless Broadband Router.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Wireless Broadband Router. Without the correct IP settings your computer will not be able to communicate with the device or access the software used to configure the Wireless Broadband Router. Without compatible IP settings on your computer, you will not be able to use a web browser to access the Internet.
4. Use the web-based management software to configure the device. Many users can install the Wireless Broadband Router with the Setup Wizard. Some users may not need to change any of the device settings that establish and maintain the network connection. Follow the instructions of your service provider to find out what is required for your account.

Requirements for Installation

To install and use the Wireless Broadband Router you need a computer equipped with an Ethernet port (such as an Ethernet NIC) and a web browser.

WLAN Ethernet Adapter

Any computer that uses the Wireless Broadband Router must be able to connect to it through the Wireless Ethernet (WLAN) on the Wireless Broadband Router. This connection is a Wireless Ethernet (WLAN or WiFi) connection and therefore requires that your computer be equipped with a Wireless Ethernet Adapter as well. Many notebook computers are now sold with a Wireless Ethernet Adapter already installed. There is also a Wired Ethernet port that is used to connect the WLAN adapter to your wired network. This port can be used to configure the Wireless Broadband Router. Most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can configure the Wireless Broadband Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Operating System

The Wireless Broadband Router uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software.

Web Browser

Any common web browser can be used to configure the Wireless Broadband Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

- **1x** Conceptronic C54BRS4A - 802.11g Wireless Broadband Router
- **1x** Antenna for C54BRS4A
- **1x** CD-ROM containing this User's Guide
- **1x** Straight-through Ethernet cable
- **1x** Power Adapter, 5V, 2A DC
- **1x** Quick Installation Guide
- **1x** Warranty Card

Wireless LAN

A Wireless LAN is a cellular computer network that transmits data using radio signals instead of cables. Wireless LAN technology is commonly used for home, small office and large corporate networks. Wireless LAN devices have a high degree of mobility and flexibility that allow network to be quickly set up or dismantled and allow them to roam freely throughout the network.

The IEEE 802.11g Wireless LAN standard is an improvement on the IEEE 802.11b standard. The 802.11g embedded Wireless LAN access point is fully compatible with legacy IEEE 802.11b devices.

Some basic understanding of wireless technology and terminology is useful when you are setting up the Wireless Broadband Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

For home users who will not incorporate a RADIUS server in their network, the security for the Conceptronic C54BRS4A, used in conjunction with other WPA-compatible 802.11 products, will still be much stronger than ever before. Utilizing the **Pre-Shared Key mode** of WPA, the Wireless Broadband Router will obtain a new security key every time it connects to the 802.11 network. You only need to input your encryption information once in the configuration menu. No longer will you have to manually input a new WEP key frequently to ensure security. With the Wireless Broadband Router, you will automatically receive a new key every time you connect, vastly increasing the safety of your communication.

The Wireless Broadband Router is an ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, trade shows and special events. The 802.11g standard is backwards compatible with 802.11b devices.

The Wireless Broadband Router has the newest, strongest, most advanced security features available today. When used with other 802.11g WPA (WiFi Protected Access) compatible products in a network with a RADIUS server, the security features include:

WPA: WiFi Protected Access, which authorizes and identifies users, based on a secret key that change automatically at regular intervals. **WPA** uses **TKIP** (**Temporal Key Integrity Protocol**) to change the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. (By contrast, the previous WEP encryption implementation required the keys to be changed manually.)

Radio Transmission

Wireless LAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the Wireless LAN nodes in its broadcast range. Wireless LAN nodes transmit digital data using FM (frequency modulation) radio signals. Wireless LAN devices generate a carrier wave and modulate this signal using various techniques. In this way, digital data can then be superimposed onto the carrier signal. This radio signal carries data to Wireless LAN devices within range of the transmitting device. The antennae of Wireless LAN devices listen for and receive the signal.

Range

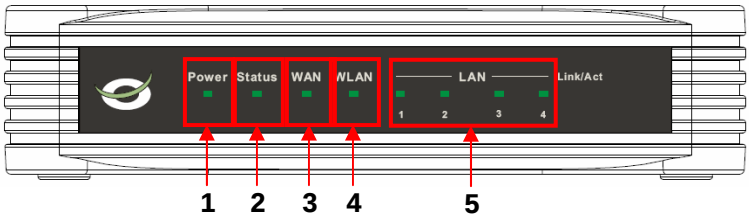
Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the device in a location between the Wireless LAN devices maintaining a roughly equal straight-line distance to all devices that need to access the Wireless Broadband Router through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength.

SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several Wireless Broadband Routers or access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network.
The Wireless Broadband Router operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. The Conceptronic C54BRS4A broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate.

Front Panel LED Display

Place the Router in a location where the LED indicators on the front panel can be viewed.
The LED indicators on the front panel include the Power, Status, WAN, and WLAN indicators. Each Ethernet LAN port displays an indicator for monitoring link status and activity (Link/Act).



Nr	Description	Status	Status Explanation
1	Power LED	**OFF**	The device is turned off
		ON	The device is turned on
2	Status LED	**OFF**	The device is turned off / System Failure*
		BLINK	The device is turned on and ready for use
3	WAN LED	**OFF**	No WAN Connection is created
		ON - STEADY	A WAN Connection is created
		ON - BLINK	Data is send or received through the WAN Port
4	WLAN LED	**OFF**	Wireless interface is disabled
		BLINK	Wireless interface enabled and active
5	LAN LED's (1, 2, 3, 4)	**OFF**	No Network Link is created to the LAN Port
		ON - STEADY	A Network Link is created on the LAN Port
		ON - BLINK	Data is send or received through the LAN Port

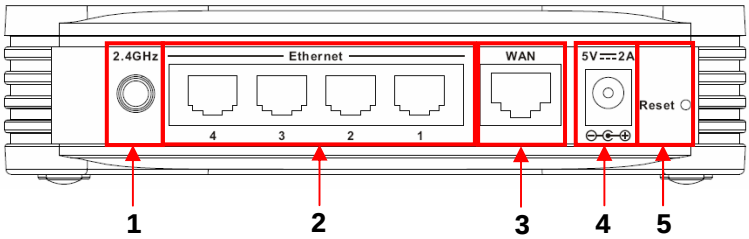
* In normal use, the Status LED will turn on and blink within 45 seconds after the device is turned on or restarted. When a system failure happens with the device, the Status LED will not turn on.
You can use the following options to solve the system failure:

a. Power down the device, wait 10 seconds and reconnect the power to the device.
b. Reset the device to factory defaults by pressing the reset button on the back of the device for +/- 15 seconds.

If the Status LED does not turn on after you tried above options, please contact Conceptronic Support at: support@conceptronic.net

Rear Panel Cable Connections

Connect the power adapter cord and network cables on the rear panel. The power switch and reset button are also located on the back of the device. Connect the antenna to the antenna post.



Nr	Description	Explanation
1	Antenna Connection	Reverse-SMA Connector for Wireless Antenna
2	LAN Ports	Connect your Computer(s) to the router
3	WAN Port	Connect your Broadband connection to the router
4	Power Connection	Connect the Power Supply to the router
5	Reset Button	Reset the router to the Factory Default Settings

Hardware Installation

Place the Wireless Broadband Router in a location where it can be easily connected to the wired interface (Ethernet link to a broadband modem, for example) as well as function effectively as a Wireless LAN access point. Make sure the Wireless Broadband Router is near a suitable power source.
Connect the bundled power supply to the power connection on the back of the C54BRS4A and to a free wall power outlet. The Power LED of the C54BRS4A will turn on.

Wireless LAN Performance and Environment

Many environmental factors can affect the effective wireless function of the Wireless Broadband Router. If this is your first time setting up a wireless network device, read and consider the points listed below.

The Wireless Broadband Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

The Wireless Broadband Router lets you access your network within range of the device. However, walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. For maximum range and signal strength, use these basic guidelines:

1. **Keep the number of walls and ceilings to a minimum:**

   The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.

2. **Consider the direct line between access points and workstations:**

   A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.

3. **Building Materials make a difference:**

   Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls may have little or no structural steel.

4. **Keep the Wireless Broadband Router away (at least 1-2 meters) from electrical devices:**

   Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

5. **Position antenna for best reception:**

   Adjust the antenna position to see if the signal strength improves. Some adapters or access points allow the user to judge the strength of the signal. Use this method, if available, to test signal strength.

WAN Connection

Use a LAN Cable to connect the C54BRS4A to your Broadband Gateway (Cable Modem, DSL Modem, Fiber Gateway, etc.)

The WAN LED on the front side of the C54BRS4A will turn on.

Note: If the WAN LED on the front side does not turn on, make sure that:
- The C54BRS4A is powered (the Power LED should burn).
- The Broadband Gateway is turned on.
- The LAN cable between both devices is connected correctly.

LAN / Wireless LAN Connection

For LAN Cable Users:
Connect the LAN Cable to 1 of the 4 LAN ports on the back panel of the C54BRS4A and to the Network Card in your computer.
The LAN LED of the used LAN port will turn on, indicating that the computer is connected. (Your LAN Connection must be enabled and your computer turned ON).

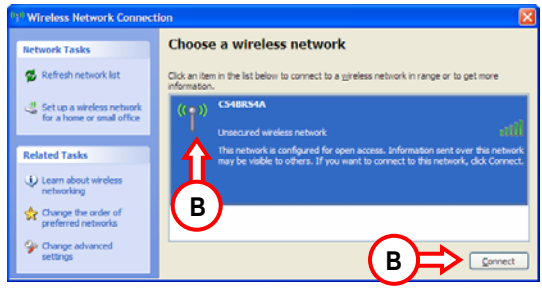
For Wireless Users:

Almost every brand/type Wireless Card uses a different Client application. Please check the manual of your Wireless Card for information how to create a connection with a Wireless Network.

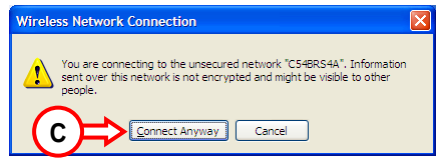
The example below is using the standard Microsoft Wireless Client, which is integrated in Windows XP with Service Pack 2.

A. Right click the Wireless Network Icon in your System tray and select "**View Available Wireless Networks**".

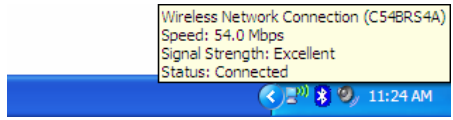
B. Select the Network "**C54BRS4A**" from the list of available wireless networks and click "**Connect**".



C. You will receive a warning about connecting to an unsecured wireless network. Click "**Connect Anyway**" to proceed with the connection.



D. When the connection is build you will see the active wireless icon in the system tray. If you move your mouse over the icon you will receive the following information (regarding on the signal strength):



Computer Configuration

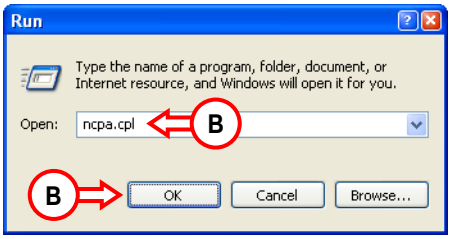
Configure your IP address

The C54BRS4A is equipped with a build-in DHCP Server. The DHCP Server will automatically assign an IP address to a connected computer if the connected computer is set to "**obtain an IP address automatically**".

To configure your computer for Automatic IP follow the instructions below:

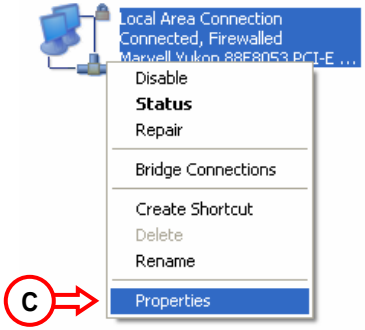
A. Click "**Start**" → "**Run**".

B. Enter the command "**NCPA.CPL**" and press "**OK**".



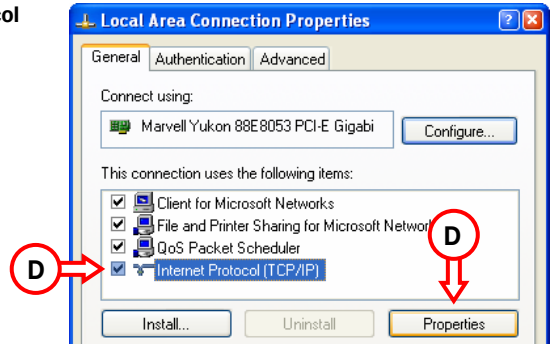
The Network Connections window will appear.

C. Right click your "**Local Area Connection**" (Wired or Wireless, depending on the connection you use) and select "**Properties**".



The Properties window of your Local Area Connection will appear.

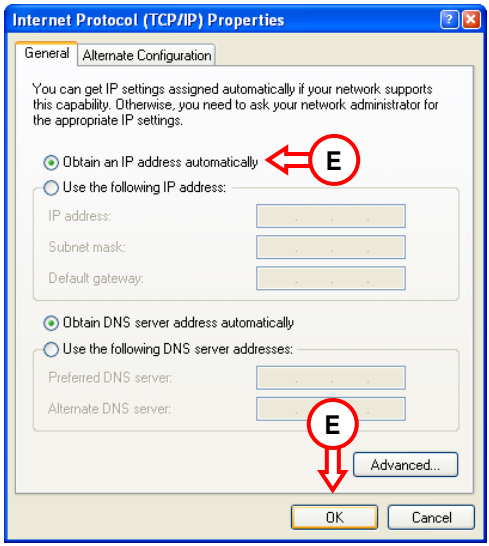
D. Select the "**Internet Protocol (TCP/IP)**" and click "**Properties**".



The Properties window of the Internet Protocol (TCP/IP) will appear.

E. Set the properties to "**Obtain an IP address automatically**" and press "**OK**" to save the settings.

F. Press "**OK**" in the properties window of the Local Area Connection to save the settings.



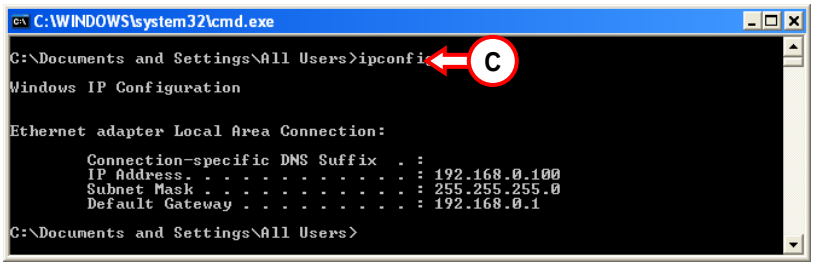
Checking your connection with the C54BRS4A

With the Command prompt of Windows you can verify if you have received a correct IP address on your Local Area Connection:

A. Click "**Start**" → "**Run**".
B. Enter the command "**CMD**" and press "**OK**".

The Command Prompt will appear.

C. Enter the command "**IPCONFIG**" and press **ENTER**.



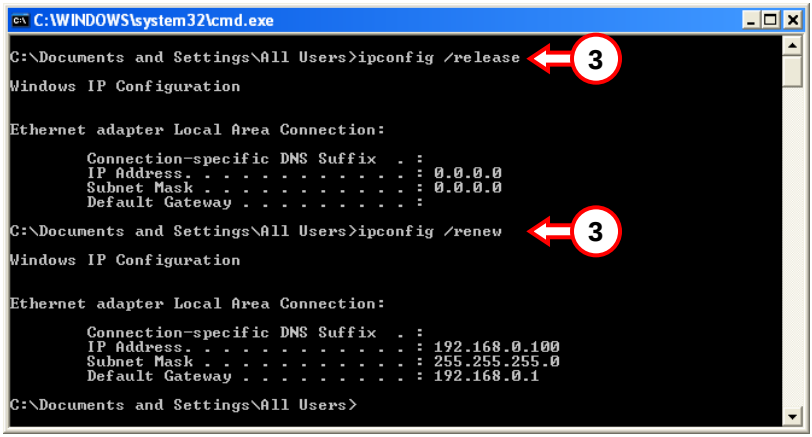
You should see the following information
IP Address **: 192.168.0.xxx** (Where **xxx** can vary between **100 ~ 199**).

Subnet Mask **: 255.255.255.0**
Default Gateway **: 192.168.0.1**

If the information shown above matches your configuration you can continue the configuration of the device in Chapter 5.

If the shown information above does not match your configuration (i.e. your IP address is 169.254.xxx.xxx) please check the options below:

1. Power OFF and Power ON the device.
2. Reconnect the LAN Cable to the device and to your computer.
3. Renew the IP address of your computer with the following commands:
   - "**IPCONFIG /RELEASE**" to release the wrong IP address.
   - "**IPCONFIG /RENEW**" to receive a new IP address from the device.



If above steps do not solve the IP address problem, you can reset the device to the factory default settings with the Reset Button on the back of the device.

Press and hold the Reset Button for +/- 15 seconds to load the Factory Default Settings. When the Status LED is active again, repeat step **C** to renew your IP address.

Configuring Router Settings

This chapter describes how to configure the Wireless Broadband Router the first time you use it or if you are configuring it after resetting the device to the factory default settings. The following sections describe how to configure the router through the Web based configuration.

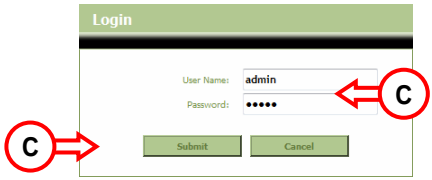
The configuration of your C54BRS4A is web based. You will need a web browser for the configuration of the device.

Note: For configuration of the router it is advised to use a LAN Cable connection to the device instead of a Wireless connection.

A. Start your web browser (like: Internet Explorer, FireFox or Safari).

B. Enter the IP address of the device in the address bar of your web browser (By default: **http://192.168.0.1/).**

The Login page of the C54BRS4A will be shown.

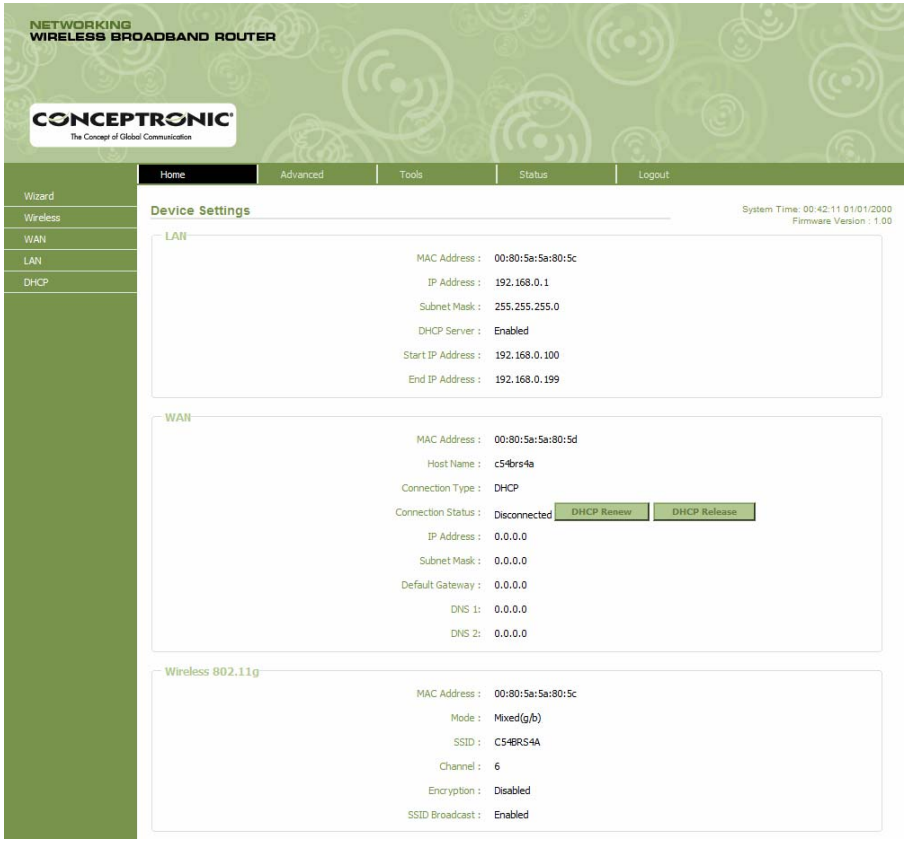


C. Enter the Username and Password (Default: '**admin**' & '**admin**') and click "**Submit**" to enter the configuration pages.

When the Username and Password are correct the router will display the "**Device Settings**" overview.

The "**Device Settings**" overview shows all configured settings for the LAN, WAN and Wireless part of the router.

The "**Home**" menu of the configuration contains the following configuration options: **Wizard**, **Wireless**, **WAN**, **LAN** and **DHCP.**

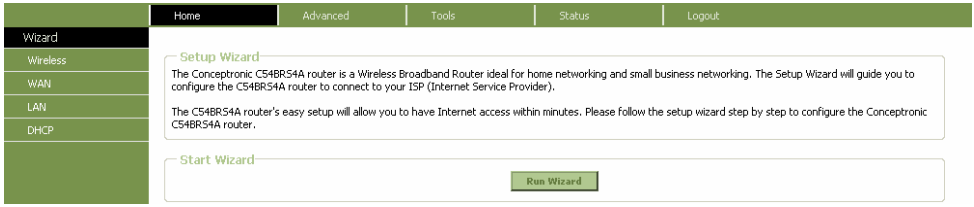


Device Settings Overview

HOME - WIZARD

You can setup the C54BRS4A through the build-in Wizard. This Wizard will help you configuring the basic settings of the C54BRS4A step by step.

To use the Setup Wizard, click the **Run Wizard** button.



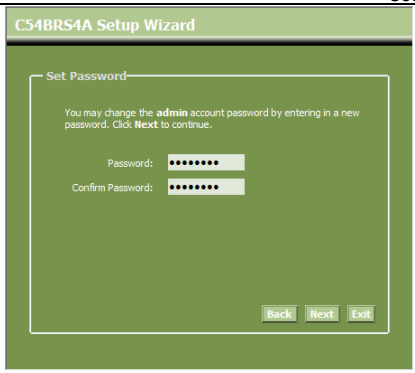
Setup Wizard window

Note: Before you begin with the Wizard Configuration, make sure you have all information for your internet settings available. (For example: Account information, connection type, etc.)

A. The welcome screen lists five steps of the wizard. Click **"Next"** to continue.

B. You are recommended to set an admin password here. Enter the new password and re-enter it for confirmation.

When completed, click "**Next**".



C. For system management purpose, a correct time setting is critical to have accurate time stamps on the system logs.

Set an appropriate Time Zone in this step.

When completed, click "**Next**".

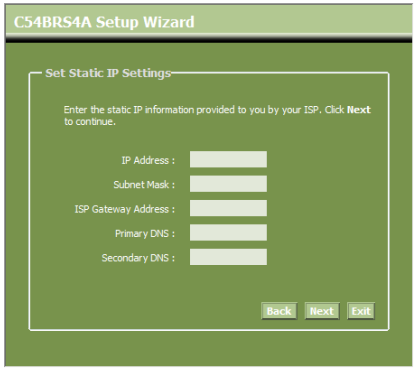
D. Select the Internet Connection method which corresponds with your provider settings.

If you don't know which option you need for your internet connection, please check the documentation of your provider or contact your provider helpdesk.

When completed, click "**Next**".

E. When your provider requires a Static IP connection, select the "**Static IP**" option.

Connection - Static IP



Enter the requested information:

- *IP Address*
- *Subnet Mask*
- *ISP Gateway Address*
- *Primary DNS*
- *Secondary DNS (Optional)*

When completed, click "**Next**".

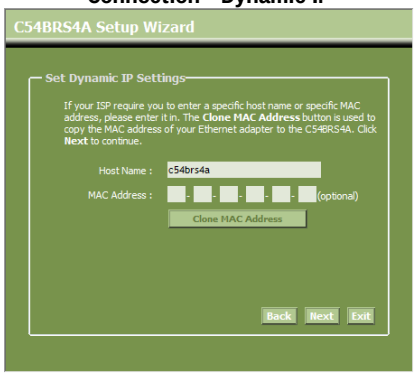
F. When your provider requires a Dynamic IP connection, select the "**Dynamic IP**" option.

Some providers require a specific Hostname for their connections. If your provider requires a specific Hostname, enter the Host Name in the field.

Some providers only allow 1 specific MAC address to connect to the internet. If your PC Network Card works with the specific required MAC address, press the "**Clone MAC Address**" button or enter the MAC Address manually.

When completed, click "**Next**".

Connection – Dynamic IP



G. When your provider requires a PPPoE connection, select the "**PPPoE**" option.

Connection - PPPoE

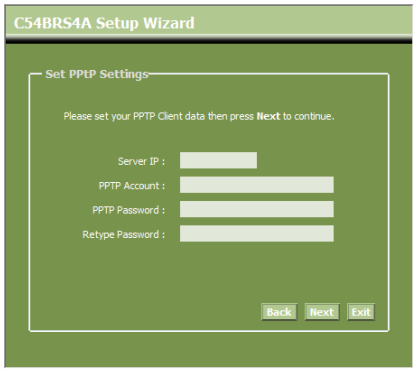
Enter the requested information:

- *User Name*
- *Password*
- *Retype Password*

When completed, click "**Next**".

H. When your provider requires a PPTP connection, select the "**PPTP**" option.

Connection - PPTP



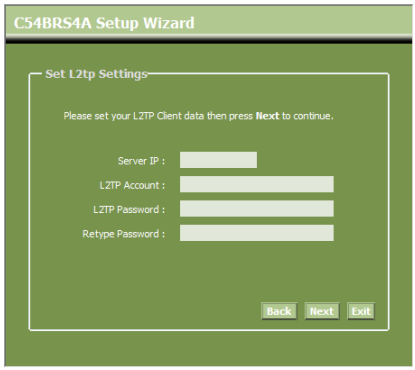
Enter the requested information:

- *Server IP*
- *PPTP Account*
- *PPTP Password*
- *Retype Password*

When completed, click "**Next**".

I. When your provider requires a L2TP connection, select the "**L2TP**" option.

Connection - L2TP



Enter the requested information:

- *Server IP*
- *L2TP Account*
- *L2TP Password*
- *Retype Password*

When completed, click "**Next**".

When the WAN configuration is complete, the Wizard will continue with the Wireless configuration:

J. You can change the SSID of the router. The SSID is the name which will be broadcasted through the Wireless part.

You can change the channel between channel **1** and **13**. If you experience slow connections or break-downs, there can be another accesspoint in your area which can interfere with your wireless channel. In that case, you can try another channel.

When completed, click "**Next**".

You can secure your Wireless Connection with encryption. By default, the Wireless Connection is not secured. To prevent unauthorized access to your network, set a security level through the Setup Wizard.

Note: All options are explained, but it is advised to secure your network with "**WPA-PSK/WPA2-PSK**" security. This is the highest WPA2 security level, with backwards compatibility to WPA only clients.

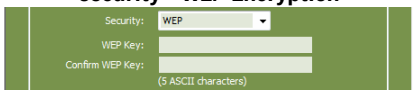
Note: Remember or write down the entered wireless security information. You will need it when you want to configure a Wireless Client to connect to the C54BRS4A!

K. Select a security level for your Wireless Network.

When a security level is chosen, the Wizard will show fields for the required information.

L. If you want to secure your network with WEP encryption, select "**WEP**" from the drop-down list. Enter the WEP key in ASCII format (input: A-Z, 0-9).

Security - WEP Encryption



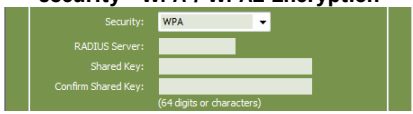
Note:

Through the Wizard you can only configure WEP 64Bits.

M. If you want so secure your network with WPA or WPA2 (with Radius Server), select "**WPA**" or "**WPA2**" from the drop-down list.

Enter the IP Address of the Radius Server, the Shared Key and confirm the Shared Key in the second field.

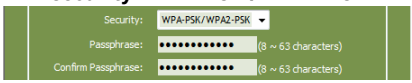
Security - WPA / WPA2 Encryption



N. If you want to secure your network with WPA-PSK or WPA2-PSK, select "**WPA-PSK**", "**WPA2-PSK**" or "**WPA-PSK/WPA2-PSK**" from the drop-down list.

Enter the Passphrase for your encryption and confirm the Passphrase in the second field.

Security - WPA-PSK / WPA2-PSK



O. When all Wireless settings are made, click "**Next**" to continue.

P. The Setup Wizard is now complete. If you want to apply your settings, click "**Save & Take Effect**".

If you want to change any setting, click "**Back**" to return to the previous screen.

If you want to close the Setup Wizard without any changes, click "**Exit**".

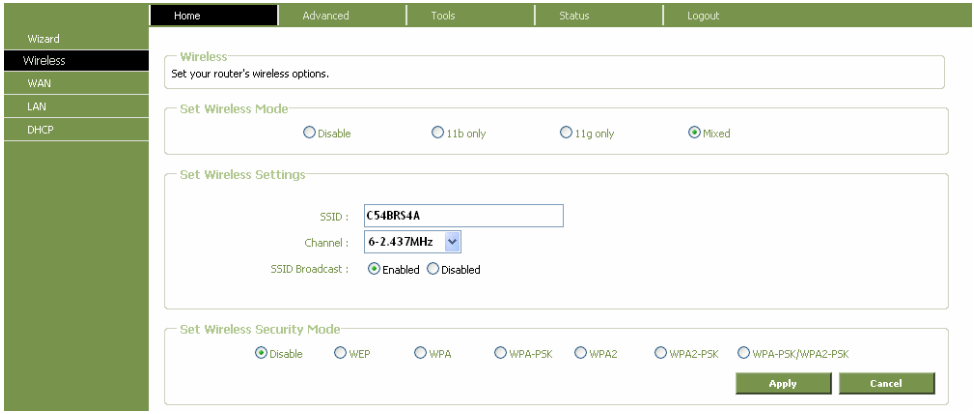
When you select "**Save & Take Effect**", the router will apply the configured settings. Please wait for the message "**Save Complete**".

Q. The configuration is now complete. Click "**Close**" to exit the Setup Wizard.

You will return to the "**Device Settings**" overview which will show you the configured settings for your WAN and Wireless connection.

HOME - WIRELESS

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the windows used to configure Wireless, WAN, LAN, and DHCP settings directly from the **Setup** directory. To access the **Wireless Settings** window, click on the **Wireless** link button on the left side of the first window that appears when you successfully access the web manager.



Wireless Settings window

Click the **Set Wireless Radio** radio-button to allow the router to operate in the wireless environment.

The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all other devices on the wireless network must use the same SSID.

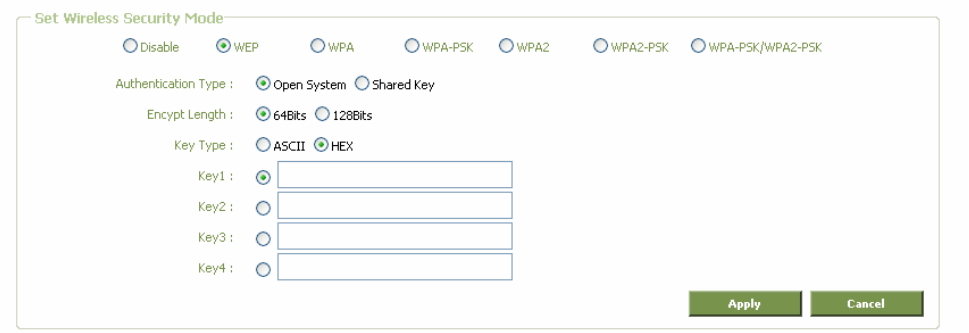
Enable **SSID Broadcast** if you want users to be able to join your wireless network based on the SSID information broadcast by the Router. If this is disabled, each new user will have to be manually configured.

What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop-down menu to select the **Channel** used for your 802.11g wireless LAN. Click **Apply**.

WEP Encryption

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. The router offers 64- or 128-bit encryption with four keys available.

To bring up the **Wireless Settings** window for WEP, select **WEP** from the **Set Wireless Security Mode** radio-buttons.



Wireless Settings window for WEP

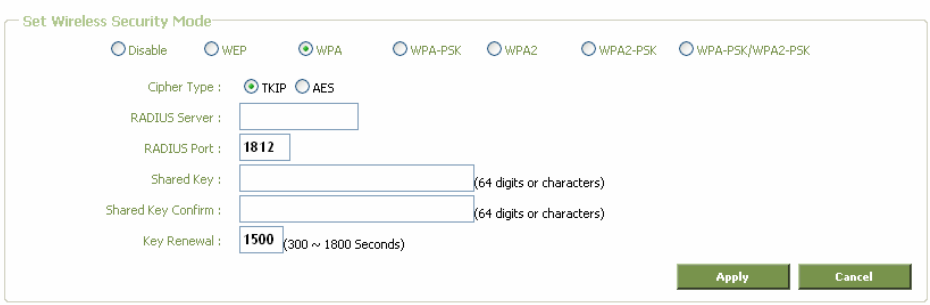
1. Select an **Authentication** type, Open System or Shared Key.
2. Select the desired level of **WEP Encryption**, *64Bit* or *128Bit*.
3. Select the desired key input format, *HEX* (*hexadecimal*) or *ASCII*.
4. Select a key by clicking a radio button on the left and then enter the proper-length key.
5. Click **Apply**.

Note: If encryption of any kind, at any level is applied to the Wireless network, all devices on the network must comply with all security measures.

WPA Encryption

WiFi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP. There are two versions, WPA and WPA2; both are supported by the Access Point. WPA includes the option of using a Pre-Shared Key similar to WEP, or a RADIUS server can be used for verification. In addition, WPA2-Auto is offered for user convenience.

WPA/WPA2 Encryption with Radius Server

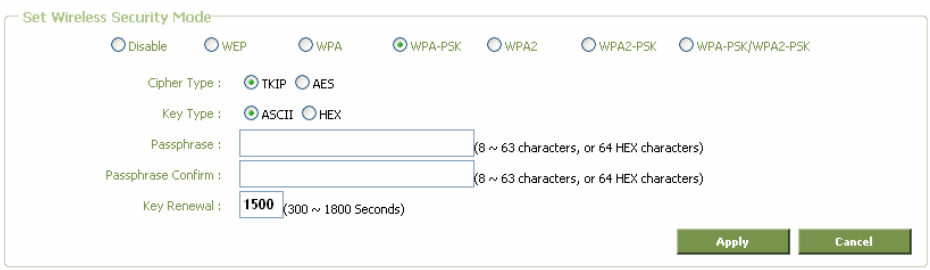


Wireless Settings window for WPA and WPA2

1. Select the type of WPA encryption for your Radius Server, **WPA** or **WPA2**.
2. Select the desired **Cipher Type**, TKIP, AES, or TKIP/AES.
3. Enter the **RADIUS Server** IP Address and the **RADIUS Port** for your Radius Server.
4. Enter the **Shared Key** (between 1 and 63 characters) which is needed for the Radius server.
5. Re-enter the Shared Key in the second field.
6. Click **Apply.**

Note: The values needed for RADIUS authentication can be obtained from your Internet Service Provider (ISP).

WPA/WPA2-PSK With Passphrase Encryption



Wireless Settings window for WPA-PSK, WPA2-PSK and WPA-PSK/WPA2-PSK

1. Select the type of WPA encryption for use with your Passphrase, **WPA-PSK**, **WPA2-PSK** or **WPA-PSK/WPA2-PSK**.

Note: If you select **WPA-PSK/WPA2-PSK**, the router will work with the highest WPA2-PSK encryption. If clients try to connect which do not support WPA2-PSK, the router will automatically authorize the client on WPA-PSK Level.

2. Select the desired **Cipher Type**, TKIP or AES.
3. Select the **Key Type**, ASCII or HEX (Hexadecimal).
4. Enter the **Passphrase** you want to use for your WPA-PSK encryption (8 ~ 63 characters ASCII, or 64 characters HEX).
5. Re-enter the Passphrase in the second field.
6. Click **Apply.**

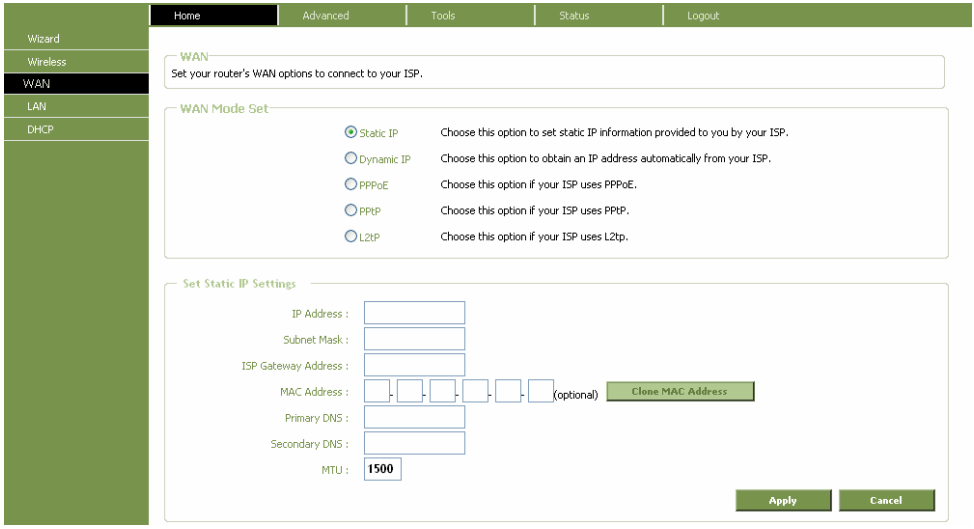
HOME - WAN

To access this window click on the **WAN** button in the left menu of the web manager.

Static IP Address

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection. Follow the instruction below to configure the Router to use Static IP Address assignment for the WAN connection.

To configure a Static IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this window.



WAN Settings window for Static IP Address

To configure a Static IP type connection for the WAN, follow these steps:

1. Click the **Static IP** radio button at the top of the window.
2. Enter an **IP Address**, **Subnet Mask**, **ISP Gateway Address**, **Primary DNS Address**, and (if available) **Secondary DNS Address** as instructed by your ISP. These are the global IP settings for the WAN interface. This is the "visible" IP address of your account. Your ISP should have provided these IP settings to you.
3. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, press the "**Clone MAC Address**" button or enter the MAC Address manually.
4. Leave the **MTU** value at the default setting (default = *1500*) unless you have specific reasons to change this (see table below).
5. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
6. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** button in the top menu and select the **System** button in the left menu. In the **System Management** window, click the **Save** button under Save Settings to Local Hard Drive and then click the **Reboot** button to reboot the C54BRS4A.
7. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

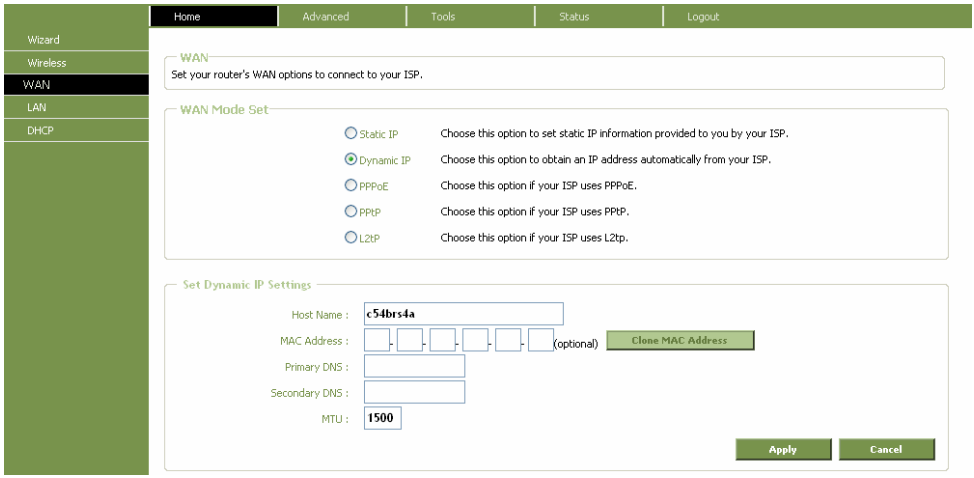
Additional settings for Static IP Address connections:

Static IP Parameters	Description
IP Address	This is the permanent global IP address for your account. This is the address that is visible outside your private network. Get this from your ISP.
Subnet Mask	This is the Subnet mask for the WAN interface. Get this from your ISP.
ISP Gateway Address	This is the IP address of your ISP's Gateway router. It provides the connection to the Router for IP routed traffic that is outside your ISP's network. That is, this will be the primary connection from the Router to most of the Internet. Get this IP address from your ISP.
MAC Address	To use the Clone MAC Address feature, enter a MAC address in this field and then click the **Clone MAC Address** button.

Primary DNS Address	This is the IP address of the first choice for Domain Name Service (DNS) used to match the named URL web address used by most browsers with the actual global IP address used for a web server. Usually this will be a server owned by the ISP. Get this IP address from your ISP.
Secondary DNS Address	This is the second choice for a DNS server. Get this IP address from your ISP.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1500* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.

Dynamic IP Address

A Dynamic IP Address connection configures the Router to automatically obtain its global IP address from a DHCP server on the ISP's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address.
To configure a Dynamic IP Address connection, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose. See the table below for a description of all the settings available in this window.



WAN Settings window for Dynamic IP Address

To configure a Dynamic IP Address connection for the WAN, follow these steps:

1. Click the **Dynamic IP** radio button at the top of the window.
2. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer's Ethernet adapter, press the "**Clone MAC Address**" button or enter the MAC Address manually.
3. Fill in the **Primary DNS Address**. This information should be available from your ISP.
4. Fill in the **Secondary DNS Address** (if available from your ISP).

5. Leave the **MTU** value at the default setting (default = *1500*) unless you have specific reasons to change this (see table below).
6. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
7. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** button in the top menu and select the **System** button in the left menu. In the **System Management** window, click the **Save** button under Save Settings to Local Hard Drive and then click the **Reboot** button to reboot the C54BRS4A.
8. The Router will save the new settings and restart. Upon restarting, the Router will automatically establish the WAN connection.

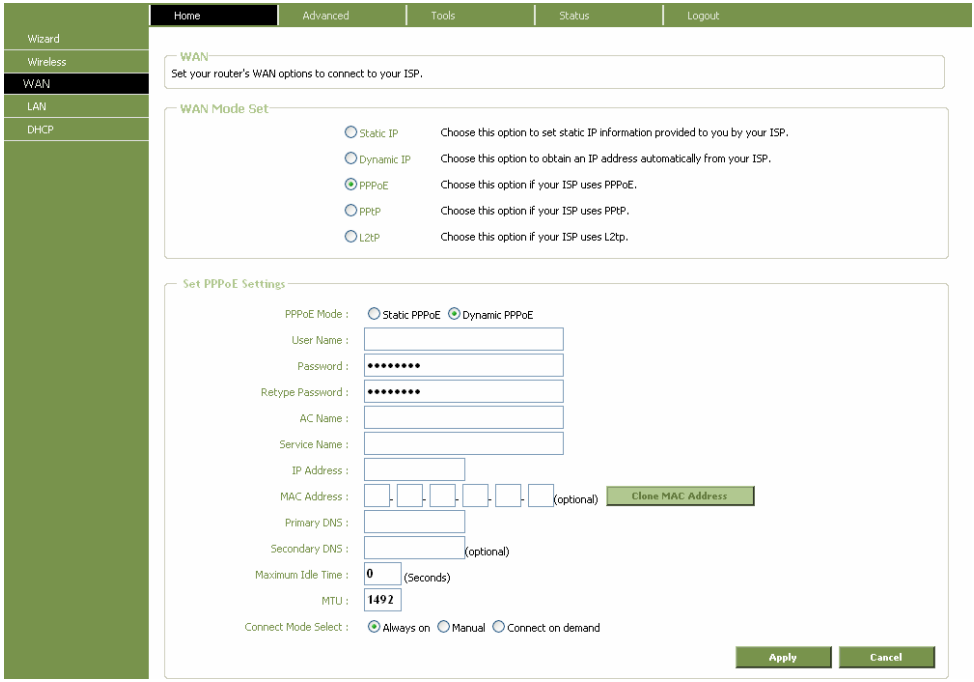
Additional settings for Dynamic IP Address connections:

Dynamic IP Parameters	Description
Host Name	This is not always necessary, but may be required for some ISPs. Type in the MAC address of your computer's Ethernet adapter in the **MAC Address** field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP's server used for DHCP. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. If you want to later replace the cloned MAC address with the factory default setting, type in all zeros – 0:0:0:0:0:0 – and click the **Clone MAC Address** button.
MAC Address	This is not always necessary, but may be required for some ISPs. Type in the MAC address of your computer's Ethernet adapter in the Cloned MAC Address field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP's server used for DHCP. Some ISPs record the unique MAC address of your computer's Ethernet adapter when you first access their network. If you want to later replace the cloned MAC address with the factory default setting, type in all zeros – 0:0:0:0:0:0 – and click the **Clone MAC Address** button.
Clone MAC Address	To clone the MAC address of your computer's Ethernet adapter, type in the MAC address in the **MAC Address** field and then click this **Clone MAC Address** button.
Primary DNS Address	Enter the Primary DNS Address. This information should be provided to you by your Internet Service Provider.

Secondary DNS Address	The Secondary DNS Address is optional. See your Internet Service Provider for further information.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1500 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.

PPPoE

Follow the instructions below to configure the Router to use a PPPoE for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.



WAN Settings window for PPPoE

To set up a PPPoE connection:

1. If not already selected, click the **PPPoE** radio button at the top of the window.
2. Under the **PPPoE Settings** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user1234@isp.co.uk. The Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.
3. Leave the **MTU** value at the default setting (default = *1492*) unless you have specific reasons to change this (see table below).
4. Typically the globally IP settings (i.e. IP address for the WAN interface) for a PPPoE connection will use Dynamic IP assignment from the ISP. Some accounts may be assigned a specific global IP address.
5. Choose the desired **Connect mode select** setting. Select from: Always on, Manual, or Connect on demand. Most users will want to choose the default connection setting, Always on.
6. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
7. The new settings must be saved and the Router must be restarted for the settings to go into effect. To save and reboot the Router, click on the **Tools** directory tab and then click the **System** button. In the **System Settings** window, click the **Save** button under Save Settings to Local Hard Drive and then click the Reboot button under Reboot the CONCEPTRONIC C54BRS4A.
8. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

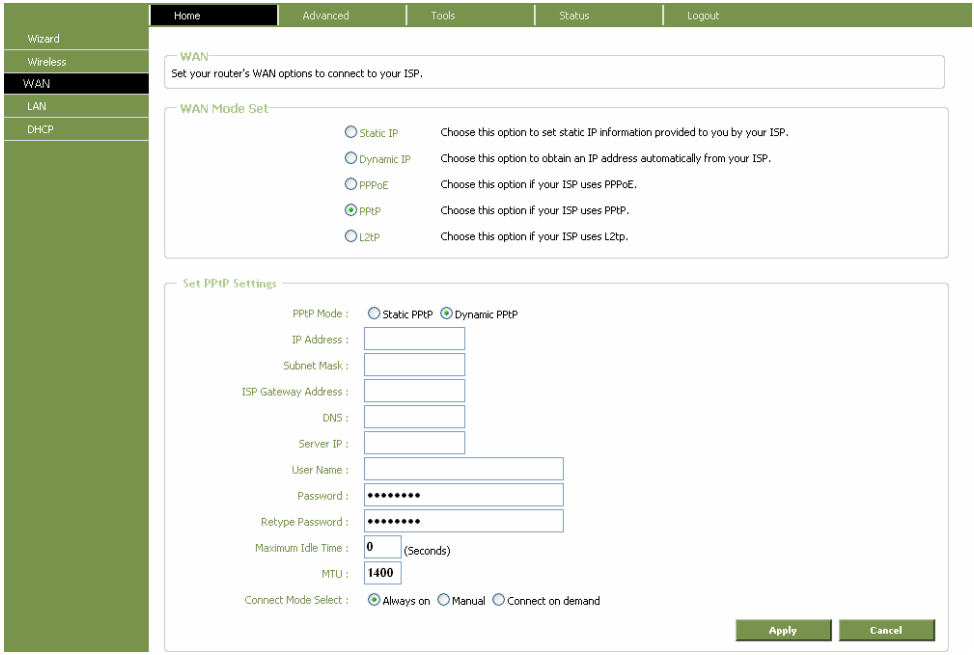
Additional settings for PPPoE/PPPoA connections:

PPPoE/PPPoA Parameters	Description
User Name	For PPP connections, a **User Name** and **Password** are used to identify and verify your account to the ISP. Enter the User Name for your ADSL service account. User names and passwords are case-sensitive, so enter this information exactly as given to you by your ISP.
Password	Together with the **User Name**, this is used to verify your account to the ISP. Enter the Password exactly as given to you by your ISP.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1492* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.

IP Address	If you have selected the *Static PPPoE* option, type in the global IP address used for your WAN interface. Your ISP should provide this IP address to you.
MAC Address	To use the Clone MAC Address feature, enter a MAC address in this field and then click the **Clone MAC Address** button.
Primary DNS	Enter the Primary DNS Address. This information should be provided to you by your Internet Service Provider.
Maximum Idle Time	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in minutes). This will disconnect the Router after the WAN connection has been idle for the amount of time specified.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1500* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
Connect mode select	Select the desired option: *Always on*, *Manual*, or *Connect on demand*. Most users will want to choose the default connection setting, Always on.

PPTP

The **P**oint to **P**oint **T**unneling **P**rotocol is used to transfer information securely between VPNs (Virtual Private Routers). Encryption methods are employed in the transfer of information between you and your ISP using a key encryption. This option is specific for European users whose ISPs support the PPTP protocol for the uplink connection. To connect to your ISP's server using this protocol, the information in this window must be provided to you by your ISP and then properly implemented.

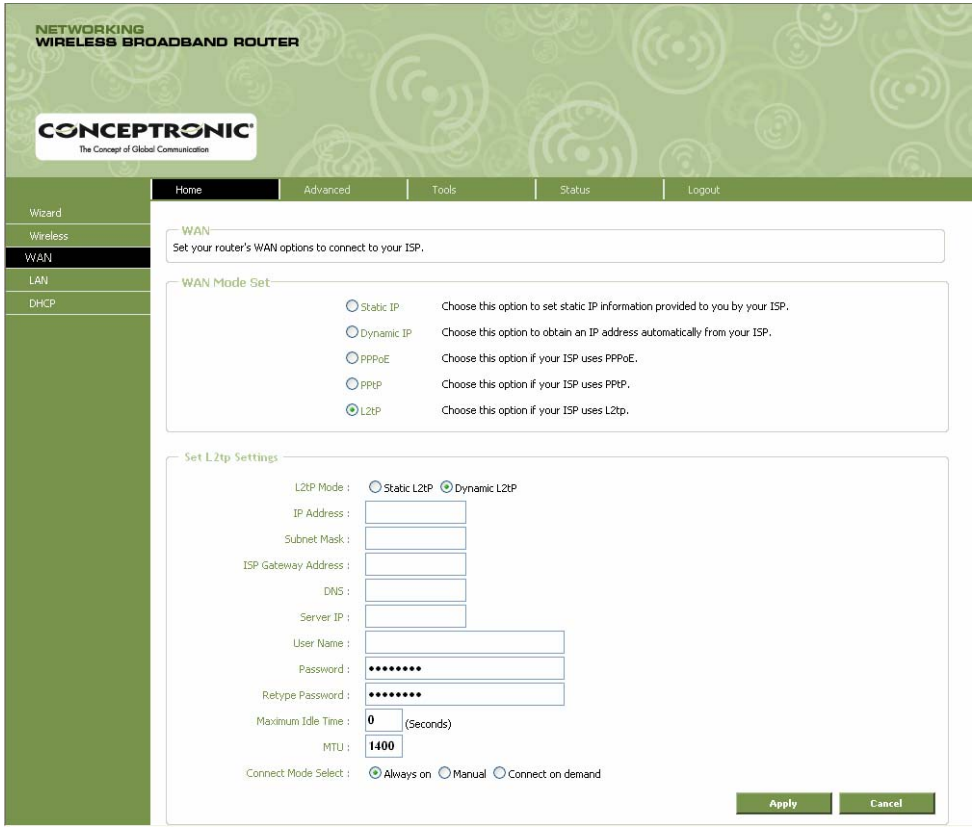


WAN Settings window for Others (PPTP)

PPTP Parameters	Description
IP Address	Enter the IP address for your Router based on the information provided to you by your ISP.
Subnet Mask	Enter the Subnet Mask for your Router based on the information provided to you by your ISP.
ISP Gateway Address	Enter the Gateway IP address based on the information provided to you by your ISP.
DNS	Enter the Domain Name Server IP address.
Server IP	Enter the IP address of the ISP server with which your router will be conveying encrypted information. This field is based on information provided to you by your ISP.
Username	Enter the name of the PPTP account as provided to you by your ISP.
Password	Enter the PPTP password as provided to you by your ISP.
Retype Password	Retype the password entered in the Password field.
Maximum Idle Time	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in minutes). This will disconnect the Router after the WAN connection has been idle for the amount of time specified.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (*1400* bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
Connect mode select	Select the desired option: Always on, Manual, or Connect on demand. Most users will want to choose the default connection setting, Always on.

L2TP

Some ISPs may require the user to uplink using the **L**ayer **2** **P**rotocol **T**unneling (L2TP) method. L2TP is a VPN protocol that will ensure a direct connection to the server using an authentication process that guarantees the data originated from the claimed sender and was not damaged or altered in transit. Once connected to the VPN tunnel, it seems to the user that the client computer is directly connected to the internal network. To set up your L2TP connection, enter the following data that was provided to you by your ISP.

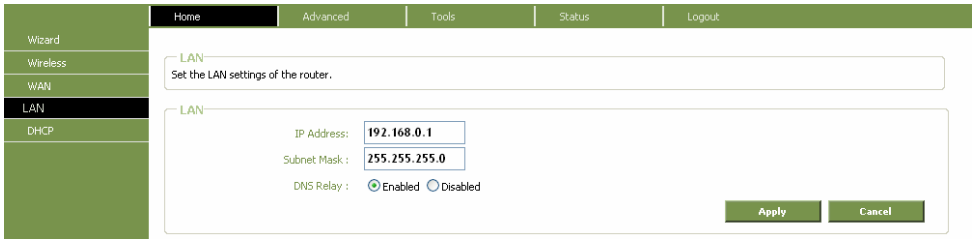


WAN Settings window for Others (L2TP)

L2TP Parameters	Description
IP Address	The IP address that will be assigned to your router for this connection, as stated by your ISP.
Subnet Mask	The IP address of the corresponding Subnet Mask, as stated to you by your ISP.
ISP Gateway Address	The IP address of the gateway device, as stated to you by your ISP.
DNS	Enter the Domain Name Server IP address.
Server IP	The IP address of your ISP's server computer, as stated to you by your ISP.
User Name	The account name of the L2PT account that has been assigned to you by your ISP.
Password	The password of the L2PT account that was supplied to you by your ISP.
Retype Password	Retype the password that was entered in the L2PT field. Ensure that these two passwords are identical or an error will occur.
Maximum Idle Time	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in minutes). This will disconnect the Router after the WAN connection has been idle for the amount of time specified.
MTU	The Maximum Transmission Unit size may be changed if you want to optimize efficiency for uploading data through the WAN interface. The default setting (1400 bytes) should be suitable for most users. Some user may want to adjust the setting to optimize performance for wireless traffic or when low latency is desired (such as with Internet gaming). It is highly recommended that the user research how adjusting the MTU may affect network traffic for better or worse.
Connect mode select	Select the desired option: Always on, Manual, or Connect on demand. Most users will want to choose the default connection setting, Always on.

HOME - LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.

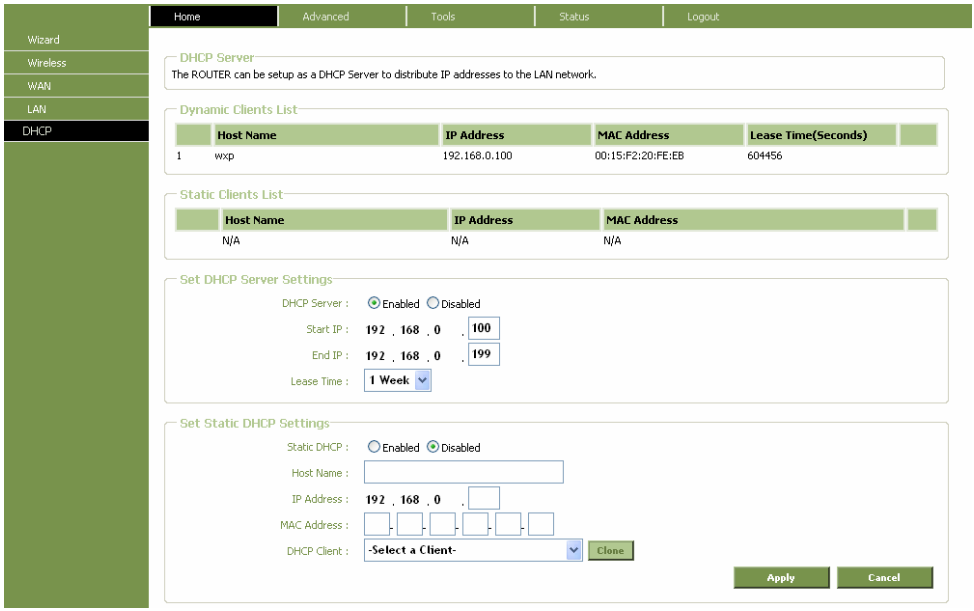


LAN Settings window

To change the LAN **IP Address** or **Subnet Mask**, type in the desired values and click the **Apply** button. Your web browser should automatically be redirected to the new IP address. You will asked to login again to the Router's web manager.

HOME - DHCP

The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.



DHCP window

To display this window, click the **DHCP** button in left menu. Any active DHCP Clients appear at the top of the window in the DHCP Clients List. The IP address and MAC address for active DHCP clients are displayed in the list.

The two options for DHCP service are as follows:

- You may use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Apply** button to commit the new settings.

Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted. The **Starting IP Address** is the lowest available IP address. If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router.

The **Ending IP Address** is the highest IP address number in the pool. Select the desired **Lease Time** from the drop-down menu. This is the amount of time that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

Disable the DHCP Server

To disable DHCP, click the Disabled **DHCP Server** radio button and then click the **Apply** button. Choosing this option requires that workstations on the local network must be configured manually or use another DHCP server to obtain IP settings.

If you configure IP settings manually, make sure to use IP addresses in the subnet of the Router. You will need to use the Router's IP address as the Default Gateway for the workstation in order to provide Internet access.

Menu - Advanced

The Advanced folder contains main windows for Virtual Server, Special Applications, Firewall Rules, DMZ, IP Filters, MAC Filters, URL Blocking, Domain Blocking, Wireless Performance, and Dynamic DNS.

ADVANCED – VIRTUAL SERVER

Use this window to set up forwarding rules applied to inbound (WAN-to-LAN) traffic. The Virtual Server function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The Wireless Broadband Router will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the Router.

UDP/TCP port redirection is used to direct inbound traffic to the specified servers or workstations on your private network. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router to direct HTTP packets to a designated HTTP server in the DMZ. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each set of instructions or rule is indexed and can be modified or deleted later as needed.

Below you will find a list of some common used ports and their corresponding application:

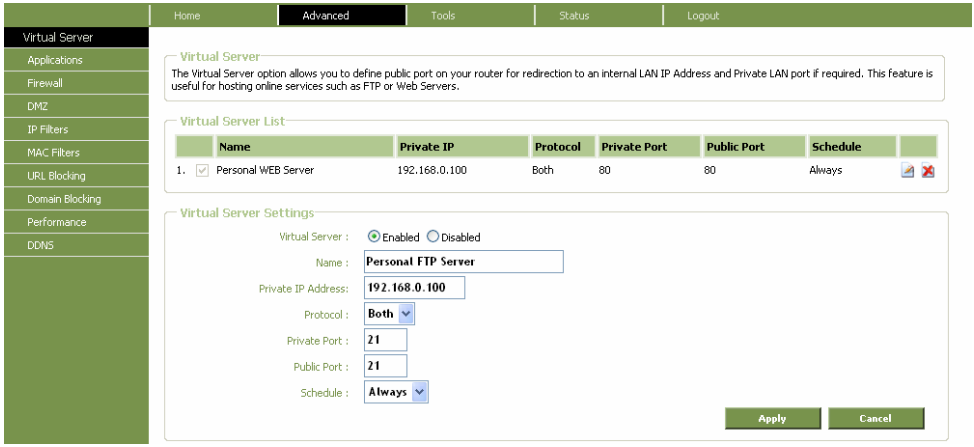
Port	Application	Port	Application
20	FTP Data (FTP Server)	**80**	HTTP (Web Server)
21	FTP (FTP Server)	**110**	POP3 (Mail Server – Incoming)
22	SSH (Secure Shell)	**2000**	Remotely Anywhere
23	Telnet	**5800**	VNC
25	SMTP (Mail Server – Outgoing)	**5900**	VNC

For more ports and their corresponding applications, see: http://portforward.com/cports.htm

Note: When you are using an application which supports UPnP Port Mapping, the router can be automatically configured by the application when needed. In that case, you don't need to setup your port mappings manually.

Note: When using Virtual Server rules, it is advised to configure the computer(s) with a Fixed IP Address instead of a Dynamic IP Address.

Note: In the picture below you will see an example of a Virtual Server configuration.



Virtual Server window

1. Set the Virtual Server rule to "**Enabled**".
2. Enter a name for your Virtual Server Rule in the "**Name**" field.
3. Enter the IP Address of your computer/server which needs the Virtual Server rule.
4. Select the Protocol for your Virtual Server rule: "**TCP**", "**UDP**" or "**Both**".

Note: If you do not know which protocol you need for your Virtual Server Rule, select "**Both**". This option will pass both TCP and UDP traffic to the configured IP Address of your computer/server.

5. Enter the desired Port of your computer/server which needs the Virtual Server rule.

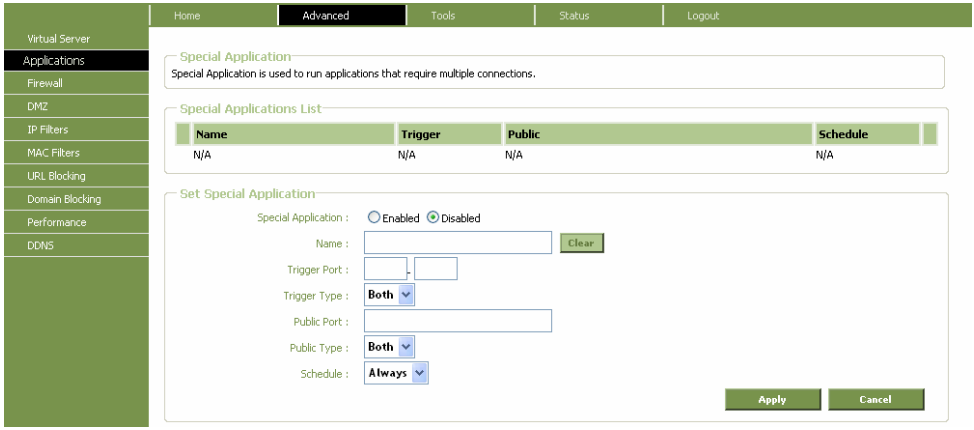
6. Enter the port which must be visible on the outside of your internet connection.

7. Click "**Apply**" to apply the created Virtual Server rule.

When the Virtual Server rule is saved, it will be shown in the "**Virtual Server List**".
To create more Virtual Server rules, repeat step **1 - 7.**

ADVANCED - APPLICATIONS

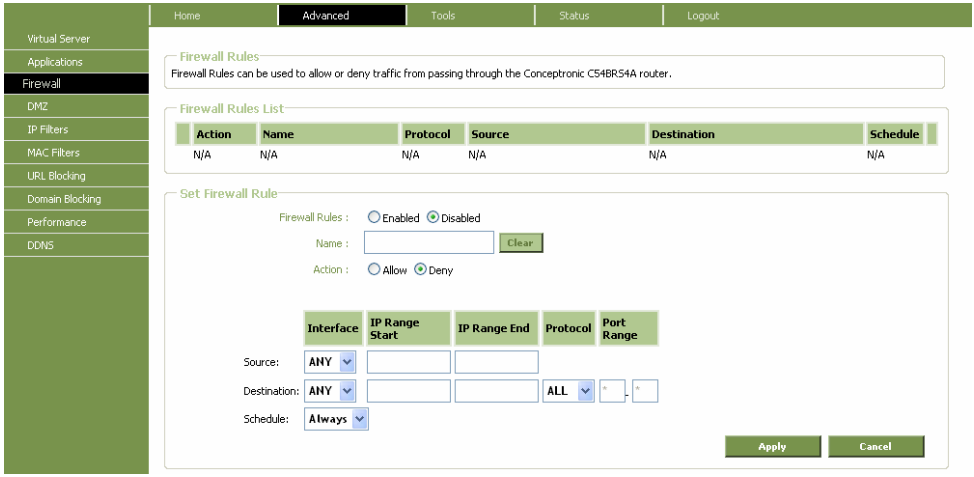
Use this window to run special applications that require multiple connections. To use the Special Applications feature, enter the requested information for your application and click the **Apply** button.



Special Application window

ADVANCED - FIREWALL

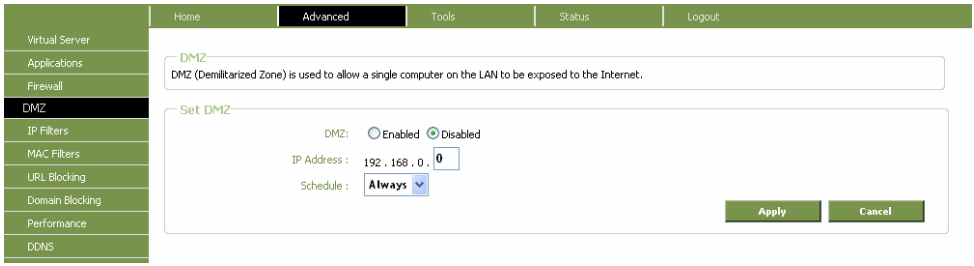
This window allows the user to allow or deny traffic from passing through the Wireless Broadband Router. Once you have completed your Firewall settings, click **Apply** to save your changes.



Firewall Rules window

ADVANCED - DMZ

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

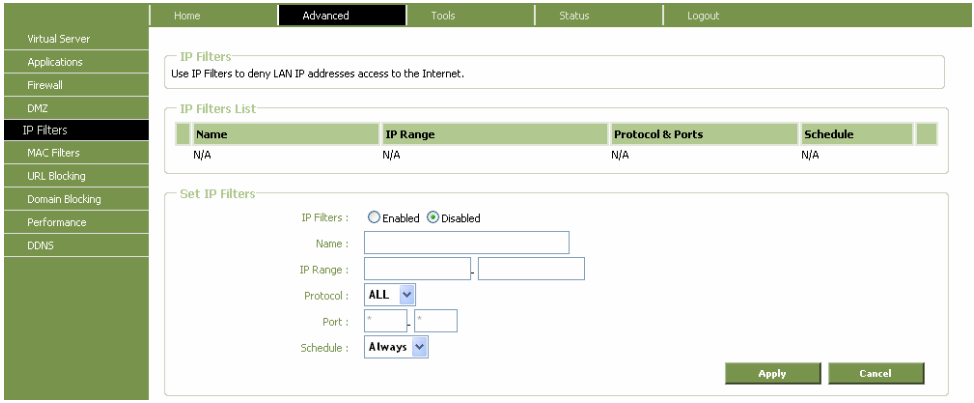


DMZ window

To designate a DMZ IP address, select the **Enabled** radio button, type in the **IP Address** of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, select the Disabled radio button and click **Apply**. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

ADVANCED - IP FILTERS

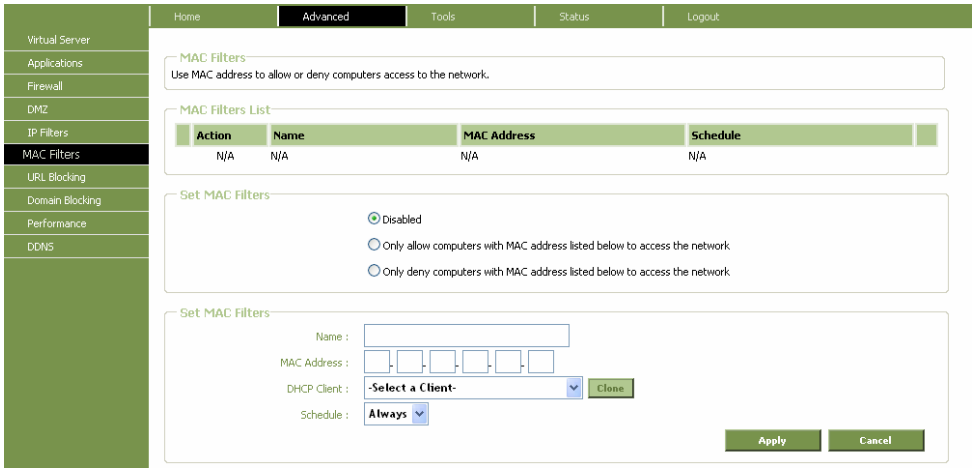
This window allows the user to allow or deny LAN IP addresses access to the Internet. Rules are based on IP address and TCP/UDP port. Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the IP Filters List at the top of the window.



IP Filters window

ADVANCED - MAC FILTERS

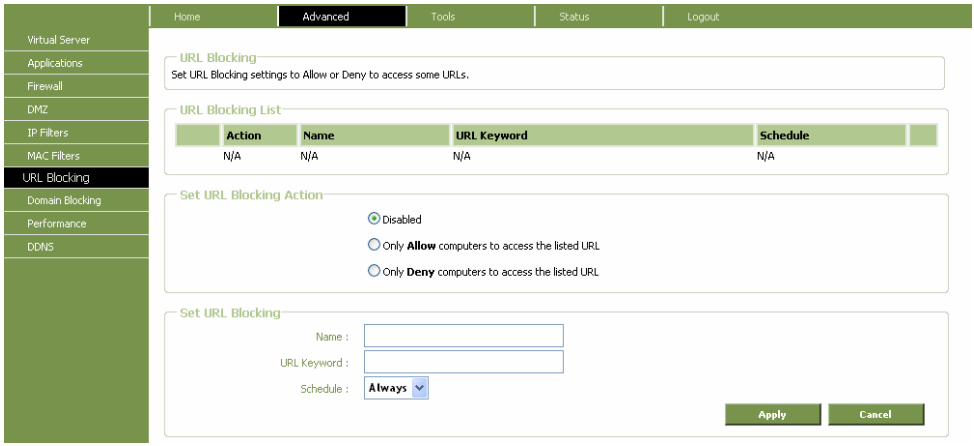
MAC filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured. Configure the MAC filter rules as desired and click the **Apply** button to create the rule.



MAC Filters window

ADVANCED - URL BLOCKING

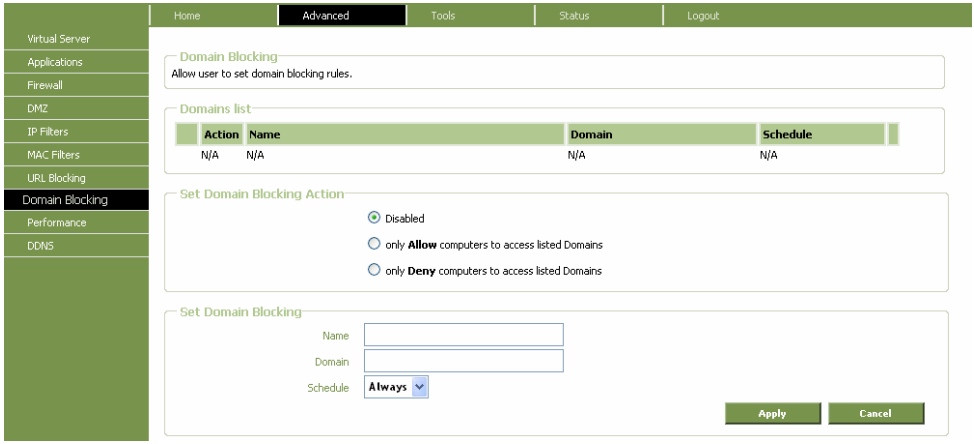
URL blocks are used to block or allow access to specific websites. Enter the URLs in the **URL Keyword** field and click the **Apply** button to add the Website to be blocked.



URL Blocking window

ADVANCED – DOMAIN BLOCKING

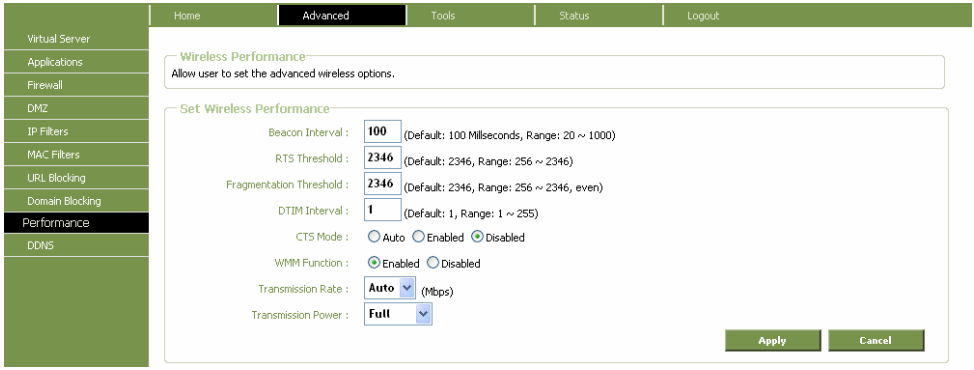
Domain blocks are used to block or allow access to specific domains. Enter a domain in either the **Blocked Domains** field or the **Permitted Domains** and click the **Apply** button to either add or subtract the domain to be blocked.



Domain Blocking window

ADVANCED - PERFORMANCE

This window allows the user to change wireless performance features pertaining to the Access Point portion of the Wireless Broadband Router. Click **Apply** to save your changes.



Wireless Performance window

Beacon Interval Beacons are packets sent by an access point to synchronize a network. Specify the beacon value for the selected device(s) here. The default value of *100* is recommended.

RTS Threshold The RTS value should not be changed unless you encounter inconsistent data flow. Only minor modifications to the value range between 256 and 2,346 are recommended. The default value is *2346*.

Fragmentation This sets the fragmentation threshold (specified in bytes) and determines whether packets will be fragmented. Packets exceeding the byte setting will be fragmented before transmission. The default is *2346* bytes.

DTIM Interval Delivery Traffic Indication Message is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default value is *1*.

CTS Mode The Clear To Send mode is designed to minimize collisions among wireless devices. Most users will want to keep the default setting of *Auto*.

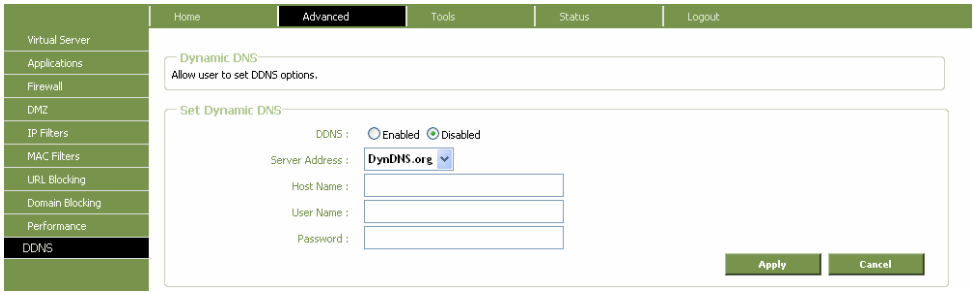
WMM Function Enable or disable the Wireless MultiMedia function.

TX Rate A pull-down menu for selecting the transmitting rate: *Auto*, *1*, *2*, *5.5*, *6*, *9*, *11*, *12*, *18*, *24*, *36*, *48*, and *54*.

Transmit Power A pull-down menu for selecting the transmit power of the device. You can choose among: *100%*, *50%*, *25%*, and *12.5%*.

ADVANCED - DDNS

The Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, and this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS providers.



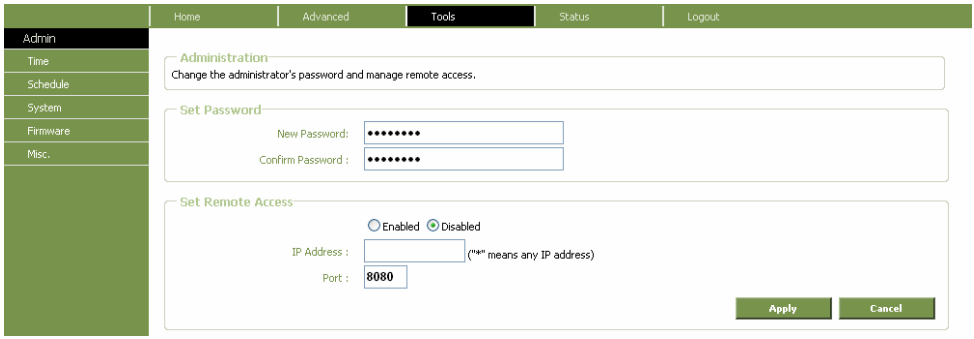
Dynamic DNS window

Please note that DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the Router. This function will not work without an accepted account with a DDNS server. Enter the required DDNS information and click **Apply** to set this information in the Router.

Menu „Tools”

TOOLS - ADMIN

If you click on **Tools** menu and then **Admin**, the following page will open.



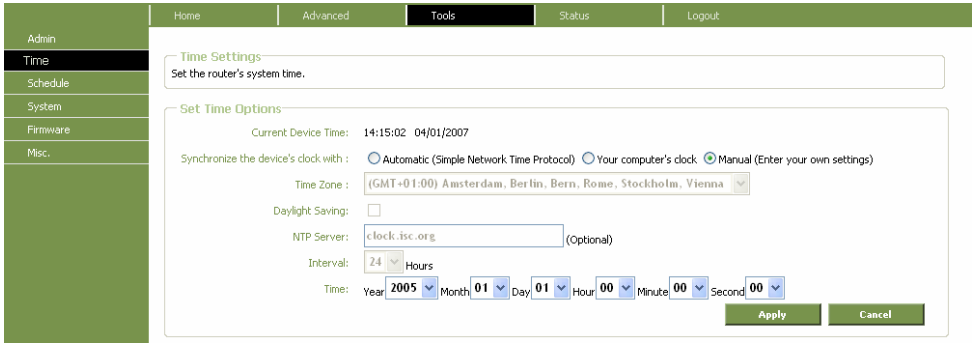
Administrator Settings window

Enter your new password in the **New Password** field and then type it again in the **Confirm New Password** field. The default User Name is “admin.”

The **Administration** window is also used to enable remote management access to the Router. To enable remote management of the Router, select the Enabled radio button and type the IP Address of the remote network used for management. Click the **Apply** button to activate remote management from the chosen IP address. Be sure to save the new setting.

TOOLS - TIME

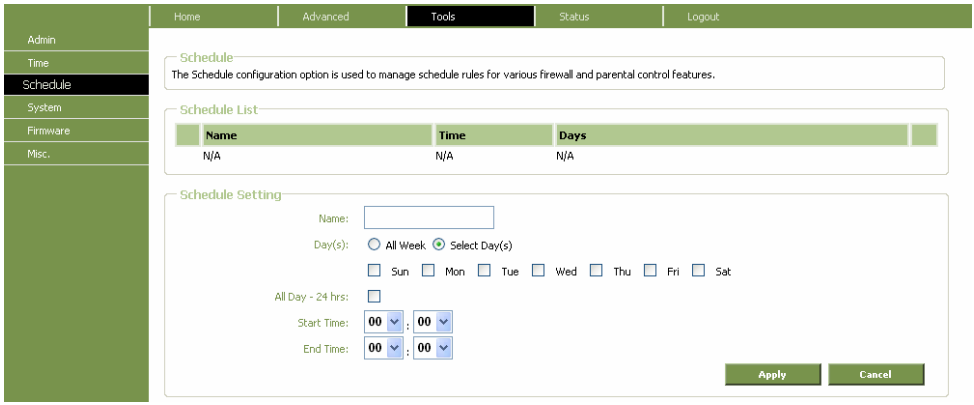
The Router provides a number of options to maintain current date and time including SNTP.



Time window

To configure system time on the Router, select the method used to maintain time. The options available include SNTP, using your computer's system clock (default) or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Apply** button to set the system time.

TOOLS - SCHEDULE



Schedule window

The Schedule configuration option is used to manage scheduled rules for various firewall and parental control features.
Enter the information needed for your schedule setting and press **Apply** to add it to the Schedule List.

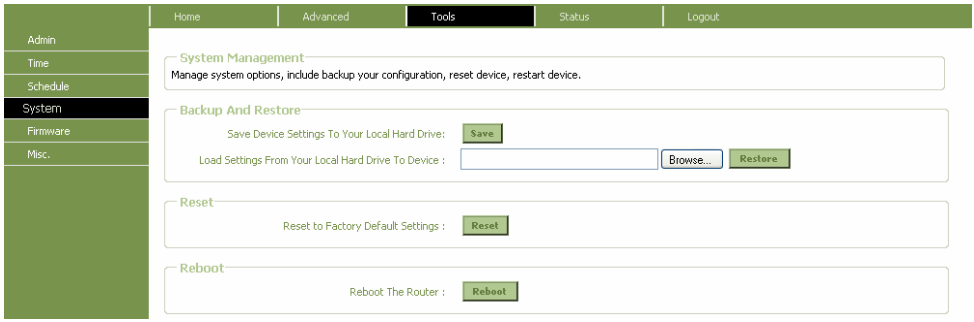
TOOLS - SYSTEM

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **System** button in the **Tools** directory to display the **System Settings** window. Click the **Save** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Restore** button to *Load Settings from Local Hard Drive*. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.

To reset the Router to its factory default settings, click the **Reset** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings (192.168.0.1) and Administrator password (admin).

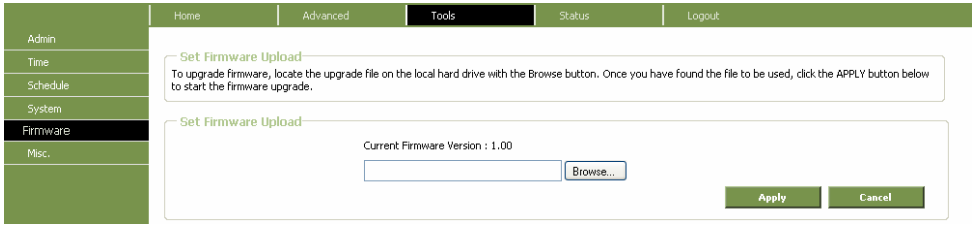
To simply restart the Router, click the **Reboot** button.



System Settings window

TOOLS - FIRMWARE

Use this window to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the **System Settings** window described above.



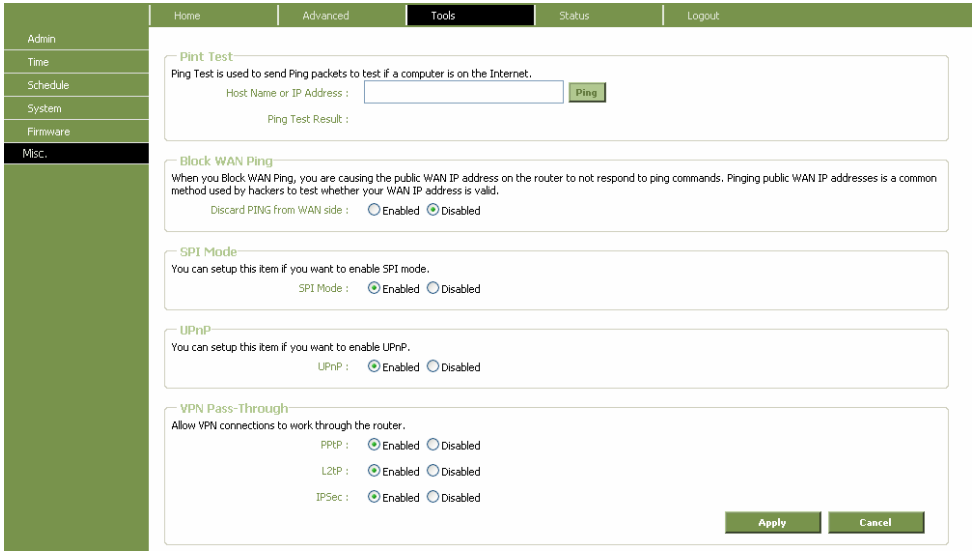
Firmware Upgrade window

To upgrade firmware to the router, type in the name and path of the file, or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the Router automatically.

Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware.

TOOLS - MISC

To perform a standard Ping test for network connectivity as well as a number of miscellaneous network tasks, click the **Misc.** button in the **Tools** menu to view the **Miscellaneous Configuration** window.



Ping Test window

Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the **Host Name or IP Address** you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below

Block WAN Ping

The Block WAN Ping feature allows the user to block hackers who may be trying to test whether your WAN IP address is valid.

SPI mode

Stateful Packet Inspection mode is an active firewall the user can enable to keep track of the state of network connections.

UPnP Settings

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network. UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.

VPN Pass-Through

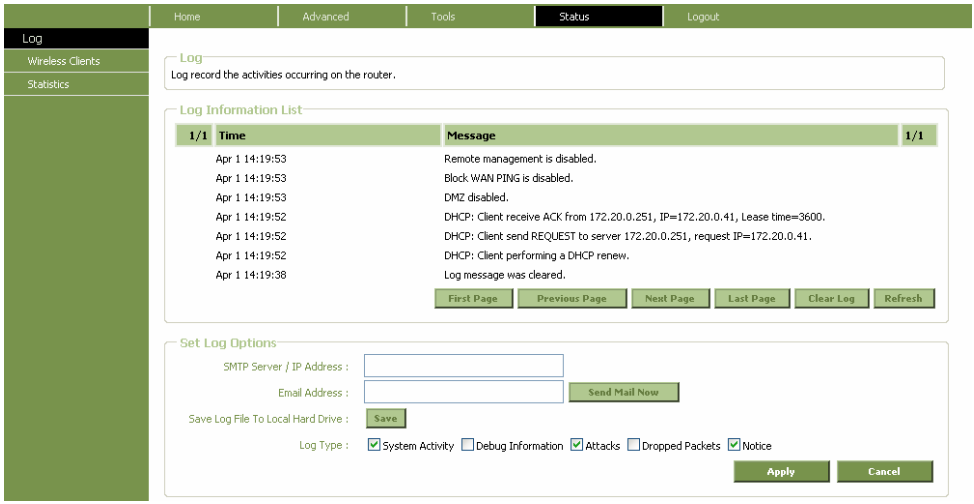
This feature allows VPN connections to pass through the Router. It is enabled by default.

Menu “Status”

Use this window to quickly view basic current information about the LAN, WAN, and wireless interfaces and device information including Firmware Version and MAC address.

STATUS - LOG

The system log displays chronological event log data. Use the navigation buttons to view or scroll log pages.

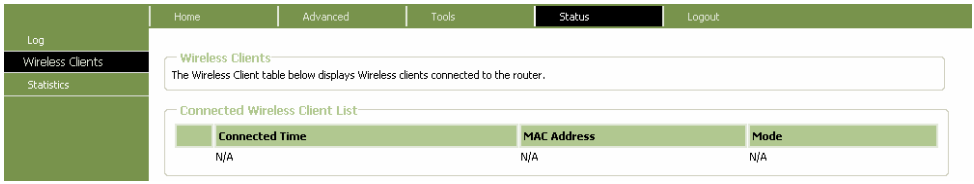


View Log window

You may also save a log by sending it to an admin e-mail address.
Complete the information on this window and then click the **Apply** button.

STATUS – WIRELESS CLIENTS

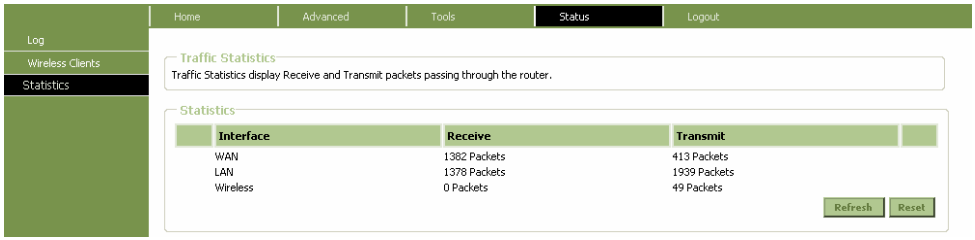
This window displays all the wireless clients currently connected to the AP portion of the Wireless Broadband Router.



Connected Wireless Client List window

STATUS - STATISTICS

Use this window to monitor traffic on the WAN, LAN, and Wireless connections.



Traffic Statistics window

Click **Refresh** to view traffic information.
Click **Reset** to reset the traffic information.

Technical Specifications

Standards

IEEE 802.11b
IEEE 802.11g
IEEE 802.3
IEEE 802.3u

Device Management

Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java-enabled browsers.

Data Rate

For 802.11g:
108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps
For 802.11b:
11, 5.5, 2, and1Mbps

Security

64- and 128-bit WEP
WPA – WiFi Protected Access (WPA-TKIP/PSK/AES)
802.1x (EAP-MD5/TLS/TTLS/PEAP)
MAC Address Access Control List

Wireless Frequency Range

2.4GHz to 2.4835GHz

Wireless Operating Range*

802.11g (Full Power with 2dBi gain diversity dipole antenna)
Indoors:
98ft (30m) @ 54Mbps
105ft (32m) @ 48Mbps
121ft (37m) @ 36Mbps
148ft (45m) @ 24Mbps
197ft (60m) @ 18Mbps
223ft (68m) @ 12Mbps
253ft (77m) @ 9Mbps
295ft (90m) @ 6Mbps
Outdoors:
312ft (95m) @ 54Mbps
951ft (290m) @ 11Mbps
378ft (420m) @ 6Mbps

Antenna Type

Dipole antenna with 2dBi gain

Operating Voltage

5VDC +/- 10%

Radio and Modulation Type

For 802.11g:

OFDM:

BPSK @ 6 and 9Mbps
QPSK @ 12 and 18Mbps
16QAM @ 24 and 36Mbps
64QAM @ 48 and 54Mbps

DSSS:

DBPSK @ 1Mbps
DQPSK @ 2Mbps
CCK @ 5.5 and 11Mbps

For 802.11b:

DSSS:

DBPSK @ 1Mbps
DQPSK @ 2Mbps
CCK @ 5.5 and 11Mbps

Wireless Transmit Power

Typical RF Output Power at each Data Rate

For 802.11g:

31mW (15dBm) @ 54 and 108Mbps
40mW (16dBm) @ 48Mbps
63mW (18dBm) @ 36, 24, 18, 12, 9, and 6Mbps

For 802.11b:

63mW (18dBm) @ 11, 5.5, 2, and 1Mbps

Receiver Sensitivity

For 802.11g:

1Mbps: -94dBm
2Mbps: -91dBm
5.5Mbps: -89dBm
6Mbps: -91dBm
9Mbps: -90dBm
11Mbps: -86dBm
12Mbps: -89dBm
18Mbps: -87dBm
24Mbps: -84dBm
36Mbps: -80dBm
54Mbps: -73dBm

For 802.11b:

1Mbps: -94dBm
2Mbps: -90dBm
5.5Mbps: -88dBm
11Mbps: -85dBm

LEDs

Power
Status
WAN
WLAN
LAN

Temperature

Operating: 32ºF to 113ºF (0ºC to 45ºC)
Storing: -4ºF to 149ºF (-20ºC to

Humidity

Operating: 10%~95% (non-condensing)
Storing: 5%~95% (non-condensing)

Certifications

FCC Class B
CE Class B
C-Tick
UL
TUV

Dimensions

L = 149mm
W = 109mm
H = 35mm

Weight

237.2g

LICENCE AGREEMENT

Licensing Information

This Conceptronic product C54BRS4A includes copyrighted third-party software licensed under the terms of the GNU General Public License.
Please see The GNU General Public License for the exact terms and conditions of this license.

Specially, the following parts of this product are subject to the GNU GPL:

1. Linux kernel 2.4.25
2. buildroot
3. busybox-1.00
4. vconfig
5. iptable-1.2.9
6. mathopd
7. pppd-2.4.2
8. dnrd-2.10
9. klogd
10. syslogd
11. telnetd
12. wireless tools
13. bpalogin
14. hostapd-0.3.7
15. smtpclient
16. ntpclient

All listed software packages are copyright by their respective authors. Please see the source code for detailed information.

Availability of source code

Conceptronic has exposed the full source code of the GPL licensed software, including any scripts to control compilation and installation of the object code. All future firmware updates will also be accompanied with their respective source code. For more information on how you can obtain our open source code, please visit our web site.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another
language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

LICENCE AGREEMENT

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not

permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this

section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

CE DECLARATION

The manufacturer Conceptronic
Address Databankweg 7
3821 AL Amersfoort, the Netherlands

Hereby declares that the product
Type Wireless 54Mbps broadband router
Product C54BRS4A

Complies with following directives:

- 1999/5/EEC R&TTE directive:
  Telecommunications Terminal Equipment and Satellite Earth Station Equipment

- 89/336/EEC EMC directive:
  Electromagnetic Compatibility

- 73/23/EEC Low Voltage Directive:
  Electrical equipment designed for use within certain voltage limits

The following standards were consulted to assess conformity:
EN 300 328-2/2000, EN 301 489-17-2000, EN 301 489-1-2000, EN55022/9.98 Class B, EN 61000-3-2/3/4/1995, EN 50082-1/1994, EN 60950/1995

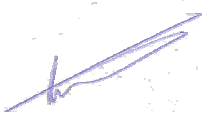
This product is for indoor use only. The purpose of this product is to send and receive data trough the ether. This is a class 2 product and the transmitted output power is less than 100mW.

CE

The CE symbol confirms that this product conforms to the above named standards and regulations.

This product is suitable for all EU countries.
For France, the output power is restricted if used outdoor and in the range 2454 to 2483,5 MHz.
For Italy, depending on the usage, a general authorization may be required.
Pour tous les pays de l'UE. Pour la France, pour une utilisationen extérieur, la puissance de sortie est limitée dans la bande 2454 to 2483,5 MHz.Pertutti i paesi ell'EU.
Per l'Italia, secondo l'uso, un 'autorizzazione generale puô essere richiesta.

Place and date of issue: Amersfoort, March 18, 2007



Herman Looijen, Product Marketing Manager