Kx EasyBackUp Pro

User's Guide

Version: 1.1

Date: October 4, 2011

KORTEX PSI
91 rue Réaumur
75002 Paris
Tel: +33-1-34043760
e-mail: contact@kortex-psi.fr

Revision History

Version	Date	Changes
1.0	December 197, 2008	First Release of Kx EasyBackUp Pro User's Guide
1.1	October, 4 2011	Logo & address update

Table of Contents

1. Product Overview

1.1 Introduction

Kx EasyBackUp Pro, a 3G/3.5G WiFi Router, with a built-in modem, it has failover function using the dial-up modem. Not only can it be used as a regular router to connect to ADSL / Cable modem but also as a PPP router using the dial-up modem to connect to the ISP. The dial-up modem could be ***PSTN V.90, GPRS, CDMA, EVDO, 3G / 3.5G HSDPA and Edge modem***, etc.

The router will use WAN as the first priority and the dial-up modem as the backup. Once the WAN port is active, it will switch to WAN and disconnect the dial-up connection. The router will automatically dial to ISP if WAN is not active and there is data to be transmitted.

1.2 Features

- Automatically backup and restore broad band WAN and Dialup WAN.
- As VPN client or pass-through.

1.3 Package Contents

– 1 x Kx EasyBackUp Pro Router

– 1 x CD with Quick Installation Guide and User's Manual

– 1 x RJ45 Ethernet Cable

– 1 x Power Adapter

2. Physical Description

The following information contains the physical description of Kx EasyBackUp Pro router. This includes the functions and the locations of each connector and indicator. This information provides useful reference when installing the product. Please familiarize yourself with Kx EasyBackUp Pro.

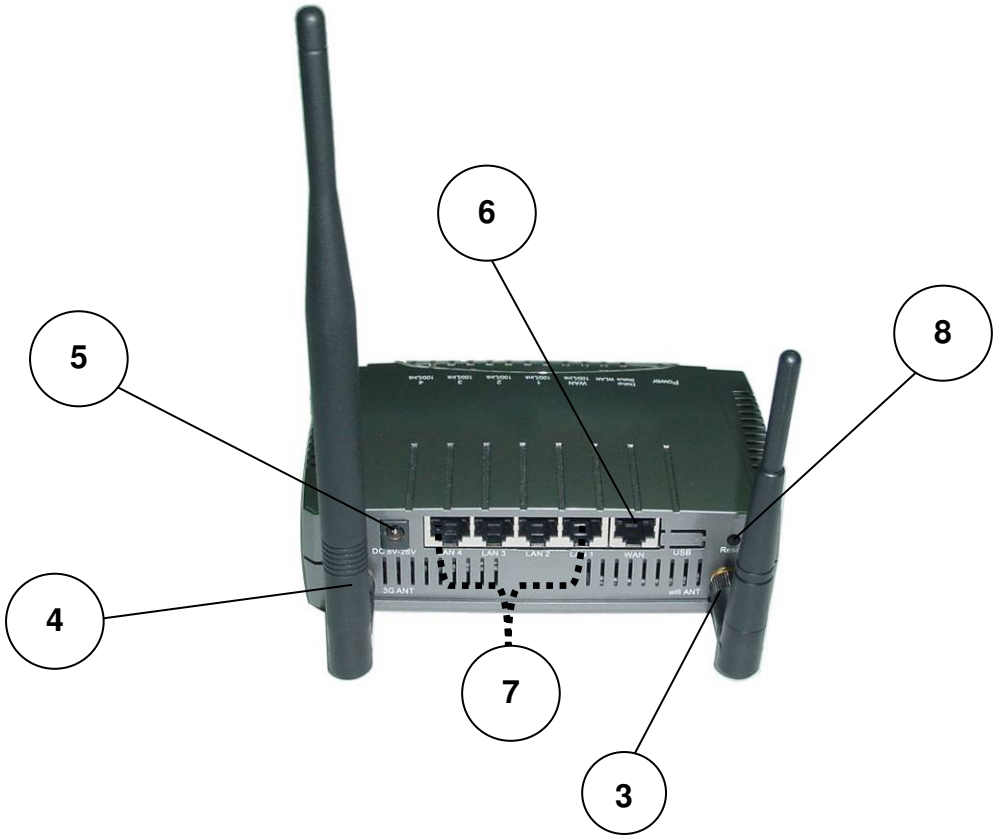
2.1 Panels

2.1.1 Front Panel

For more related description, please refer to the Section 2.2 and Section 2.2.1.

2.1.2 Rear Panel

For more detailed description, please refer to the Section 2.2 and Section 2.2.2.



2.2 Illustration

No. in Figures	Name on Kx EasyBackUp Pro	Description	Remark
1	SIM Card Slot	To connect with the internal modem	Refer to section 2.2.1 for the front panel information
2	LEDs	To display the status of Kx EasyBackUp Pro	Refer to section 2.2.3 for the LED description on the front panel
3	Wifi ANT SMA Connector	To connect with the wifi antenna	Refer to section 2.2.2 for Real panel information
4	3G ANT SMA Connector	To connect with the 3G antenna	Refer to section 2.2.2 for Real panel information
5	Power Supply Connector	To connect with the Kx EasyBackUp Pro and the power adapter	Refer to section 2.2.2 for Real panel information
6	WAN Port	For the access of Internet	Refer to section 2.2.2 for Real panel information
7	LAN1~LAN 4 Network Connectors	To connect to the device and Ethernet port via RJ45 cable	Refer to section 2.2.2 for Real panel information
8	Reset Button	To reset the Kx EasyBackUp Pro to its factory defaults	Refer to section 2.2.2 for Real panel information

2.2.1 Front Panels Information

SIM Card Slot

Plug the internal modem.

LEDs

Include the LED of POWER, Dialup status, WLAN (Wireless LAN), WAN 100/10 or Link, LAN 100/10 or Link.

2.2.2 Rear Panel Information

wifi ANT SMA Connector

Support WEP and WPA modes for wireless access.

3G ANT SMA Connector

Support 3G mode for wireless access.

Power Supply Connector

Plug the power adapter. The specifications of Kx EasyBackUp Pro's power adapter are as follows:

- Input: 100 ~ 240V AC, 50/60Hz
- Output: 12V DC / 1.5A

WAN Port

Offer the access of Internet.

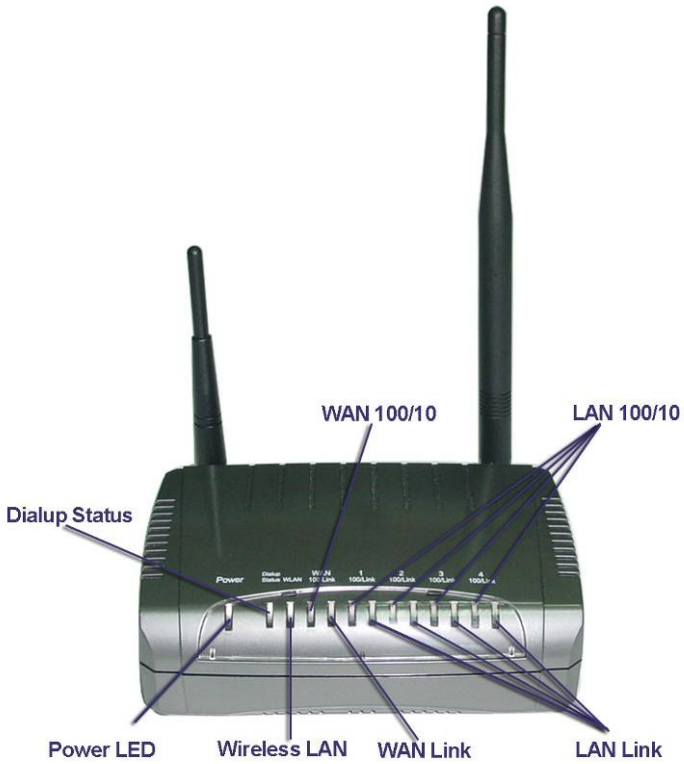
LAN Port

Kx EasyBackUp Pro is designed for 10/100Mbps Ethernet networks. Kx EasyBackUp Pro connects to the network via category 5 cable.

Reset Button

Support the hardware reset function.

2.2.3 LED Description on the Front Panel

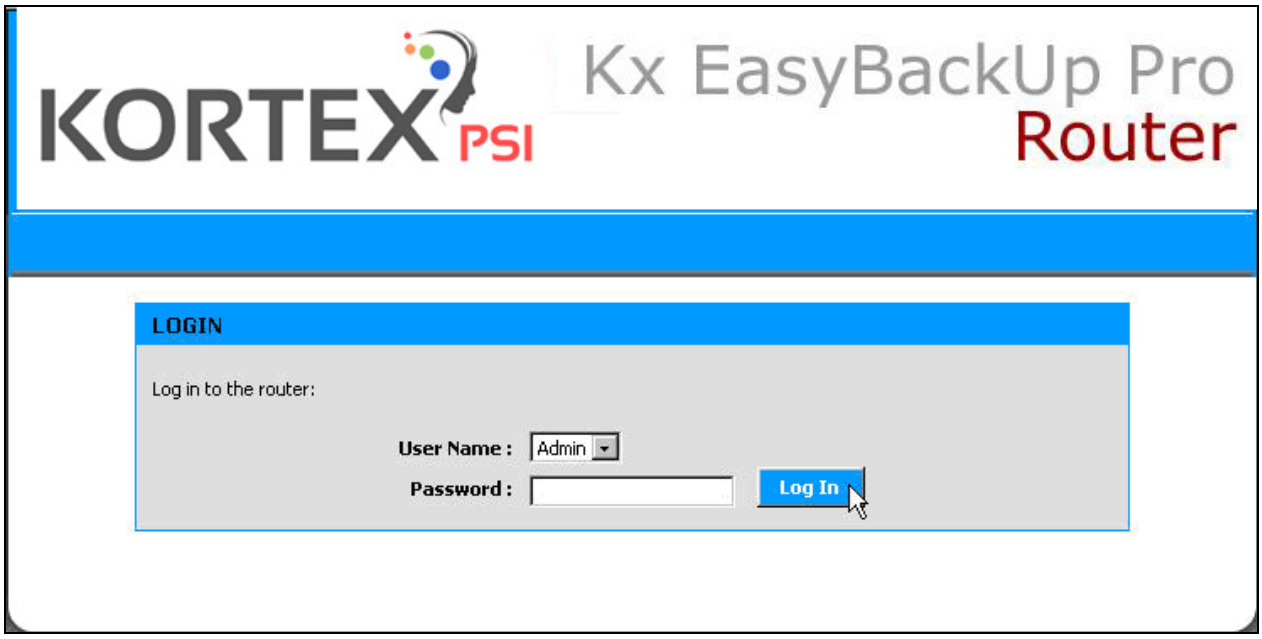


LED	Color	Status
POWER	Green	Lit when +12V DC power is on and working.
Dialup status	Green	Lit when dialup is connected. Flash when dialup is connecting at 1Hz rate. Off when dialup is disconnected. Flash when any traffic is present.
WLAN(Wireless LAN)	Green	Lit when device is normal. Flash when any traffic is present.
WAN 100/10 or Link		
WAN 100/10	Green	Lit when connection with remote device is 100MHz. Off when connection with remote device is 10MHz.
WAN Link	Green	Lit when connection with remote device is good. Flash when any traffic is present. Off when cable connection is not good.
LAN Port 1 to 4 100/10 or Link		
LAN 100/10	Green	Lit when connection with remote device is 100MHz. Off when connection with remote device is 10MHz.
LAN Link	Green	Lit when connection with remote device is good. Flash when any traffic is present. Off when cable connection is not good.

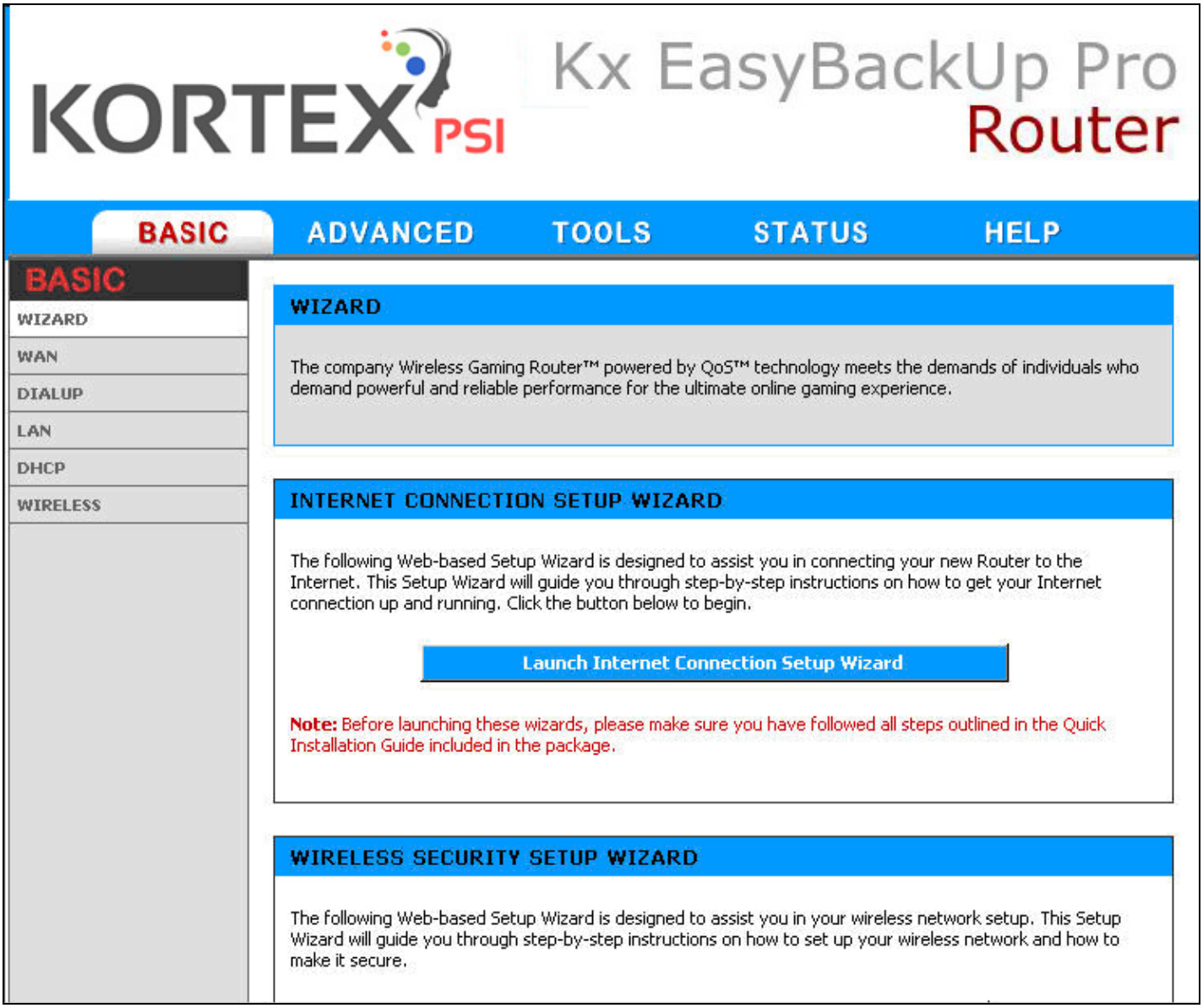
3. Web-Based Management

This chapter instructs you how to configure and manage the Kx EasyBackUp Pro through the web user interface it supports. With this facility, you can easily access and monitor through any one LAN port of the Kx EasyBackUp Pro router.

After Kx EasyBackUp Pro has been connected to your PC via RJ45 network cable, type http://192.168.8.1 in IE browser, it will show the following screen and ask you to input the user name and password in order to login and access authentication. The default user name is **"admin"** or **"user"**, and the password is blank. With the former user name to login, the user is able to fully access and configure the system. As to the latter, the user merely owns the right to read the system. For the first time to use, please enter the default user name and keep the password blank, then click the **Log In** button. The setup page for Kx EasyBackUp Pro will be displayed once the login process is successful.



In the router, it supports a simple user management function to configure the system. As the figure below shows, for example, left section is the whole list of sub functions while each of main functions, including BASIC, ADVANCED, TOOLS, STATUS AND HELP is selected.



3.1. Basic

3.1.1 Wizard

Internet Connection Setup Wizard:
This wizard guides you through the following basic router setup steps:

- Set your Password
- Select your Time Zone
- Configure your Internet Connection

3.1.2 WAN

The WAN (Wide Area Network) section is where you configure your Internet connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, L2TP, and BigPond. If you are unsure of your connection method, please contact your Internet Service Provider. Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.

3.1.2.1 Static WAN Mode

Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings. You must enter the **IP address**, **Subnet Mask**, **Gateway**, **Primary DNS Server**, and **Secondary DNS Server**. Your ISP provides you with all of this information.

3.1.2.2 DHCP WAN Mode

A method of connection where the ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet.

Host Name: Some ISP's may check your computer's Host Name. The Host Name identifies your system to the ISP's server. This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service.

Use Unicasting: This option is normally turned off, and should remain off as long as the WAN-side DHCP server correctly provides an IP address to the router. However, if the router cannot obtain an IP address from the DHCP server, the DHCP server may be one that works better with unicast responses. In this case, turn the unicasting option on, and observe whether the router can obtain an IP address. In this mode, the router accepts unicast responses from the DHCP server instead of broadcast responses.

Enable BigPond: Check this option to connect to the Internet through Telstra BigPond Cable Broadband in Australia. Telstra BigPond provides the values for **BigPond Server**, **BigPond User Id**, and **BigPond Password**.

3.1.2.3 PPPoE

Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Dynamic IP: If your ISP has assigned a fixed IP address, select this option. The ISP provides the value for the **IP Address**.

Static IP: If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.

Service Name: Some ISP's may require that you enter a Service Name. Only enter a Service Name if your ISP requires one.

Reconnect Mode: Typically connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.
- **Manual:** You have to open up the web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.

Maximum Idle Time: Time interval the machine can be idle before the PPPoE connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

3.1.2.4 PPTP

PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Dynamic IP: If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields: **PPTP IP Address**, **PPTP Subnet Mask**, and **PPTP Gateway IP Address**.

Static IP: If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.

PPTP Server IP Address: The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.

Reconnect Mode: Typically PPTP connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.
- **Manual:** You have to open up the web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.

Maximum Idle Time: Time interval the machine can be idle before the PPTP connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

3.1.2.5 L2TP

L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Dynamic IP: If your ISP has assigned a fixed IP address, select this option. The ISP provides the values for the following fields: **L2TP IP Address**, **L2TP Subnet Mask**, and **L2TP Gateway IP Address**.

Static IP: If the ISP's servers assign the router's IP addressing upon establishing a connection, select this option.

L2TP Server IP Address: The ISP provides this parameter, if necessary. The value may be the same as the Gateway IP Address.

Reconnect Mode: Typically L2TP connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.
- **Manual:** You have to open up the web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.

Maximum Idle Time: Time interval the machine can be idle before the L2TP connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

Use These DNS Servers: This option should be enabled if your ISP requires you to enter the DNS Server information. You will then be able to enter a primary and secondary DNS server.

Advanced >>: These options apply to all WAN modes.

Use the default MTU: If this option is checked (the default case), the router selects the usual MTU settings for the type of WAN interface in use. If this option is unchecked, the router uses the value of the MTU option (which follows).

MTU: The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

WAN Port Speed: Normally, this is set to "auto". If you have trouble connecting to the WAN, try the other settings.

Respond to WAN Ping: If you leave this option unchecked, you are causing the public WAN IP address of the router not to respond to **ping** commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

WAN Ping Inbound Filter: Select a filter that controls access as needed for WAN pings. If you do not see the filter you need in the list of filters, go to the Advanced -> Inbound Filter screen and create a new filter.

MAC Cloning Enabled: Some ISP's may check your computer's MAC address. Each networking **device** has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new KORTEX PSI router has a different MAC address than the computer or router that initially connected to the ISP. To resolve this problem, the KORTEX PSI router has a special feature that allows you to clone (that is, replace the router's MAC address with) another MAC address.

MAC Address: If you have enabled MAC Cloning, you can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the KORTEX PSI router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

3.1.3 DIALUP

The Dialup WAN (Wide Area Network) section is where you configure your Dialup up Backup Connection type. There are several modem types to choose from: Standard landline PSTN and two Cellular GPRS and CDMA.

Enable Dialup WAN: If you want to have a backup Dialup WAN connection, click on this checkbox and then configure the following sections.

WAN Interaction: This controls how long the router will look for the Ethernet WAN port before attempting to use the Dialup port. If the value of WAN Link Timeout is set to 0 then the Ethernet WAN port will not be used at all. In this mode of operation the KORTEX PSI router will operate between the LAN and the Dialup port only. The router will also connect to PPTP or L2TP server once you choose PPTP or L2TP as your WAN Mode while accessing the Internet.

Modem Type: Select PSTN (Public Switched Telephone Service) for wired modems, There are two types of cellular modems supported: GPRS (GSM General Packet Radio Service) and CDMA.

PSTN Modem Control (Please note that this function does not work in Kx EasyBackUp Pro router): If you are using a PSTN Dialup modem, edit the following configuration parameters or use the default values.

Maximum Connecting Time: This is the amount of time that will be waited before ending a connection attempt.

Maximum Dial Retrys: This is the number of dialing attempts that will be retried per connection attempt.

Reconnect Mode: Typically connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.

Maximum Idle Time: Time interval the machine can be idle before the PSTN connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

Modem Initialization String: Enter any extra AT commands here. AT commands start with AT. Normally you will not need to enter any.

PSTN CallerID Phone Number: The user can wake up remotely the idle router to return into working status with this phone number / mobile phone number.

PSTN ISP Settings: Your ISP will provide you with the values to fill in for the required fields of **Phone Number**, **Username** and **Password**.

GPRS Modem Control: GPRS Modem Control. If you are using a GPRS Dialup modem, edit the following configuration parameters or use the default values.

Maximum Connecting Time: This is the amount of time that will be waited before ending a connection attempt.

Maximum Dial Retrys: This is the number of dialing attempts that will be retried per connection attempt.

Reconnect Mode: Typically connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.

Maximum Idle Time: Time interval the machine can be idle before the GPRS connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

Modem Initialization String: Enter any extra AT commands here. AT commands start with AT. Normally you will not need to enter any.

GPRS CallerID Phone Number: The user can wake up remotely the idle router to return into working status with this phone number / mobile phone number you set up.

GPRS ISP Settings: Your GPRS service provider will provide you with the values to fill in for the required fields of **GPRS Dial Command**, **Username**, **Password**, **Access Point Name (APN Gateway)**, and the correct **PDP Type**.

GPRS Dial Command: If your modem supports modem compatibility enter ATD*99***1#. If your modem does not enter AT+CGDATA=1.

PDP Type: IP is typically chosen.

Access Point Name (APN Gateway): This is required.

Local IP Address: If your service provided a static IP address enter it here. Else leave it blank or as 0.0.0.0 to get a dynamic IP address using DHCP.

Data Compression: The default is usually OFF.

Header Compression: The default is usually OFF.

SIM card PIN code: SIM card password for authentication.

CDMA Modem Control: If you are using a CDMA Dialup modem, edit the following configuration parameters or use the default values.

Maximum Connecting Time: This is the amount of time that will be waited before ending a connection attempt.

Maximum Dial Retrys: This is the number of dialing attempts that will be retried per connection attempt.

Reconnect Mode: Typically connections are not always on. The KORTEX PSI router allows you to set the reconnection mode. The settings are:

- **Always on:** A connection to the Internet is always maintained.
- **On demand:** A connection to the Internet is made as needed.

Maximum Idle Time: Time interval the machine can be idle before the PSTN connection is disconnected. The Maximum Idle Time value is only used for the "On demand" connection mode.

Modem Initialization String: Enter any extra AT commands here. AT commands start with AT. Normally you will not need to enter any.

CDMA CallerID Phone Number: The user can wake up remotely the idle router to return into working status with this phone number / mobile phone number you set up.

CDMA ISP Settings: Your CDMA service provider will provide you with the values to fill in for the **required** fields of **CDMA Dial Command**, **Username**, **Password** and **Data Service Type**.

CDMA Dial Command: If your modem supports modem compatibility enter ATD*99***1#. If your modem does not enter AT+CGDATA=1.

Data Service Type: This sets the AT command +CRM value. For Quick-Net-Connect(QNC) and 1xRTT select the correct PPP Packet Data service.

SIM card PIN code: SIM card password for authentication.

3.1.4 LAN

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

IP Address: The IP address of your router on the local area network. Your local area network settings are based on the address assigned here. For example, 192.168.0.1.

Subnet Mask: The subnet mask of your router on the local area network.

RIP Announcement: Used with multiple routers to broadcast routing information.

Router Metric: The metric or cost of the routes advertised in RIP announcements.

DNS Relay: When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.

Disable communication between wired and wireless LAN: Clicking on the checkbox in front of this function will cease the communication between wired and wireless LAN port.

Disable NAT: Disable the function of NAT(Network Address Translation).

3.1.5 DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).

Enable DHCP Server: Once your KORTEX PSI router is properly configured and this option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to your Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to "DHCP" or "Obtain an IP address automatically". When you set **Enable DHCP Server**, the following options are displayed.

DHCP IP Address Range: These two values (*from* and *to*) define a range of addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

It is possible for a computer or device that is manually configured to have an address that does reside within this range. In this case the address should be reserved (see Static DHCP Client below), so that the DHCP Server knows that this specific address can only be used by a specific computer or device.

Your KORTEX PSI router, by default, has a static IP address of 192.168.0.1. This means that addresses 192.168.0.2 to 192.168.0.254 (from 2 to 254) can be made available for allocation by the DHCP Server.

Example,

Your KORTEX PSI router uses 192.168.0.1 for the IP address. You've assigned a computer that you want to designate as a Web server with a static IP address of 192.168.0.3. You've assigned another computer that you want to designate as an FTP server with a static IP address of 192.168.0.4. Therefore the starting IP address for your DHCP IP address range needs to be 5 or greater.

Example,

Suppose you configure the DHCP Server to manage addresses From 100 To 199. This means that 3 to 99 and 200 to 254 are NOT managed by the DHCP Server. Computers or devices that use addresses from these ranges are to be manually configured. Suppose you have a web server computer that has a manually configured address of 192.168.0.100. Because this falls within the "managed range" be sure to create a reservation for this address and match it to the relevant computer (see Static DHCP Client below).

DHCP Lease Time: The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

Always Broadcast: If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

Number of Dynamic DHCP Clients:

In this section you can see what LAN devices are currently leasing IP addresses.

Revoke: The **Revoke** option is available for the situation in which the lease table becomes full or nearly full, you need to recover space in the table for new entries, and you know that some of the currently allocated leases are no longer needed. Clicking **Revoke** cancels the lease for a specific LAN device and frees an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

Add/Edit DHCP Reservation: This option lets you reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the KORTEX PSI router. The KORTEX PSI router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use this option.

MAC Address: To input the MAC address of your system, enter it in manually or connect to the KORTEX PSI router's Web-Management interface from the system and click the **Copy Your PC's MAC Address** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the KORTEX PSI router from the computer and click the **Copy Your PC's MAC Address** button to enter the MAC address.

As an alternative, you can locate a MAC address in a specific operating system by following the steps below:

Windows 98 Windows Me	Go to the Start menu, select Run, type in **winipcfg**, and hit Enter. A popup window will be displayed. Select the appropriate adapter from the pull-down menu and you will see the Adapter Address. This is the MAC address of the device.
Windows 2000 Windows XP	Go to your Start menu, select Programs, select Accessories, and select Command Prompt. At the command prompt type **ipconfig /all** and hit Enter. The physical address displayed for the adapter connecting to the router is the MAC address.
Mac OS X	Go to the Apple Menu, select System Preferences, select Network, and select the Ethernet Adapter connecting to the KORTEX PSI router. Select the Ethernet button an the Ethernet ID will be listed. This is the same as the MAC address.

Computer Name: You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way.
e.g. Game Server

DHCP Reservations List: This shows clients that you have specified to have reserved DHCP addresses. An entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit DHCP Reservation" section is activated for editing.

3.1.6 Wireless

The wireless section is used to configure the wireless settings for your Company router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

Enable Wireless Radio: This option turns off and on the wireless connection feature of the router. When you set this option, the following parameters are displayed.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

Visibility Status: The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Auto Channel Select: If you select this option, the router automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the router uses the channel that you specify with the following **Channel** option.

Channel: A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

Transmission Rate: By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

802.11 Mode: If all of the wireless devices you want to connect with this router can connect in 802.11g mode, you can improve performance slightly by changing the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.

Super G™ Mode: Super G Turbo Modes must use channel 6 for communication. For Super G with Static Turbo, 802.11 Mode must be set to 802.11g. For proper operation, RTS threshold and Fragmentation Threshold on the Advanced -> Advanced Wireless screen should both be set to their default values.

Super AG without Turbo: Performance enhancing features such as Packet Bursting, FastFrames, and Compression.

Super AG with Static Turbo: This mode is not backwards compatible with non-Turbo (legacy) devices. This mode should only be enabled when all devices on the wireless network are Static Turbo enabled.

Super AG with Dynamic Turbo: This mode is backwards compatible with non-Turbo (legacy) devices. This mode should be enabled when some devices on the wireless network are not Turbo enabled but support other Super G features mentioned above.

WEP: A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.

Example,

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)

WPA-Personal and WPA-Enterprise: Both of these options select some variant of Wi-Fi Protected Access (WPA) -- security standards published by the Wi-Fi Alliance. The **WPA Mode** further refines the variant that the router should employ.

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the router associates only with clients that also support WPA2 security.

Cipher Type: The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the router negotiates the cipher type with the client, and uses AES when available.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

WPA-Personal: This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

Example,

Wireless Networking technology enables ubiquitous communication.

WPA-Enterprise: This option works with a RADIUS Server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through this Gateway. Furthermore, it may be necessary to configure the RADIUS Server to allow this Gateway to authenticate users.

Authentication Timeout: Amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A pass-phrase that must match with the authentication server.

MAC Address Authentication: If this is selected, the user must connect from the same computer whenever logging into the wireless network.

Advanced >>:

Optional Backup RADIUS Server: This option enables configuration of an optional second RADIUS server. A second RADIUS server can be used as backup for the primary RADIUS server. The second RADIUS server is consulted only when the primary server is not available or not responding. The fields **Second RADIUS Server IP Address**, **Second RADIUS Server Port**, **Second RADIUS server Shared Secret**, **Second MAC Address Authentication** provide the corresponding parameters for the second RADIUS Server.

3.2. ADVANCED HELP

3.2.1 Virtual Server

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or game servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and LAN port.

Example,

You are hosting a Web Server on a PC that has LAN IP Address of 192.168.0.50 and your ISP is blocking Port 80.

1. Name the Virtual Server (for example: **Web Server**)
2. Enter the IP Address of the machine on your LAN (for example: **192.168.0.50)**
3. Enter the Private Port as [80]
4. Enter the Public Port as [8888]
5. Select the Protocol - TCP
6. Ensure the schedule is set to **Always**
7. Click **Save** to add the settings to the Virtual Servers List
8. Repeat these steps for each Virtual Server Rule you wish to add. After the list is complete, click **Save Settings** at the top of the page.

   With this Virtual Server entry, all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.0.50.

3.2.1.1 Add/Edit Virtual Server

In this section you can add an entry to the Virtual Servers List below or edit an existing entry.

Enable: Entries in the list can be either active (enabled) or inactive (disabled).

Name: Assign a meaningful name to the virtual server, for example **Web Server**. Several well-known types of virtual server are available from the "Select Virtual Server" list. Selecting one of these entries fills some of the remaining parameters with standard values for that type of server.

IP Address: The IP address of the system on your internal network that will provide the virtual service, for example, **192.168.0.50**.

Protocol: Select the protocol used by the service.

Private Port: The port that will be used on your internal network.

Public Port: The port that will be accessed from the Internet.

Inbound Filter: Select a filter that controls access as needed for this virtual server. If you do not see the filter you need in the list of filters, go to the Advanced -> Inbound Filter screen and create a new filter.

Schedule: Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.

Save: Saves the new or edited virtual server entry in the following list. When finished updating the virtual server entries, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.1.2 Virtual Servers List

The section shows the currently defined virtual servers. A Virtual Server can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Virtual Server" section is activated for editing.

Note: You might have trouble accessing a virtual server using its public identity (WAN-side IP-address of the gateway or its dynamic DNS name) from a machine on the LAN. Your requests may not be looped back or you may be redirected to the "Forbidden" page. This will happen if you have an Access Control Rule configured for this LAN machine.

The requests from the LAN machine will not be looped back if Internet access is blocked at the time of access. To work around this problem, access the LAN machine using its LAN-side identity.
Requests may be redirected to the "Forbidden" page if web access for the LAN machine is restricted by an Access Control Rule. Add the WAN-side identity (WAN-side IP-address of the router or its dynamic DNS name) on the Advanced -> Web Filter screen to work around this problem.

3.2.2 Special Applications

Application Level Gateway (ALG) Configurations:
Here you can enable or disable ALGs. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSec VPN: Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

Windows Messenger: Supports use of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) on LAN computers. The SIP ALG must also be enabled when the Windows Messenger ALG is enabled.

FTP: Allows FTP clients and servers to transfer data across NAT. Refer to the Advanced -> Virtual Server page if you want to host an FTP server.

NetMeeting: Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the Advanced -> Virtual Server page for information on how to set up a virtual server.

SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Wake-On-LAN: This feature enables forwarding of "magic packets" (that is, specially formatted wake-up packets) from the WAN to a LAN computer or other device that is "Wake on LAN" (WOL) capable. The WOL device must be defined as such on the Advanced -> Virtual Server page. The LAN IP address for the virtual server is typically set to the broadcast address 192.168.0.255. The computer on the LAN whose MAC address is contained in the magic packet will be awakened.

AOL: Use this ALG if you are experiencing frequent disconnects from the AOL server due to inactivity.

MMS: Allows Windows Media Player, using MMS protocol, to receive streaming media from the Internet.

L2TP: Allows multiple machines on the LAN to connect to their corporate network using the L2TP protocol.

3.2.2.1 Add/Edit Special Applications Rule

The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Example,

You need to configure your router to allow a software application running on any computer on your network to connect to a web-based server or another user on the Internet.

Name: Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. You can also select from a list of common applications, and the remaining configuration values will be filled in accordingly.

Trigger Port Range: Enter the outgoing port range used by your application. [6500-6700]

Trigger Protocol: Select the outbound protocol used by your application. [Both]

Input Port Range: Enter the port range that you want to open up to Internet traffic. [6000-6200]

Input Protocol: Select the protocol used by the Internet traffic coming back into the router through the opened port range.[Both]

Schedule: Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.

Save: Saves the new or edited Special Applications Rule in the following list. When finished updating the special applications rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent. With this Special Application Rule enabled, the router will open up a range of ports from 6000-6200 for incoming traffic from the Internet, whenever any computer on the internal network opens up an application that sends data to the Internet using a port in the range of 6500-6700.

3.2.2.2 Special Applications Rules List

The section shows the currently defined special applications rules. A special applications rule can be changed by clicking the Edit icon  , or deleted by clicking the Delete icon  . When you click the Edit icon, the item is highlighted, and the "Edit Special Applications Rule" section is activated for editing.

3.2.3 Gaming

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). The Gaming section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats:

Range (50-100)

Individual (80, 68, 888)

Mixed (1020-5000, 689)

3.2.3.1 Add/Edit Game Rule

Here you can add entries to the Game Rules List below, or edit existing entries.

Example,

You are hosting an online game server that is running on a PC with a Private IP Address of 192.168.0.50. This game requires that you open multiple ports (6159-6180, 99) on the router so Internet users can connect.

Enable: Each entry in Game Rules List can be active (enabled) or inactive (disabled).

Name: Give the Gaming Rule a name that is meaningful to you, for example **Game Server**. You can also select from a list of popular games, and many of the remaining configuration values will be filled in accordingly. However, you should check whether the port values have changed since this list was created, and you must fill in the IP address field.

IP Address: Enter the local network IP address of the system hosting the game server, for example, 192.168.0.50.

TCP Ports To Open: Enter the TCP ports to open. [6159-6180, 99]

UDP Ports To Open: Enter the UDP ports to open. [6159-6180, 99]

Inbound Filter: Select a filter that controls access as needed for this game rule. If you do not see the filter you need in the list of filters, go to the Advanced -> Inbound Filter screen and create a new filter.

Schedule: Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.

Save: Saves the new or edited Game Rule in the following list. When finished updating the game rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent. With this Gaming Rule enabled, all TCP and UDP traffic on ports 6159 through 6180 and port 99 is passed through the router and redirected to the Internal Private IP Address of your Game Server at 192.168.0.50.

3.2.3.2 Game Rules List

The section shows the currently defined game rules. A game rule can be changed by clicking the Edit icon  , or deleted by clicking the Delete icon  . When you click the Edit icon, the item is highlighted, and the "Edit Game Rule" section is activated for editing.

3.2.4 QoS

The QoS™ feature helps improve your network gaming performance by prioritizing applications. By default, the QoS settings are disabled.

3.2.4.1 QoS Setup

Enable QoS: This option is disabled by default. Enable it for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Classification: This option is enabled by default so that your router will automatically determine which programs should have network priority.

Dynamic Fragmentation: This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

Automatic Uplink Speed: When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).

Measured Uplink Speed: This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.

Uplink Speed: If Automatic Uplink Speed is disabled, this option allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISPs often specify speed as a downlink/uplink pair; for example, 1.5Mbits/284Kbits.

For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as www.dslreports.com. Note however that sites such as DSL Reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the Measured Uplink Speed or the ISP rated speed.

Connection Type: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as **Detected xDSL or Frame Relay Network**. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the WAN settings, setting this option to **xDSL or Other Frame Relay Network** ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing **xDSL or Other Frame Relay Network** causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL or Other Frame Relay Network: When the connection type is set to **Auto-detect**, the automatically detected connection type is displayed here.

3.2.4.2 Add/Edit QoS Rule

Automatic classification will be adequate for most applications, and specific QoS Rules will not be required. A QoS Rule identifies a specific message flow and assigns a priority to that flow.

Enable: Each entry in QoS Rules List can be active (enabled) or inactive (disabled).

Name: Create a name for the rule that is meaningful to you.

Priority: The priority of the message flow is entered here. 0 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).

Protocol: The protocol used by the messages.

Source IP Range: The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.

Source Port Range: The rule applies to a flow of messages whose LAN-side port number is within the range set here.

Destination IP Range: The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

Destination Port Range: The rule applies to a flow of messages whose WAN-side port number is within the range set here.

Save: Saves the new or edited QoS Rule in the following list. When finished updating the QoS rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.4.3 QoS Rules List

The section shows the currently defined QoS rules. A QoS rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit QoS Rule" section is activated for editing.

3.2.5 Routing

3.2.5.1 Add/Edit Route

Adds a new route to the IP routing table or edits an existing route. **Enable:** Specifies whether the entry will be enabled or disabled. **Destination IP:** The IP address of packets that will take this route.

Netmask: One bits in the mask specify which bits of the IP address must match.

Gateway: Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN. **Interface:** Specifies the interface -- LAN or WAN -- that the IP packet must use to transit out of the router, when this route is used.

Metric: The relative cost of using this route.

Save: Saves the new or edited route in the following list. When finished updating the routing table, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.5.2 Routes List

The section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Routes that you add can be changed by clicking the Edit icon  , or deleted by clicking the Delete icon  . When you click the Edit icon, the item is highlighted, and the "Edit Route" section is activated for editing.

3.2.6 Access Control

The Access Control section allows you to control access in and out of devices on your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications such as peer-to-peer utilities or games.

3.2.6.1 Enable

By default, the Access Control feature is disabled. If you need Access Control, check this option, and you will see the following configuration sections.

Note: When Access Control is disabled, every device on the LAN has unrestricted access to the Internet. However, if you enable Access Control, Internet access is restricted for those devices that have an Access Control Policy configured for them. All other devices have unrestricted access to the Internet.

3.2.6.2 Policy Wizard

The Policy Wizard guides you through the steps of defining each access control policy. A policy is the "Who, What, When, and How" of access control -- whose computer will be affected by the control, what internet addresses are controlled, when will the control be in effect, and how is the control implemented. You can define multiple policies. The Policy Wizard starts when you click the button below and also when you edit an existing policy.

Add Policy: Click this button to start creating a new access control policy.

3.2.6.3 Policy Table

This section shows the currently defined access control policies. A policy can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the Policy Wizard starts and guides you through the process of changing a policy. You can enable or disable specific policies in the list by clicking the **Enable** checkbox.

3.2.7 Web Filter

The Web Filter section is where you add the Web sites to be used for Access Control.

3.2.7.1 Add/Edit Web Site

This is where you can add Web sites to the Allowed Web Site List or change entries in the Allowed Web Site List. The Allowed Web Site List is used for systems that have the Web filter option enabled in Access Control. **Enable** Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default.

Web Site: Enter the URL (address) of the Web Site that you want to allow; for example: **google.com**. Do not enter the **http://** preceding the URL. Enter the most inclusive domain; for example, enter **dlink.com** and access will be permitted to both **www.dlink.com** and **support.dlink.com**.

Note: Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access **my.yahoo.com**, you need to enable access to **yahoo.com**, **yimg.com**, and **doubleclick.net**.

Save: Saves the new or edited Allowed Web Site in the following list. When finished updating the Allowed Web Site List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.7.2 Allowed Web Site List

The section lists the currently allowed web sites. An allowed web site can be changed by clicking the Edit icon  , or deleted by clicking the Delete icon  . When you click the Edit icon, the item is highlighted, and the "Edit Web Site" section is activated for editing.

3.2.8 MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). A MAC address is a unique ID assigned by the manufacturer of the network adapter.

3.2.8.1 Enable MAC Address Filter

When this is enabled, computers are granted or denied network access depending on the mode of the filter.

Note: Misconfiguration of this feature can prevent any machine from accessing the network. In such a situation, you can regain access by activating the factory defaults button on the router itself.

3.2.8.2 Filter Settings

Mode: When "only allow listed machines" is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When "only deny listed machines" is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

3.2.8.3 Add/Edit MAC Address

In this section, you can add entries to the MAC Address List below, or edit existing entries.

Enable: MAC address entries can be activated or deactivated with this checkbox.

MAC Address: Enter the MAC address of the desired computer or connect to the router from the desired computer and click the **Copy Your PC's MAC Address** button.

Save: Saves the new or edited MAC Address entry in the following list. When finished updating the MAC Address List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.8.4 MAC Address List

The section lists the current MAC Address filters. A MAC Address entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit MAC Address" section is activated for editing.

3.2.9 Firewall

3.2.9.1 Enable SPI

SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyberattacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol.

3.2.9.2 Enable DMZ

DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

3.2.9.3 DMZ IP Address

Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address automatically using DHCP, then you may want to make a static reservation on the Basic -> DHCP page so that the IP address of the DMZ machine does not change.

3.2.10 Inbound Filter

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on IP Address.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter Wireless Local Loop using internal 3G / 3.5 G cellular modem might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.

3.2.10.1 Add/Edit Inbound Filter Rule

Here you can add entries to the Inbound Filter Rules List below, or edit existing entries.

Name: Enter a name for the rule that is meaningful to you.

Action: The rule can either Allow or Deny messages.

Source IP Range: Define the ranges of Internet addresses this rule applies to. For a single IP address, enter the same address in both the **Start** and **End** boxes. Up to eight ranges can be entered. The **Enable** checkbox allows you to turn on or off specific entries in the list of ranges.

Save: Saves the new or edited Inbound Filter Rule in the following list. When finished updating the Inbound Filter Rules List, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.10.2 Inbound Filter Rules List

The section lists the current Inbound Filter Rules. An Inbound Filter Rule can be changed by clicking the Edit icon  , or deleted by clicking the Delete icon  . When you click the Edit icon, the item is highlighted, and the "Edit Inbound Filter Rule" section is activated for editing.

In addition to the filters listed here, two predefined filters are available wherever inbound filters can be applied:

Allow All: Permit any WAN user to access the related capability.

Deny All: Prevent all WAN users from accessing the related capability. (LAN users are not affected by Inbound Filter Rules.)

3.2.11 Advanced Wireless

The description of related parameter for the Advanced Wireless function is as follows:

Fragmentation Threshold: This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.

RTS Threshold: This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Beacon Period: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

DTIM Interval: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

802.11d Enable: Enables 802.11d operation. 802.11d is a wireless specification for operation in additional regulatory domains. This supplement to the 802.11 specifications defines the physical layer requirements (channelization, hopping patterns, new values for current MIB attributes, and other requirements to extend the operation of 802.11 WLANs to new regulatory domains (countries). The current 802.11 standard defines operation in only a few regulatory domains (countries). This supplement adds the requirements and definitions necessary to allow 802.11 WLAN equipment to operate in markets not served by the current standard. Enable this option if you are operating in one of these "additional regulatory domains".

Transmit Power: Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

WDS Enable: When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP.

WDS AP MAC Address: Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.

3.2.12 Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

3.2.12.1 Add/Edit Schedule Rule

In this section you can add entries to the Schedule Rules List below or edit existing entries.

Name: Give the schedule a name that is meaningful to you, such as "Weekday rule".

Day(s): Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

All Day - 24 hrs: Select this option if you want this schedule in effect all day for the selected day(s).

Start Time: If you don't use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are normally triggered only by the start time.

End Time: The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not normally used for email events.

Save: Saves the new or edited Schedule Rule in the following list. When finished updating the Schedule Rules, you must still click the **Save Settings** button at the top of the page to make the changes effective and permanent.

3.2.12.2 Schedule Rules List

The section shows the currently defined Schedule Rules. A Schedule Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit Schedule Rule" section is activated for editing.

3.2.13 Ping WAN

Ping WAN function provides you with an option to check the WAN connection is valid or not, if not, the router will switch from Ethernet to the modem Dialup, or from the modem Dialup(Always on mode) to Ethernet.

After Ping WAN is enabled, it does not doing the PING all the time, it only happens after finding that there are data packets going out(to WAN) but none is coming in(form WAN).

Note 1: When modem Dialup is activated, Ping WAN will take place only for "Always on mode", not for "On demand mode".

Note 2: When modem Dialup(Always on mode) is activated and "WAN LInk Timeout = 0", after Ping WAN confirms that WAN connection is not ok, the modem Dialup will be disconnected and tried to connect again, it will not switch to Ethernet.

Note 3: The Ping WAN packet is transmitted from current activated WAN interface to the assigned IP, such as from Ethernet or the modem Dialup, it can not transmit from both Ethernet and the modem Dialup simultaneously, so when the modem Dialup is activated, only after failure of Ping WAN (Always on mode), idle timeout or max connection timeout(On demand mode), the router will switch from the modem Dialup to Ethernet.

The description of related parameter for the Ping WAN function is as follows:

Enable Ping WAN: Enable the function of Ping WAN.

Start to Ping when: Set up the circumstance that Ping will start to activate. Two options are offered to allow you choosing the Ping mode. The settings are:

- **Always Ping:** The router will always do the ping.
- **After tx to WAN, find no response:** The router will do the ping if no response is found from Ethernet WAN.

Ping repetition time(time between 2 Ping): The time interval of sending the Ping packet.

Max Allowed Successive Lost Ping: The maximum times that the Kx EasyBackUp Pro allows to receive no response from the successive Ping. The WAN connection will be transferred from Ethernet_WAN into the modem Dialup in case it exceeds this limit.

Ping WAN IP Address: The IP address is used for the ping.

Max Dialup (on demand) connection time: The maximum time duration of the dial up (on demand) connection. The connection of the modem Dialup will be disconnected and have the Ethernet take over the WAN connection in case it exceeds this limit.

3.3. TOOLS HELP

3.3.1 Admin

The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.

Admin Password: Enter a password for the user "admin", who will have full access to the web-based management interface.

User Password: Enter a password for the user "user", who will have read-only access to the web-based management interface.

Gateway Name: The name of the router can be changed here.

Enable Remote Management: Enabling Remote Management allows you to manage the router from anywhere on the Internet. Disabling Remote Management allows you to manage the router only from computers on your LAN.

Remote Admin Port: The port that you will use to address the management interface from the Internet. For example, if you specify port 1080 here, then, to access the router from the Internet, you would use a URL of the form: **http://my.domain.com:1080/**.

Remote Admin Inbound Filter: Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the Advanced -> Inbound Filter screen and create a new filter.

Admin Idle Timeout: The amount of time before the administration session (either remote or local) is closed when there is no activity.

Enable UPnP: Enable the function of UPnP (Universal Plug and Play).

3.3.2 Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the router's internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight saving can also be configured to automatically adjust the time when needed.

3.3.2.1 Time Configuration

Time Zone: Select your local time zone from pull down menu.

Enable Daylight Saving: Check this option if your location observes daylight saving time.

Daylight Saving Offset: Select the time offset, if your location observes daylight saving time.

DST Start and DST End: Select the starting and ending times for the change to and from daylight saving time. For example, suppose for DST Start you select Month="Oct", Week="3rd", Day="Sun" and Time="2am". This is the same as saying: "Daylight saving starts on the third Sunday of October at 2:00 AM."

3.3.2.2 Automatic Time Configuration

Enable NTP Server: Select this option if you want the router's clock synchronized to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.

NTP Server Used: Select a Network Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

3.3.2.3 Set the Date and Time Manually

If you do not have the NTP Server option in effect, you can either manually set the time for your router here, or you can click the **Copy Your Computer's Time Settings** button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

Note: If the router loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the router, or you must enable the NTP Server option.

3.3.3 Syslog

This section allows you to archive your log files to a Syslog Server.

3.3.3.1 Enable Logging to Syslog Server

Enable this option if you have a syslog server currently running on the LAN and wish to send log messages to it. Enabling this option causes the following parameter to be displayed.

3.3.3.2 Syslog Server IP Address

Enter the LAN IP address of the Syslog Server.

3.3.4 Email

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

3.3.4.1 Enable

Enable Email Notification: When this option is enabled, router activity logs or firmware upgrade notifications can be emailed to a designated email address, and the following parameters are displayed.

3.3.4.2 Email Settings

From Email Address: This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email Address: Enter the email address where you want the email sent.

SMTP Server Address: Enter the SMTP server address for sending email.

Enable Authentication: If your SMTP server requires authentication, select this option.

Account Name: Enter your account for sending email.

Password: Enter the password associated with the account.

Verify Password: Re-type the password associated with the account.

3.3.4.3 Email Log When Full or on Schedule

On Log Full: Select this option if you want logs to be sent by email when the log is full.

Schedule: Select this option if you want logs to be sent by email according to a schedule.

Select Schedule: If you selected the Schedule option, select one of the defined schedule rules. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.

Note: Normally email is sent at the start time defined for a schedule, and the schedule end time is not used. However, rebooting the router during the schedule period will cause an additional email to be sent.

3.3.5 System

This section allows you to reboot the device, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

3.3.5.1 Reboot the Device

This restarts the router. Useful for restarting when you are not near the device.

3.3.5.2 Restore all Settings to the Factory Defaults

This option restores all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost. If you want to save your router configuration settings, you can do so from the Tools -> Admin page.

3.3.5.3 Restore Configuration from File

Use this option to load previously saved router configuration settings.

3.3.5.4 Save Configuration

This option allows you to save the router's configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

3.3.6 Firmware

The Firmware Upgrade section can be used to update your router to the latest firmware code to improve functionality and performance.

To upgrade the firmware, follow these steps:

1. Click the **Browse** button to locate the KORTEX PSI upgrade file on your computer.
2. Once you have found the file to be used, click the **Upload** button below to start the firmware upgrade process. This can take a minute or more.
3. Wait for the router to reboot. This will take another minute or more.
4. Confirm updated firmware revision on status page.

3.3.6.1 Firmware Information

Here are displayed the version numbers of the firmware currently installed in your router and the most recent upgrade that is available.

3.3.6.2 Firmware Upgrade

Note: Some firmware upgrades reset the router's configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools -> Admin screen.

Upload: Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the router.

3.3.7 Dynamic DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, your friends can enter your domain name to connect to your server, no matter what your IP address is.

3.3.7.1 Enable Dynamic DNS

Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following parameters are displayed when the option is enabled.

Server Address: Select a dynamic DNS service provider from the pull-down list.

Host Name: Enter your host name.

Username or Key: Enter the username or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Password or Key: Enter the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Verify Password or Key: Re-type the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Timeout: The time between periodic updates to the Dynamic DNS if your dynamic IP address has not changed. The timeout period is entered in hours.

Note 1: If a dynamic DNS update fails for any reason (for example, when incorrect parameters are entered), the router automatically disables the Dynamic DNS feature and records the failure in the log.

Note 2: After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example **http://www.mydomain.info**) and the router will attempt to forward the request to port 80 on your LAN. If, however, you do this from a LAN-side computer and there is no virtual server defined for port 80, the router will return the router's configuration home page. Refer to the Advanced -> Virtual Server configuration page to set up a virtual server.

3.4. STATUS HELP

3.4.1 Device Info

All of your Internet and network connection details such as the internal time of the router, firmware version, date of the firmware upgrade, plug or unplug USB modem as well as the information about WAN, LAN and wireless LAN are displayed on this Device Info page.

Note: Some browsers have limitations that make it impossible to update the WAN status display when the status changes. Some browsers require that you refresh the display to obtain updated status. Some browsers report an error condition when trying to obtain WAN status.

Depending on the type of WAN connection, you can take one of the following sets of actions:

3.4.1.1 DHCP Connection

Clicking the **DHCP Release** button unassigns the router's IP address. The router will not respond to IP messages from the WAN side until you click the **DHCP Renew** button or power-up the router again. Clicking the **DHCP Renew** button causes the router to request a new IP address from the ISP's server.

3.4.1.2 PPPoE, PPTP, L2TP Connection

Depending on whether the WAN connection is currently established, you can click either the **Connect** to attempt to establish the WAN connection or the **Disconnect** to break the WAN connection.

3.4.1.3 BigPond Connection

Depending on whether you are currently logged in to BigPond, you can click either the **BigPond Login** to attempt to establish the WAN connection or the **BigPond Logout** to break the WAN connection.

3.4.1.4 LAN Computers

This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your router. The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to "Automatically obtain an address") supplies a Host Name then that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show, however its host name will not.

3.4.2 Wireless

The wireless section allows you to view the wireless clients that are connected to your wireless router.

MAC Address: The Ethernet ID (MAC address) of the wireless client.

IP Address: The LAN-side IP address of the client.

Mode: The transmission standard being used by the client. Values are 11a, 11b, or 11g for 802.11a, 802.11b, or 802.11g respectively.

Rate: The actual transmission rate of the client in megabits per second.

Signal: This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

3.4.3 Routing

The routing section displays all of the routing details configured for your router.

A value of 0.0.0.0 for gateway means there is no next hop, and the IP address is directly connected to the router on the interface specified: LAN or WAN. A value of 0.0.0.0 in both the destination IP and netmask means that this is the default route.

3.4.4 Logs

The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

What to View:

Select the kinds of events that you want to view.

- Firewall and Security
- System
- Router Status

View Levels:

Select the level of events that you want to view.

- Critical
- Warning
- Informational

Apply Log Settings Now: Click this button after changing Log Options to make them effective and permanent.

Refresh: Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear: Clicking this button erases all log entries.

Email Now: If you provided email information with the Tools -> Email screen, clicking the **Email Now** button sends the router log to the configured email address.

Save Log: Select this option to save the router log to a file on you computer.

3.4.5 Statistics

The Statistics page displays all of the LAN and WAN packet transmit and receive statistics.

Sent: The number of packets sent from the router.

Received: The number of packets received by the router.

TX Packets Dropped: The number of packets that were dropped while being sent, due to errors, collisions, or router resource limitations.

RX Packets Dropped: The number of packets that were dropped while being received, due to errors, collisions, or router resource limitations.

Collisions: The number of packets that were dropped due to Ethernet collisions (two or more devices attempting to use an Ethernet circuit at the same time).

Errors: The number of transmission failures that cause loss of a packet.

3.4.6 Active Sessions

The Active Sessions page displays full details of active sessions through your router. A session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

Internal: The IP address and port number of the LAN-side application.

Protocol: The communications protocol used for the conversation.

External: The IP address and port number of the WAN-side application.

NAT: The port number of the LAN-side application as viewed by the WAN-side application.

Priority: The preference given to outbound packets of this conversation by the QoS logic. Smaller numbers represent higher priority.

State: State for sessions that use the TCP protocol.

- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- CW: Close Wait -- the server system has requested that the connection be stopped.
- TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
- LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
- CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Dir: The direction of initiation of the conversation:

Egress: Initiated from LAN to WAN.

Ingress: Initiated from WAN to LAN.

Time Out: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

120 seconds: UDP connections.

20 seconds: Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

120 seconds: Opening or closing TCP connections.

7800 seconds: Established TCP connections.