Product Guide

for

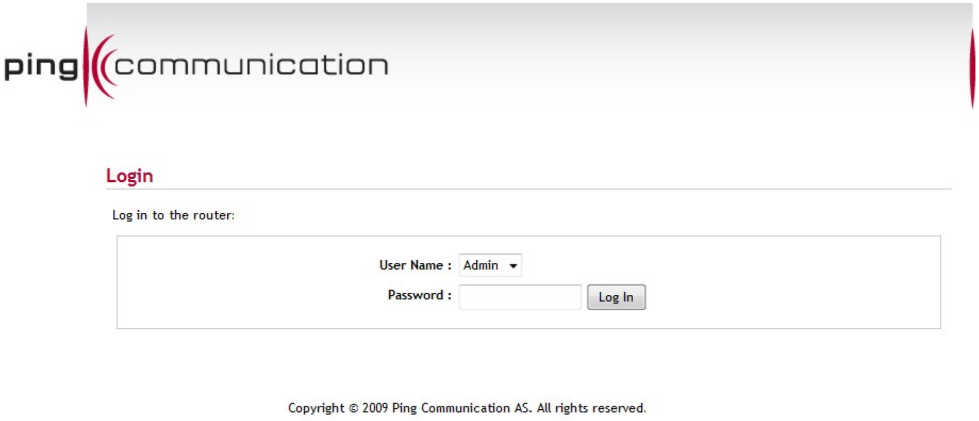
Residential Gateway

RGW208EN

Version: 17th of March 2010

1 Getting started

The Configuration Interface can be accessed from your Web browser. Open up your Web browser and type **http://192.168.176.1** in the address field and press **Enter**. The Configuration Interface login screen will appear. By default, there is no password. Click on the **Log In** button to access the Configuration main screen.



Login

Log in to the router:

User Name : Admin

Password :

Copyright © 2009 Ping Communication AS. All rights reserved.

1.1 Troubleshooting

Make sure your computer is connected to LAN port on the device. Then open a command window and type ipconfig (Windows) or ifconfig (Linux/Mac). You should then be able to read the IP address of the Default Gateway of the LAN connection on your computer (assuming you only have one LAN network interface). If this IP address do not appear, the computer is not connected to the device. If it does appear, use that address instead of 192.168.176.1 (assuming it differ).

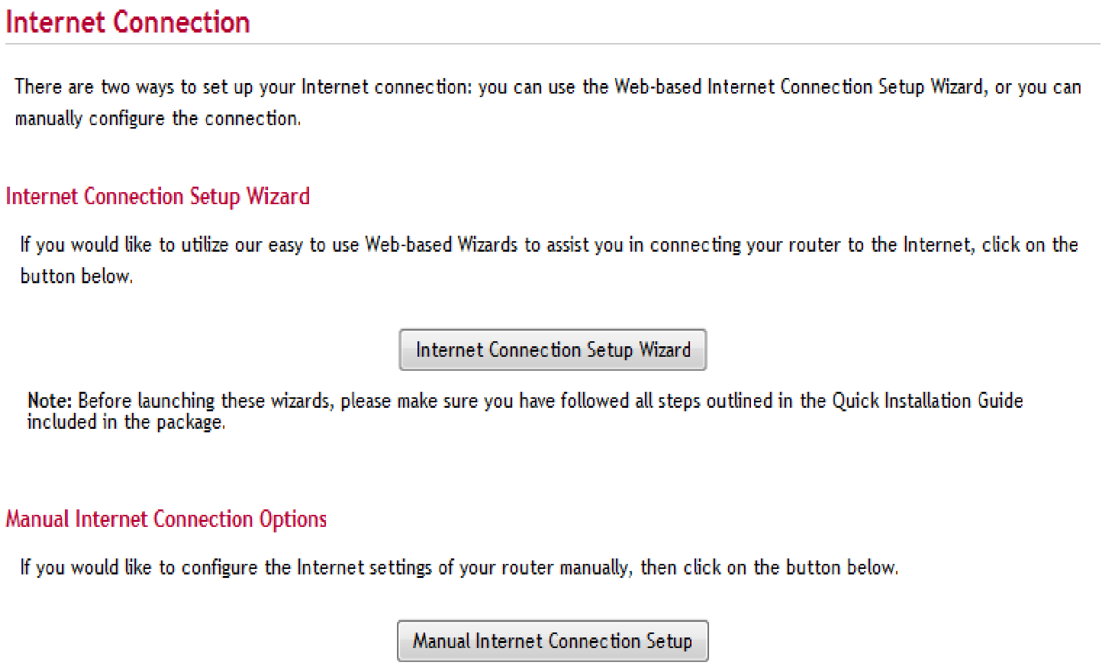
1.2 How to read the manual

This manual will go through all menus in an orderly fashion. Chapter 2 starts with the first left menu item (Basic) and the sub chapters covers the upper menu. Then if you look up a certain chapter in this manual you can always know that the main chapter heading denotes the left menu choice and the sub chapter heading denotes the upper menu choice.

2 Basic menu

2.1 Internet

The Internet Connection screen contains the Internet Connection Wizard that assists you in configuring the device to allow it to connect to the Internet, as well as the Manual Internet Connection Options screen in which you can set up your Internet connection manually.



Internet Connection

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection.

Internet Connection Setup Wizard

If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your router to the Internet, click on the button below.

Note: Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Manual Internet Connection Options

If you would like to configure the Internet settings of your router manually, then click on the button below.

2.1.1 Internet Connection Setup Wizard

The Internet Connection Setup Wizard will assist you with connecting the device to the Internet. The step by step guide will prompt you for the necessary information to get you connected. The Internet Connection Setup Wizard guides you through the following basic router setup steps:

To begin, click on the **Launch Internet Connection Setup Wizard** button.
The **Welcome** screen appears, click Next to continue.

Note: The device is intelligent, and will in some cases manage to connect to the Internet automatically. In this case the Wizard will report that a connection has been established successfully, but will still let the user proceed through steps 1 and 2.

Step 1: Set Your Password prompts you to enter a password for the Web-based configuration interface. You can enter the password in the Verify Password prompt.

Step 2: Select Your Time Zone prompts you to select your time zone from the pull-down menu.

Step 3: Configure Your Internet Connection. At this stage we assume that the device is not connected to the internet, otherwise the wizard would have skipped this step. Still, there are possibilities if the connection type of your Internet Service Provider (ISP) is known (or can be established).

If your ISP is listed in the drop-down menu (and you choose it) then the connection type is chosen for you. Otherwise, specify the connection type manually.

Depending upon your Internet Service Provider or the type of connection you selected in the previous step, one of five screens will appear. If you are unsure of any of the information, please contact your Internet Service Provider (ISP) for details.

- **DHCP Connection (Dynamic IP Address).** DHCP is a much used connection type. It should usually not require any setup on your behalf. However, at this point we have an "unusual" situation (since you're reading this). If you have put your device behind a cable modem[1] (a device which is connected to a coax cable) there are some things you could try:
  - Try to restart that modem. Cancel this setup and try again.
  - If you previously had equipment (like your PC) connected to the cable modem and actually had a working internet connection, you can try to clone/copy the MAC address of that equipment into this device. By pressing the **Clone Your PC's MAC Address** you will copy the MAC address of the PC you're connecting to this device. If, let's say, you had a router connected behind the cable modem, you could read MAC address (usually printed underneath the router) and enter it manually. You can always reverse this step later by entering the MAC address printed on this device (the WAN MAC).

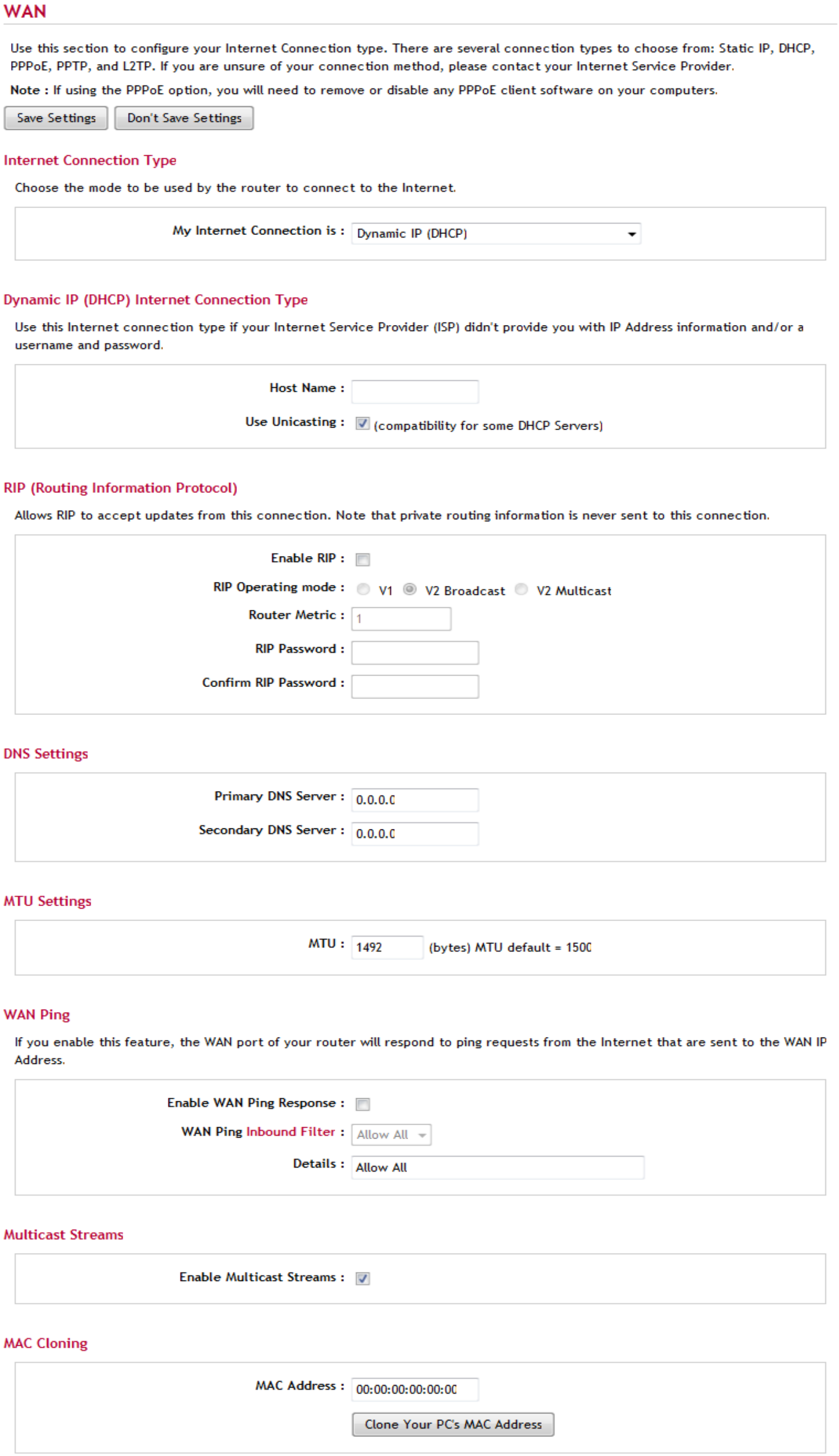
  A last resort may be to add a hostname if that is provided by the ISP. This is not very common.
  The settings for DNS could be left untouched, unless you have been able to retrieve this information from the ISP. Usually (again) this information is automatically populated when connecting on DHCP.
- **Set Username and Password Connection (PPPoE)** prompts you to enter your Username and Password. This information must be provided by the ISP (typically in a welcome letter). You must also verify the Password. If your ISP requires a Service Name entry, please enter it here. The default setup is to get the IP address dynamically. In some cases the ISP has chosen to give you a static IP. You can then choose the static radio button and enter the IP address.
- **Set Username and Password Connection (PPTP)** prompts you to enter your PPTP IP Address, PPTP Subnet Mask, PPTP Gateway IP Address, PPTP Server IP Address, Username, and Password. You must also verify the Password. This information must be provided by the ISP (typically in a welcome letter).

[1] A cable modem or any device which is not connecting on the IP layer. That excludes all DSL modems.

- **Set Username and Password Connection (L2TP)** prompts you to enter your L2TP IP Address, L2TP Subnet Mask, L2TP Gateway IP Address, L2TP Server IP Address, Username and Password. You must also verify the Password. This information must be provided by the ISP (typically in a welcome letter).
- **Set Static IP Address Connection** prompts you to enter the IP address, Subnet Mask, Gateway Address, Primary and Secondary DNS address information. This information must be provided by the ISP (typically in a welcome letter).
- **Setup Complete** will appear after all of the settings have been entered. Click **Connect** to save your settings and reboot the router.

2.1.2 Manual setup

2.1.2.1 Modes



WAN

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Internet Connection Type

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Dynamic IP (DHCP)

Dynamic IP (DHCP) Internet Connection Type

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Use Unicasting : ☑ (compatibility for some DHCP Servers)

RIP (Routing Information Protocol)

Allows RIP to accept updates from this connection. Note that private routing information is never sent to this connection.

Enable RIP : □

RIP Operating mode : ○ V1 ● V2 Broadcast ○ V2 Multicast

Router Metric : 1

RIP Password :

Confirm RIP Password :

DNS Settings

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

MTU Settings

MTU : 1492 (bytes) MTU default = 1500

WAN Ping

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Response : □

WAN Ping Inbound Filter : Allow All

Details : Allow All

Multicast Streams

Enable Multicast Streams : ☑

MAC Cloning

MAC Address : 00:00:00:00:00:00

There are five connection modes to choose from as shown below. If you are unsure of your connection settings, contact your Internet Service Provider (ISP) and you can enter the necessary information on the Quick Installation Guide (QIG) or print this page and write the settings for future reference.

Primary DNS Server: ______.______.______.______
Secondary DNS Server: ______.______.______.______

Static: 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.

IP Address: ______.______.______.______
Subnet Mask: ______.______.______.______
Def. Gateway: ______.______.______.______

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

Host Name:______________________

PPPoE: A method of connection that requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.
Username: ____________________
Password: ____________________
Service Name (Optional): ____________________

PPTP: A method of connection that requires you to enter information provided by your Internet Service Provider to gain access to the Internet.

PPTP IP Address: ______.______.______.______
PPTP Subnet Mask: ______.______.______.______
PPTP Gateway IP Address: ______.______.______.______
PPTP Server IP Address: ______.______.______.______
Username: ________________________
Password: ________________________

L2TP: A method of connection that requires you to enter information provided by your Internet Service Provider to gain access to the Internet.
L2TP IP Address: ______.______.______.______
L2TP Subnet Mask: ______.______.______.______
L2TP Gateway IP Address: ______.______.______.______
L2TP Server IP Address: ______.______.______.______
Username: ________________________
Password: ________________________

All five modes have some common configuration options. The Primary and Secondary DNS Server settings are required for Static configurations and optional for DHCP and PPPoE configurations. The Advanced options on the following page can be modified for any of the five connection modes. You should be able to get the **Primary DNS**

and Secondary DNS Servers settings from your router configuration settings, ISP, or your network administrator. Only the primary DNS server address is required, though it is best to have both the primary and secondary addresses.

2.1.2.2 Advanced

The Advanced options apply to all WAN modes.

Use the Default MTU: This option is enabled by default allowing the router to select the typical MTU settings for the selected WAN interface. If this option is unchecked, the router will use the value assigned in the MTU field.

MTU: The MTU (Maximum Transmission Unit) 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.

MAC Cloning Enabled: Some ISP's may check your computer's MAC address. Each networking device has it's own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer with this particular MAC address. The device has a different MAC address than the computer that initially connected to the ISP. To resolve this problem, enable this option.

MAC Address: When MAC Cloning is enabled, you can enter in a MAC address manually in this field or click the Clone Your Computer's MAC Address button.

Clone Your PC's MAC Address: When this button is clicked, the WAN port will use the MAC Address of the network adapter in the computer that you are using to access the router.

Multicast Streams The router uses the IGMP protocol to support efficient multicasting -- transmission of identical content, such as multimedia, from a source to a number of recipients. This option must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling this option.

RIP (Routing Information Protocol) RIP enables the router to share routing information with other routers and hosts on the LAN. Enable RIP if the LAN has multiple routers or if the LAN has other hosts that listen for RIP messages, such as auto-IP devices or the Windows XP RIP Listener Service. This is (almost) never used in private homes, only in large corporate networks.

- RIP Operating mode. This router supports both version 2 and version 1 of the RIP specification.

  V1. Use if none of the routers supports Version 2.

V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1.

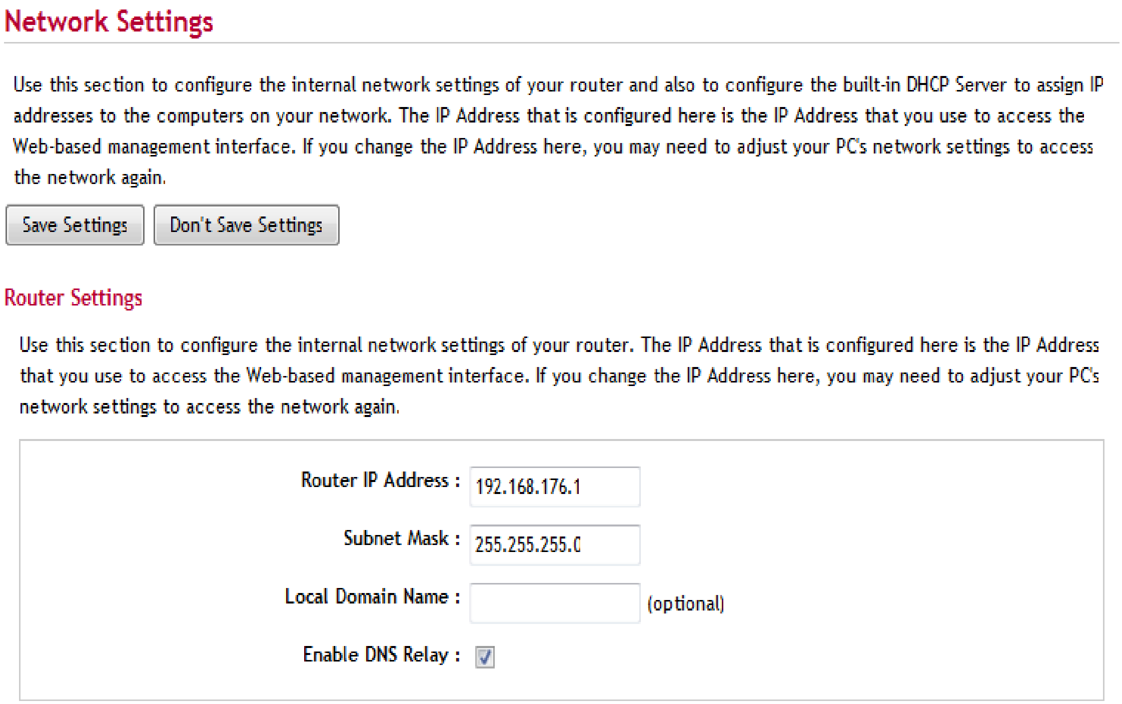
V2 Multicast. Use if this is the only router on the LAN or if all the routers support Version 2.

- Router Metric. The additional cost of routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.
- RIP Password. This router supports the use of clear-text passwords in RIP version 2 messages. Only routers with the same RIP password can share routes via RIP. RIP passwords serve more as a mechanism to limit route sharing rather than as a security mechanism. You might use RIP passwords, for example, to prevent routes from one subnet from being seen by a router on another subnet that has conflicting IP addresses. Enter the password twice for verification. Leave both password fields empty if RIP passwords are not used.

2.2 Network Settings

Your internal network 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.

2.2.1 Router Settings



Network Settings

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router Settings

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :	192.168.176.1
Subnet Mask :	255.255.255.0
Local Domain Name :	(optional)
Enable DNS Relay :	☑

Router IP Address: The IP address of the router on the local area network. The local network settings are based on the address assigned here.

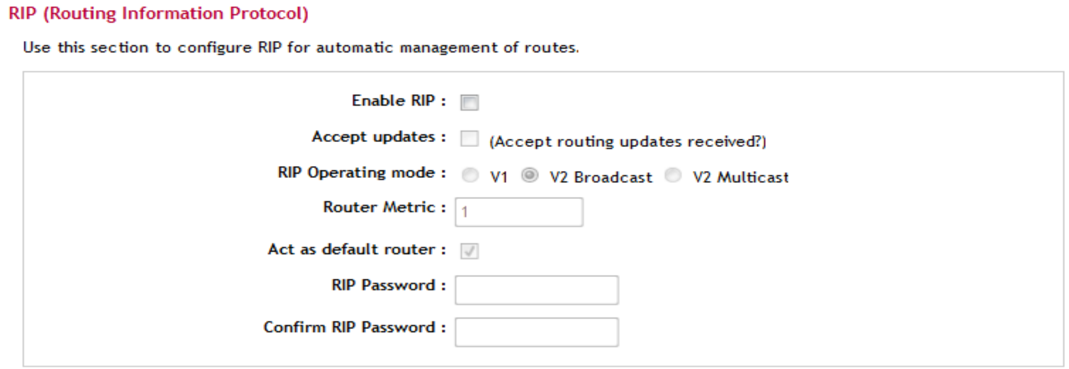
Troubleshoot: In some rare cases, this IP-address will conflict with the address (or rather address range) of the WAN side. This situation occurs if a similar device like this (e.g. a router) is placed in front of this device, causing the same IP-subnet on both WAN and LAN on this device. In that case: Change to 192.168.100.1 and also change the DHCP IP-range (a field further down) accordingly: exchange 176 with 100.

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

Local Domain Name: This entry is optional. Enter a domain name for the local network. Your LAN computer will assume this domain name when it gets an address from the router's built in DHCP server. So, for example, if you enter mynetwork.net here, and you have a LAN side laptop with a name of “chris”, that laptop will be known as chris.mynetwork.net. Note, however, the entered domain name can be overridden by the one obtained from the router's upstream DHCP server.

Enable 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.

2.2.2 RIP (Routing Information Protocol)



RIP (Routing Information Protocol)

Use this section to configure RIP for automatic management of routes.

Enable RIP :	□
Accept updates :	□ (Accept routing updates received?)
RIP Operating mode :	○ V1 ● V2 Broadcast ○ V2 Multicast
Router Metric :	1
Act as default router :	☑
RIP Password :	
Confirm RIP Password :	

Enable RIP: Check this options to enable the *Routing Information Protocol.* This protocol is used with multiple routers to broadcast routing information. Enable RIP if required by the ISP, if the LAN has multiple routers, or if the LAN has auto-IP devices.

Accept updates (from WAN): Enable this option if required by your ISP. Otherwise, for security reasons, leave disabled.

RIP Operating Mode: Select which version of the *Routing Information Protocol* to run. Use **V1** if none of the other routers support V2. Use **V2 Broadcast** if some, but not all, of the other routers are capable of V2. Use **V2 Multicast** if this is the only router on the LAN or if all the routers support Version 2.

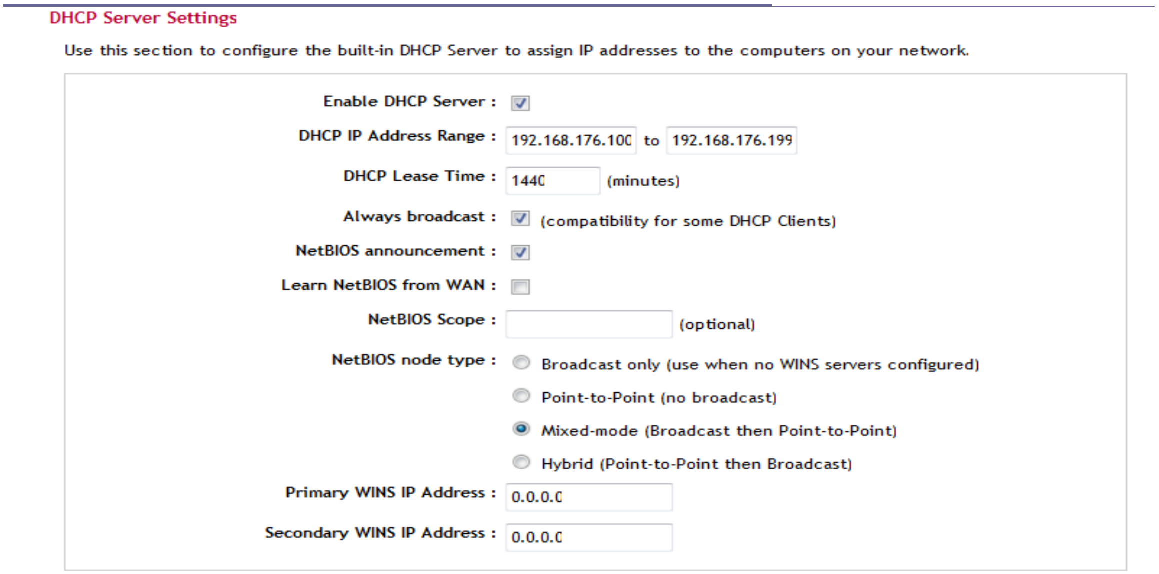
Router Metric: The additional cost of routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.

Act as default router: Make this router the preferred destination for packets that are not otherwise destined.

RIP Password: RIP Version 2 supports the use of a password to limit access to routers through the RIP protocol. If the ISP or other LAN router requires a RIP password, enter the password here.

2.2.3 DHCP Server Settings

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.



DHCP Server Settings

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server : ☑

DHCP IP Address Range : 192.168.176.10C to 192.168.176.199

DHCP Lease Time : 144C (minutes)

Always broadcast : ☑ (compatibility for some DHCP Clients)

NetBIOS announcement : ☑

Learn NetBIOS from WAN : □

NetBIOS Scope : (optional)

NetBIOS node type :
○ Broadcast only (use when no WINS servers configured)
○ Point-to-Point (no broadcast)
● Mixed-mode (Broadcast then Point-to-Point)
○ Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address : 0.0.0.C

Secondary WINS IP Address : 0.0.0.C

Enable DHCP Server: Once your device is properly configured and this option is enabled, the DHCP Server function will assign your network devices the necessary information to connect to the LAN and Internet. This eliminates the need to manually configure each device on your network with IP settings. When you set the DHCP server to *Enabled*, the following options appear.
Note: The devices on your network must have TCP/IP bound to the Ethernet connection with the "DHCP" or "Obtain an IP address automatically" option enabled.

DHCP IP Address Range: This option defines the range of addresses available for the Router to assign to your internal network. If you have any devices using static IP addresses, be sure the addresses do not fall within the range defined here. A Static IP address is one that is entered in manually on the device. Also, the range must be specified with the same 192.168.176–prefix as the Router IP Address.

Example: Your device uses an IP address of 192.168.176.1. You've assigned a computer designated as a Web server with a static IP address of 192.168.176.3. You've assigned another computer designated as an FTP server with a static IP address of 192.168.176.4. The starting IP address for your DHCP server needs to be 192.168.176.5 or above.

DHCP Lease Time: The amount of time 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 expires then a new lease is established. If the lease expires and the address is no longer needed, then 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.

NetBIOS Announcement: Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allow LAN hosts to discover all other computers within the network, e.g. within Network Neighborhood. Setting NetBIOS Advertisement to *Enabled* will reveal the following options.

Learn NetBIOS information from WAN: If NetBIOS advertisement is switched on, switching this setting on causes WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

NetBIOS Scope: This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

NetBIOS Registration mode: Indicates how network hosts are to perform NetBIOS name registration and discovery.

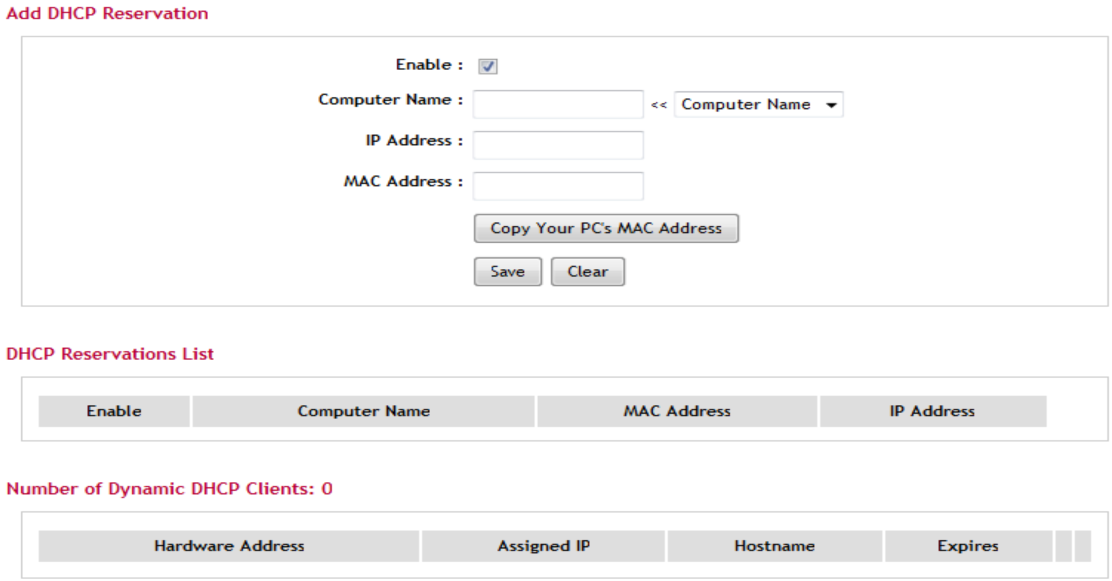
- **Broadcast Only:** Indicates usage of local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.
- **Point-to-point:** Indicates usage of WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server.
- **Mixed (default):** Indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favors broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN.
- **Hybrid:** Indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers.

Primary WINS Server IP Address: Configure the IP address of the preferred WINS server. WINS Servers store information regarding network hosts, allowing hosts to 'register' themselves as well as discover other available hosts, e.g. for use in Network Neighborhood. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

Secondary WINS Server IP Address: Configure the IP address of the backup WINS server, if any. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

2.2.4 Add 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 (like your computer) has a static IP address except that the device must still request an IP address from this device. This device will provide the other device (ex: your computer) 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.



Add DHCP Reservation

Enable : ☑

Computer Name : << Computer Name

IP Address :

MAC Address :

DHCP Reservations List

Enable	Computer Name	MAC Address	IP Address

Number of Dynamic DHCP Clients: 0

Hardware Address	Assigned IP	Hostname	Expires

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. Example: Game Server.

IP Address: The LAN address that you want to reserve. The IP address must have the same "prefix" as the Router IP Address (usually 192.168.176).

MAC Address: The MAC address of the device that will receive the reserved IP. 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 RGW208EN from the computer and click the Copy Your PC's MAC Address button to enter the MAC address.
Note: If you replace the Ethernet adapter in a computer that is using a DHCP reservation, you will need to Copy the PC's MAC address again, because every Ethernet adapter has a unique MAC address. The same goes for any network device. If you replace a network device such as a print server, you will need to input the MAC address of the new print server into the Static DHCP configuration.

2.2.5 DHCP Reservations list

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

2.2.6 Number of Dynamic DHCP Clients

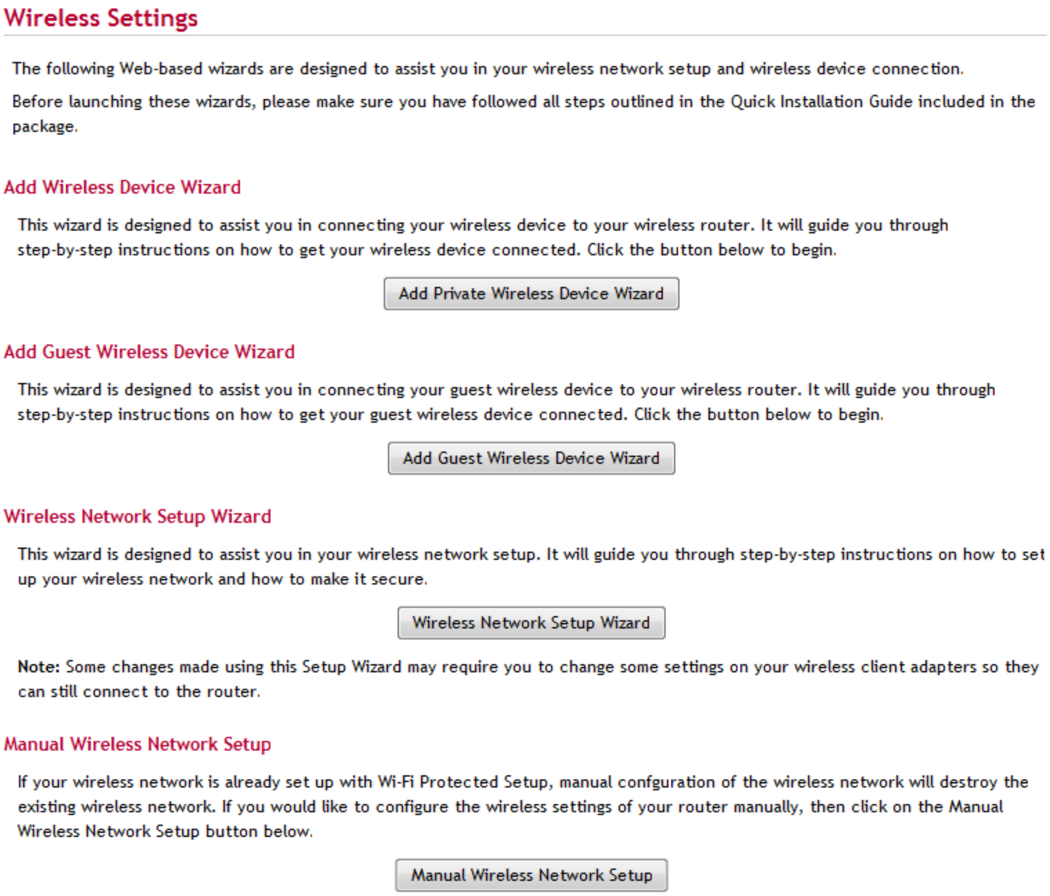
In this section, you can see what LAN devices are currently leasing IP addresses. The DHCP Client table displays the number of clients that are receiving an IP address from the router. The computer name, MAC address, and IP address assigned to each computer are displayed here as well.

Revoke: Pressing **Revoke** cancels the lease of IP for a specific LAN device, freeing this entry in the lease table. This feature is useful for freeing up addresses when the client table is full or nearly full. Make sure you only revoke addresses from devices that are no longer needed and/ or present on the network.

Reserve: The **Reserve** option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

2.3 Wireless settings

The wizards cannot be used unless have set up a wireless network. Therefore we start with Manual Wireless Network Setup



Wireless Settings

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Add Wireless Device Wizard

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

Add Guest Wireless Device Wizard

This wizard is designed to assist you in connecting your guest wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your guest wireless device connected. Click the button below to begin.

Wireless Network Setup Wizard

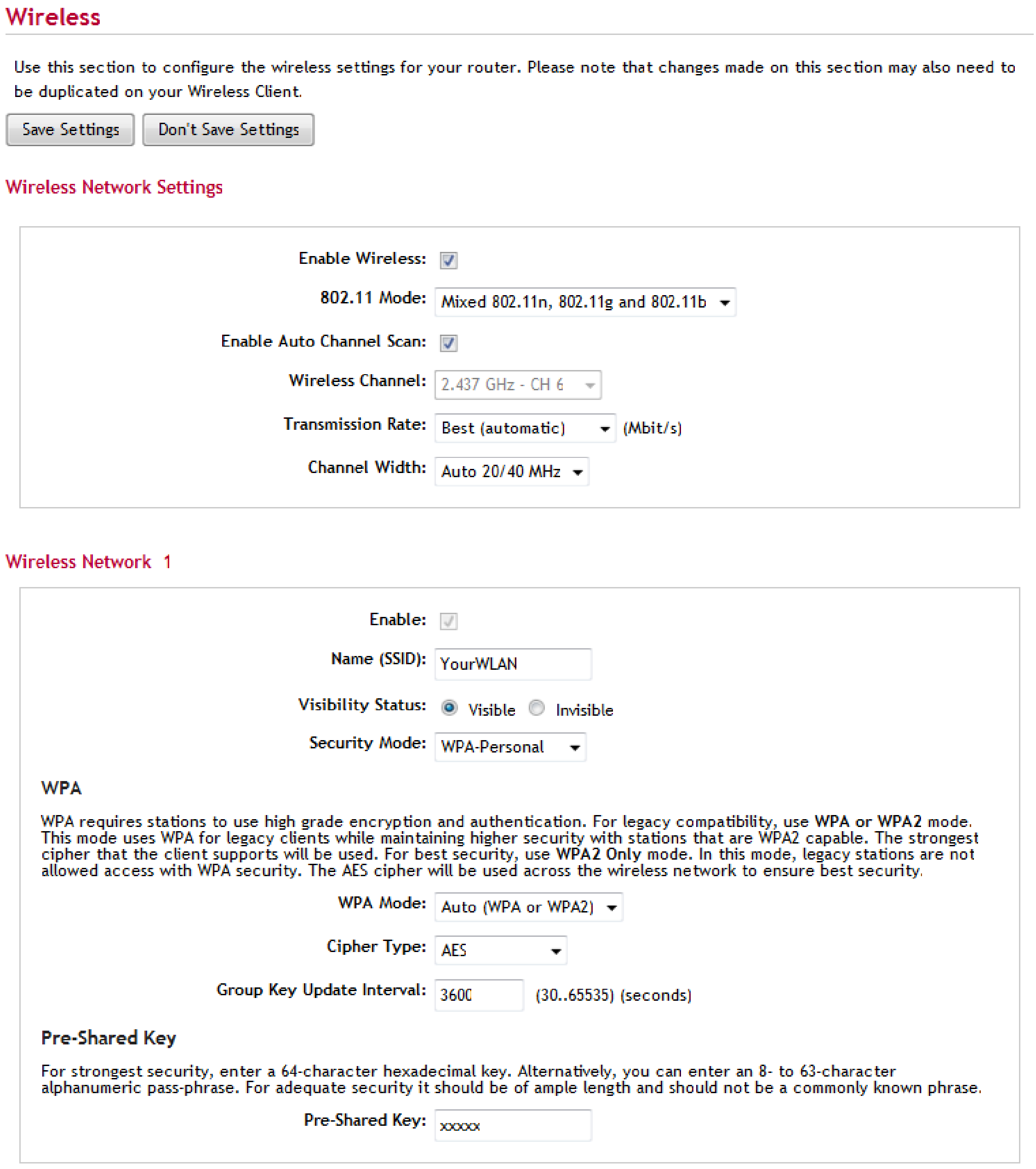
This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the router.

Manual Wireless Network Setup

If your wireless network is already set up with Wi-Fi Protected Setup, manual confguration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your router manually, then click on the Manual Wireless Network Setup button below.

2.3.1 Manual Wireless Network Setup



Wireless

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

Wireless Network Settings

Enable Wireless: ☑

802.11 Mode: Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan: ☑

Wireless Channel: 2.437 GHz - CH 6

Transmission Rate: Best (automatic) (Mbit/s)

Channel Width: Auto 20/40 MHz

Wireless Network 1

Enable: ☑

Name (SSID): YourWLAN

Visibility Status: ● Visible ○ Invisible

Security Mode: WPA-Personal

WPA

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA or WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode: Auto (WPA or WPA2)

Cipher Type: AES

Group Key Update Interval: 3600 (30..65535) (seconds)

Pre-Shared Key

For strongest security, enter a 64-character hexadecimal key. Alternatively, you can enter an 8- to 63-character alphanumeric pass-phrase. For adequate security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key: xxxxx

2.3.1.1 Wireless Network Settings

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

802.11 Mode: Over the years there has been developed many wireless modes. 802.11b (11 Mb/s) is the oldest, then came 802.11g (54 Mb/s) and the newest is

802.11n (270 Mb/s). You can choose to run all of these modes or just some of them. The reason to not choose n-mode is if you have devices which are too old to support n-mode. Choosing an "Only"-choice will improve the performance slightly.

Enable Auto Channel Scan: If chosen the network will try to choose channels with the least interference (from other wireless devices).

Wireless channel: If Auto Channel Scan is disabled you may choose the the channel manually. You can find out which channels are in use by downloading a wireless scanner from the Internet.

Transmission rate: You may restrict the transmission rate at a lower rate than maximum or leave it in default position: Best (automatic).

Channel width: 802.11n mode uses 40MHz channel width, while the other modes use 20MHz. Setting the mode to Auto is the preferred choice.

2.3.1.2 Wireless Network 1

Enable: Will enable/disable wireless network 1.

Name (SSID): Specify a name for the network.

Visibility Status: If "Visible" the network will show up when searching for wireless network on your computer.

Security Mode: None, WEP, WPA-Personal or WPA-Enterprise.

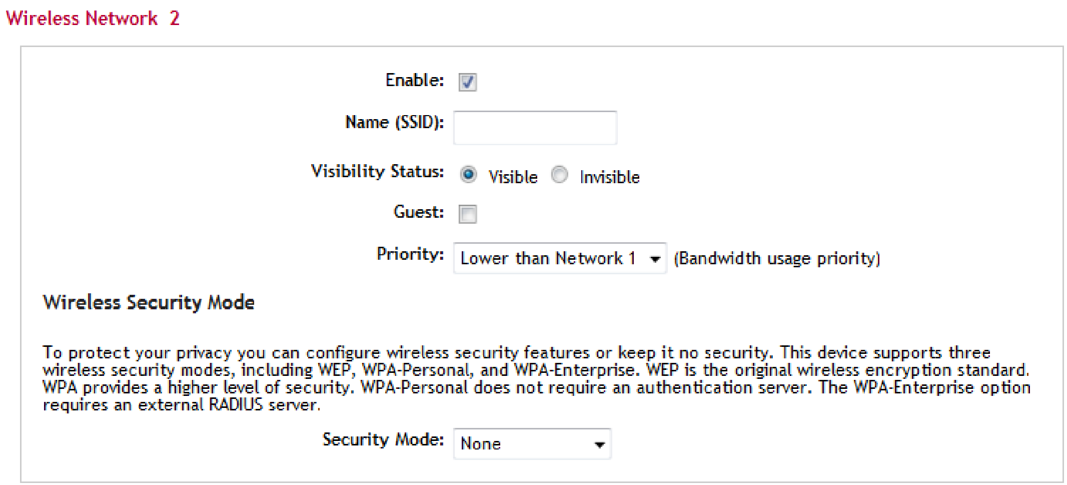
If you choose **None** then your wireless network will be open for all wireless devices in your neighborhood. Do not use this setting unless you have no neighbors or you really trust them.

WEP is the oldest encryption scheme supported by this device. It is not to be used unless the other devices you connect to the wireless network supports only this encryption scheme. WEP can hacked in less than 60 seconds if you have the right tools and enough traffic. However, it's better than None. If you choose WEP then you must decide WEP Key Length. Set it to 64bit and then make a 5 character password (since there only a few seconds more protection in 128bit than 64bit). If there are problems with the password, try to only use 0-9 and a-f as characters. Authentication can be set to "Open" or "Shared Key". Open is considered the most secure way of running WEP, albeit not actually secure.

WPA-Personal is the second best encryption scheme offered, but it has one big advantage over the best encryption: It's easy to setup! It also goes by other names like WPA-PSK and WPA-Home. WPA have two modes, WPA and WPA2, WPA2 is a stronger encryption than WPA. Set to Auto unless you want to avoid WPA. Cipher type can be AES (newest and best) or TKIP (old and outdated). Set to both if in doubt whether your wireless clients can handle AES. Group Key Update Interval should be left at 3600 sec, at least not lowered. The Pre-Shared key is the password you will set on each of the wireless clients/devices. In order to make a secure password use 8-10 characters with a mix of letters a-z, A-Z and digits 0-9. Make sure not to use any dictionary words. It should then take between 100 and 1000 years to break with the best computer of today (2010).

WPA-Enterprise is for usage in an enterprise environment or to make your home network really, really secure. The point of this setup is to distribute the WPA keys on a regular pattern via a so-called RADIUS server. In that case an attacker will have even less time to break the encryption. How to setup up such a server is outside the scope of this manual. Otherwise it is the same as for WPA-Personal.

2.3.1.3 Wireless Network 2-4



Wireless Network 2

Enable: ☑

Name (SSID):

Visibility Status: ● Visible ○ Invisible

Guest: □

Priority: Lower than Network 1 (Bandwidth usage priority)

Wireless Security Mode

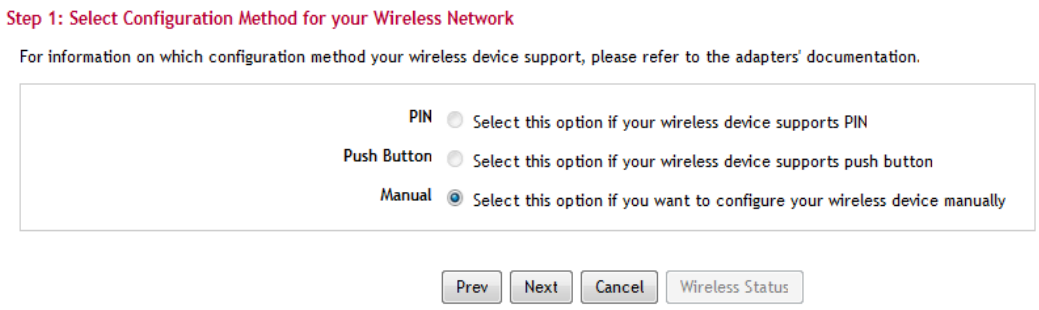
To protect your privacy you can configure wireless security features or keep it no security. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode: None

The wireless networks 2-4 are identical. They can be setup as Guest network which means that devices connecting to this network can only get access to the Internet (WAN) and not the local network (LAN). You may also prioritize the bandwidth compared to the other networks. Otherwise it's the same settings as for Network 1.

2.3.2 Add Private Wireless Device Wizard

This wizard will help you connect a device with this router. There are 3 ways to go about it:



Step 1: Select Configuration Method for your Wireless Network

For information on which configuration method your wireless device support, please refer to the adapters' documentation.

PIN ○ Select this option if your wireless device supports PIN

Push Button ○ Select this option if your wireless device supports push button

Manual ● Select this option if you want to configure your wireless device manually

The Manual way is simply to copy the necessary data from this router til the device you're trying to connect (things like Key, Cipher type, SSID, etc.). The wizard will only tell you what to copy.

The Push Button and PIN method both relies on something called Wi-Fi Protected Setup. If these buttons are not enabled, go to Advanced->Wi-Fi Protected Setup and enable it. The point of Wi-Fi protected Setup is to support and easy way of connecting a device to the wireless access point. The key point is that the devices must support this kind of method (with a button or a way to enter a PIN).

2.3.3 Add Guest Wireless Device Wizard

This is the same wizard as above, except that it will only connect your device to a Guest network (see chapter "Wireless Network 2-4")

2.3.4 Wireless Network Setup Wizard

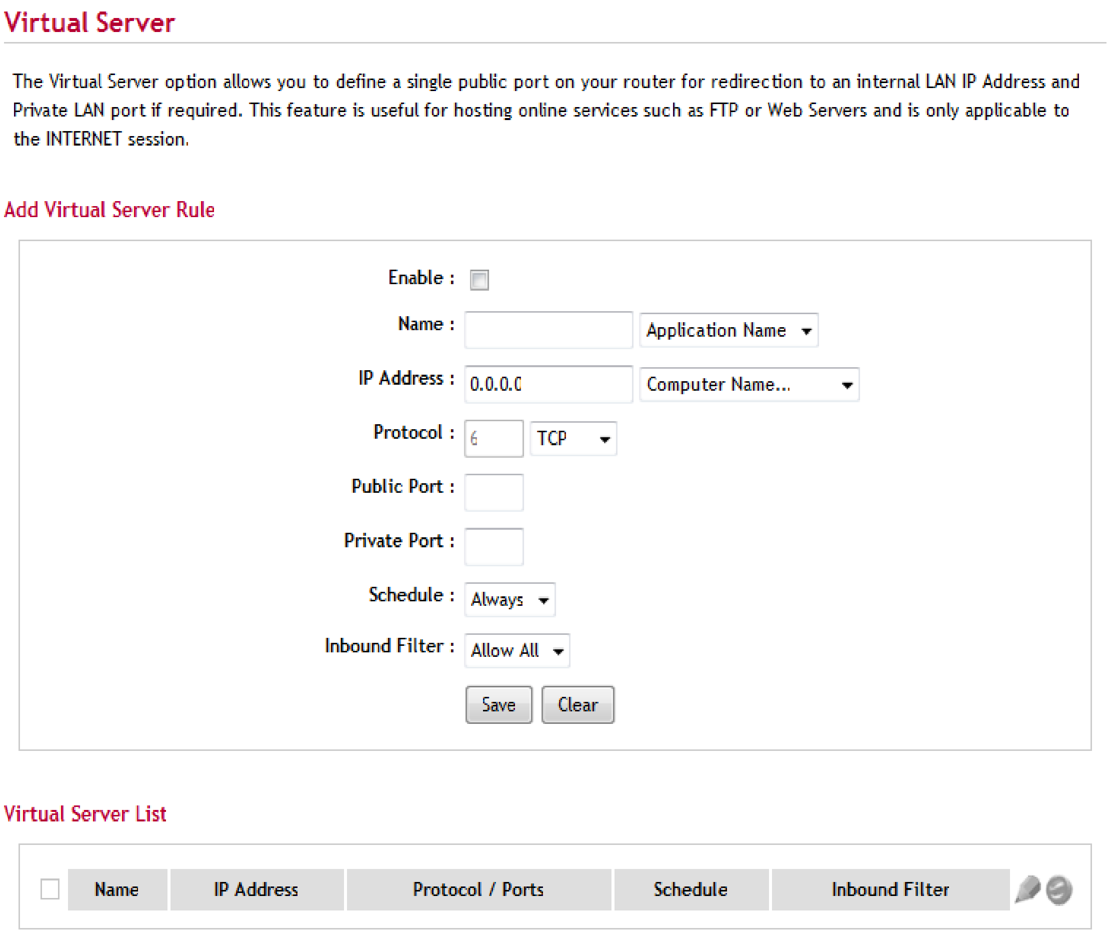
This Wizard is supposed to help you setup a network. As of this moment, it can only update/change an existing network. For that reason it is not very useful, since it will change the settings of your network (if you choose Auto mode). The recommendation is not use it, use the Manual Wireless Network Setup instead.

3 Advanced

The Advanced options allow you to configure a variety of advanced features including ports, application priority, Internet access, filters, and advanced wireless settings.

3.1 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 port.



Virtual Server

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers and is only applicable to the INTERNET session.

Add Virtual Server Rule

Enable : □

Name : Application Name

IP Address : 0.0.0.0 Computer Name...

Protocol : 6 TCP

Public Port :

Private Port :

Schedule : Always

Inbound Filter : Allow All

Virtual Server List

□	Name	IP Address	Protocol / Ports	Schedule	Inbound Filter

Example: You are hosting a Web Server on a PC that has Private IP Address of 192.168.176.50 and your ISP is blocking Port 80.

1. Name the Virtual Server Rule (ex. Web Server)
2. Enter in the IP Address of the machine on your LAN – 192.168.176.50
3. Enter the Private Port as [80] and the Public Port as [8888]
4. Select the Protocol - TCP and ensure the schedule is set to Always
5. Check the Add Rule to add the settings to the Virtual Server List
6. 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 Rule all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.176.50.

3.1.1 Add/Edit Virtual Server

Enable: Toggle whether a *virtual server* is *Enabled* or *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 "Application Name" drop-down 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 192.168.176.50. You can select a computer from the list of DHCP clients in the "Computer Name" drop-down menu, or you can manually enter the IP address of the server computer.

Protocol: Select the protocol used by the service. The common choices -- UDP, TCP, and both UDP and TCP -- can be selected from the drop-down menu. To specify any other protocol, select "Other" from the list, then enter the corresponding protocol number (as assigned by the IANA) in the Protocol box

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

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

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.

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.

Save: Saves the new *virtual server* or modified existing *virtual server* to the **Virtual Servers List**. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

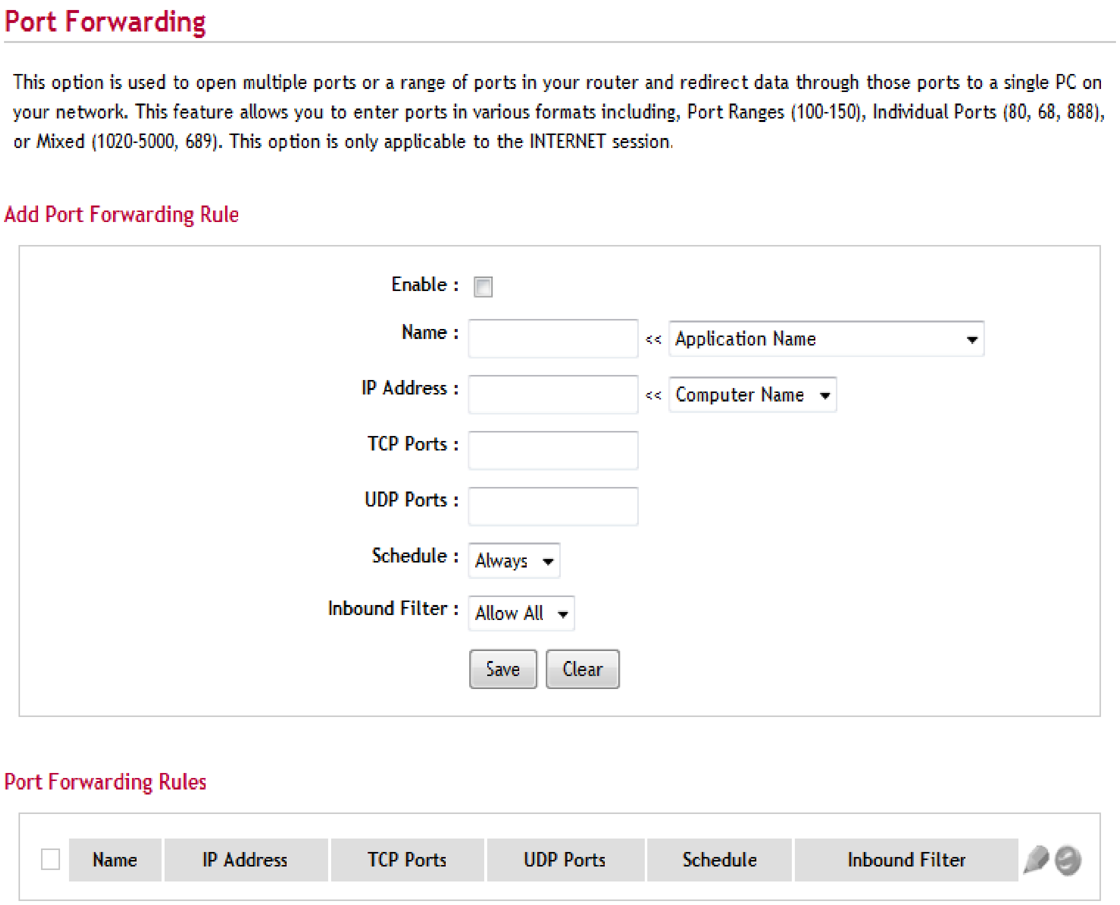
Clear: Clears the selections you have made and returns the fields to their original value.

3.1.2 Virtual Servers List

This 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.

3.2 Port Forwarding

This option 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 including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).



Port Forwarding

This option 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 including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

Add Port Forwarding Rule

Enable :	□
Name :	<< Application Name ▾
IP Address :	<< Computer Name ▾
TCP Ports :	
UDP Ports :	
Schedule :	Always ▾
Inbound Filter :	Allow All ▾

Port Forwarding Rules

□	Name	IP Address	TCP Ports	UDP Ports	Schedule	Inbound Filter

Enable: Check to enable this rule

Name: Name of the rule

IP Address: The IP Address of the computer/device you want to forward to

TCP Ports: Specify a list or a range, or a mix of both

UDP Ports: Specify a list or a range, or a mix of 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.

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.

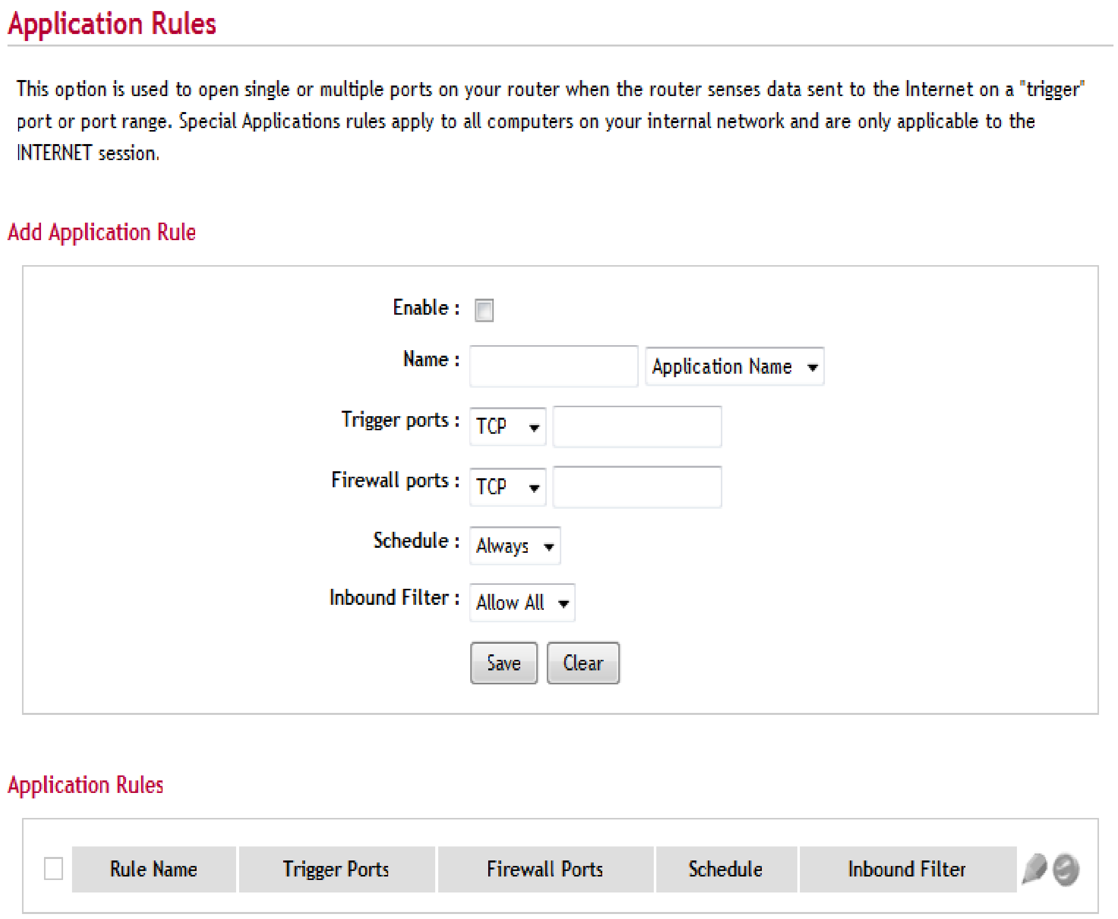
Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

3.2.1 Port forwarding Rules

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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.3 Special Applications

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.



Application Rules

This option 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 and are only applicable to the INTERNET session.

Add Application Rule

Enable : □

Name : Application Name ▾

Trigger ports : TCP ▾

Firewall ports : TCP ▾

Schedule : Always ▾

Inbound Filter : Allow All ▾

Application Rules

□	Rule Name	Trigger Ports	Firewall Ports	Schedule	Inbound Filter	

3.3.1 Add/Edit Special Applications Rule

In this section you can set up the parameters of a new *special applications rule*, or edit the parameters of an existing rule.

Enable: Toggle whether a *special applications rule* is *Enabled* or *Disabled*.

Rule Name: Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. Alternatively, you can select from the **Application** list of common applications.

Application: Instead of entering a name for the *special applications rule*, you can select from this list of common applications, and the remaining configuration values will automatically be filled in according to your selection.

Trigger Port Range: Enter the outgoing port range used by your application.

Trigger Port Protocol: Select the outbound protocol used by your application.

Input Port Range: Enter the port range that you want to open up to Internet traffic.

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

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.

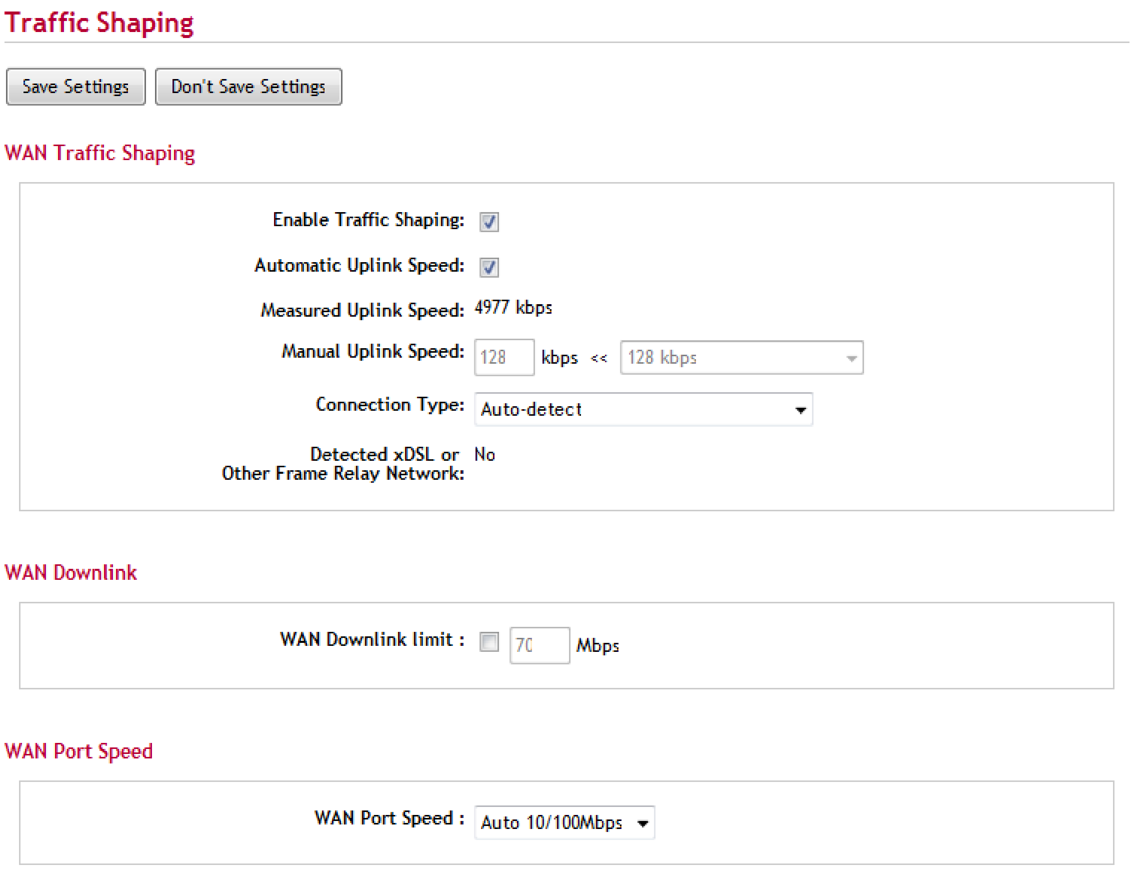
Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

3.3.2 Special Applications Rules List

This 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. After you've completed all modifications, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.4 Traffic Shaping

This section contains options for configuring the flow of traffic.



Traffic Shaping

WAN Traffic Shaping

Enable Traffic Shaping: ☑

Automatic Uplink Speed: ☑

Measured Uplink Speed: 4977 kbps

Manual Uplink Speed: 128 kbps << 128 kbps

Connection Type: Auto-detect

Detected xDSL or Other Frame Relay Network: No

WAN Downlink

WAN Downlink limit : □ 70 Mbps

WAN Port Speed

WAN Port Speed : Auto 10/100Mbps

Enable Traffic Shaping: When this option is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.

Automatic Uplink Speed: Enable/ Disable the automatic determination of uplink speed. When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is reestablished (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.

Manual Uplink Speed: If **Automatic Uplink Speed** is disabled, this options 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, 1.5Mbps/284kbps. 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 Frame Relay Network: When **Connection Type** is set to *Auto-detect*, the automatically detected connection type is **displayed** here.

WAN Downlink: If you want to restrict the downlink, you can do that here. Setting the downlink higher than the downlink provided by your ISP will not have any effect.

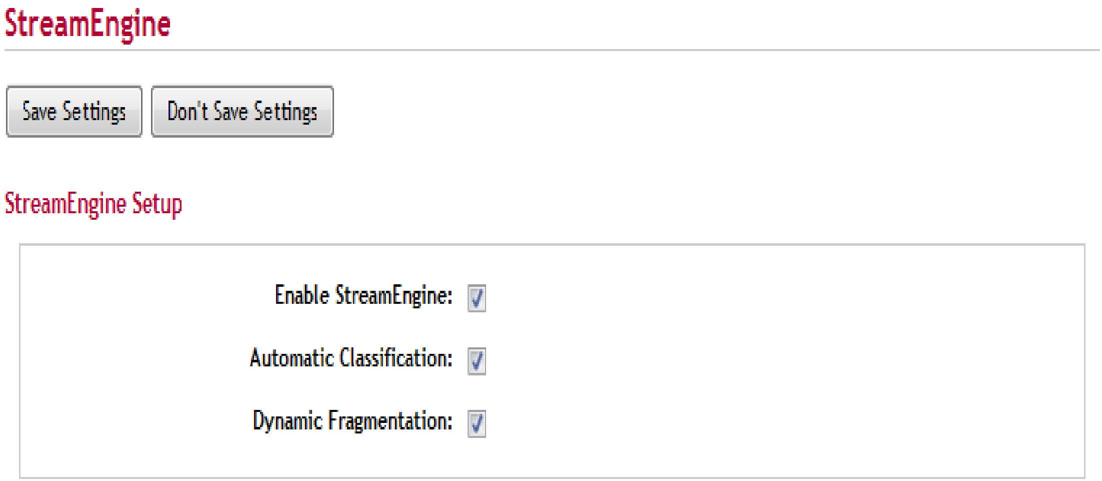
WAN Port Speed: Leave it in Auto mode, unless in special circumstances.

3.5 StreamEngine™

The StreamEngine™ option helps improve your network performance by prioritizing applications. By default the StreamEngine™ settings are disabled and application priority is not classified automatically. To enable this menu you must first enable Traffic Shaping (previous chapter). StreamEngine™ is developed by Ubicom (www.ubicom.com).

3.5.1 StreamEngine™ Setup

In this section you may configure the StreamEngine™ and its features.



StreamEngine

StreamEngine Setup

Enable StreamEngine: ☑

Automatic Classification: ☑

Dynamic Fragmentation: ☑

Enable StreamEngine™: This option is enabled by default. Disable this option for testing how the traffic and services performs without StreamEngine™ enabled. This engine will enhance VoIP, video conferencing, gaming, data throughput while keeping control of P2P applications.

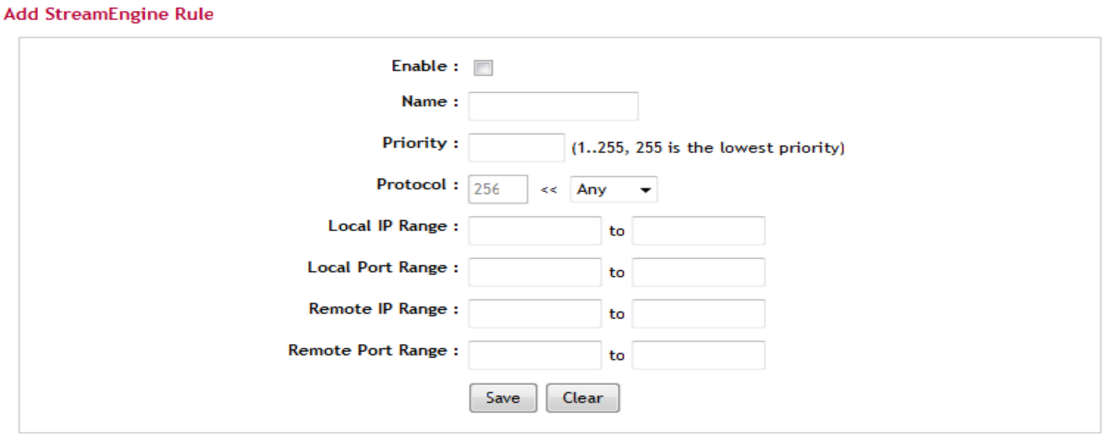
Automatic Classification: This option is enabled by default so that your router will automatically determine which programs should have network priority. Leave this option enabled for best performance, so that it may automatically set the priorities for your applications.

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

3.5.2 Add/Edit StreamEngine™ Rule

A *StreamEngine™ rule* identifies a specific message flow and assigns a priority to that flow. For most applications, *automatic classification* will be adequate, and specific *StreamEngine™ rules* will not be required.

Note: Conflicting rules are not permitted. Conflicting rules are those that share any combination of source address/port, destination address/port, and protocol. Rejecting conflicting rules ensures the that every flow defined in a rule receives the expected priority and avoids indeterminate prioritization that could reduce QoS effectiveness.



Add StreamEngine Rule

Enable : □

Name :

Priority : (1..255, 255 is the lowest priority)

Protocol : 256 << Any

Local IP Range : to

Local Port Range : to

Remote IP Range : to

Remote Port Range : to

Enable: Toggle whether a *StreamEngine™ rule* is *Enabled* or *Disabled*.

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

Priority: The priority of the message flow is entered here. 1 receives the highest priority (most urgent) and 255 receives the lowest priority. 0 is reserved. Flows that are not prioritized by any rule receive lowest priority.

Protocol: The *protocol* used by the messages. The common choices can be selected from the drop-down menu. To specify any other protocol, enter its *protocol number* (as assigned by the IANA) in the **Protocol** box.

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

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

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

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

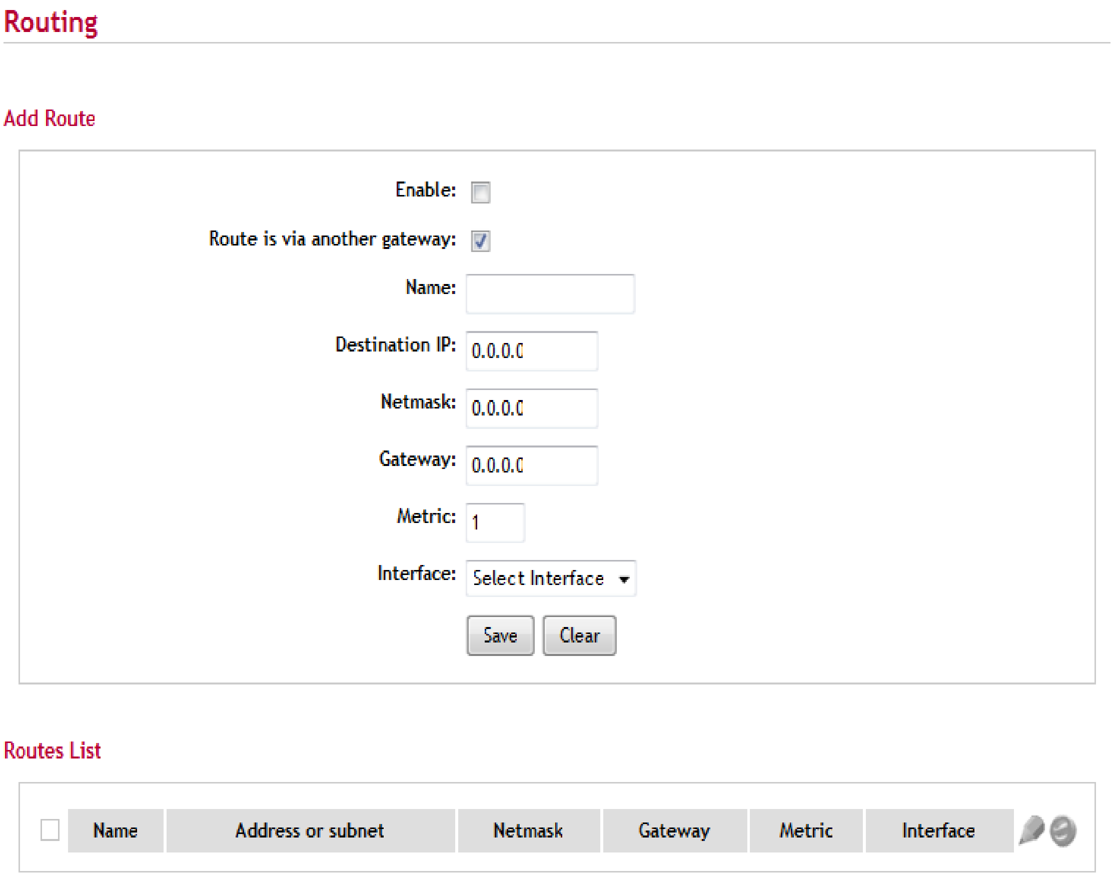
Save: Saves the new rule or modified existing rule to the *StreamEngine™ Rules* list. When you are done editing the settings, you must click the *Save Settings* button at the top of the page to make the changes effective and permanent.

3.5.3 StreamEngine™ Rules List

The section shows the currently defined *StreamEngine™ rules*. A *StreamEngine™ 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 StreamEngine™ Rule*" section is activated for editing. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.6 Routing

This section contains *Routing* options, allowing you to define fixed routes to defined destinations.



Routing

Add Route

Enable:	□
Route is via another gateway:	☑
Name:	
Destination IP:	0.0.0.0
Netmask:	0.0.0.0
Gateway:	0.0.0.0
Metric:	1
Interface:	Select Interface

Routes List

□	Name	Address or subnet	Netmask	Gateway	Metric	Interface

3.6.1 Add/ Edit Route

Adds a new route to the IP routing table, or edits an existing route.

Enable: Toggle whether a *route* is *Enabled* or *Disabled*.

Route is via another gateway: When checked, the Gateway box is displayed and must be completed with the IP address of the gateway/router to which this route corresponds. Datagrams sent to this route are forwarded onto the given Gateway IP address for further processing. When unchecked, this route represents a local route for which this router has its own IP address with which to communicate.

Name: Assign a meaningful name to this route for your own use.

Destination IP: The IP address or network that the packets will be attempting to access
Note: 192.168.1.0 with a Netmask of 255.255.255.0 means traffic will be routed to the entire 192.168.1.x network.

Netmask: The bits in the mask specify which bits of the IP address must match.
Note: 255.255.255.255 is used to signify only the host that was entered in the Destination IP field.

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.

Metric: The route metric is a value from 1 to 16 that indicates the cost of using this route. A value of 1 is the lowest cost, and 15 is the highest cost. A value of 16 indicates that the route is not reachable from this router. When trying to reach a particular destination, computers on your network will select the best route, ignoring unreachable routes.

Interface: Specifies the interface, LAN or WAN, that the IP packet must use to transit out of the router when this route is used.

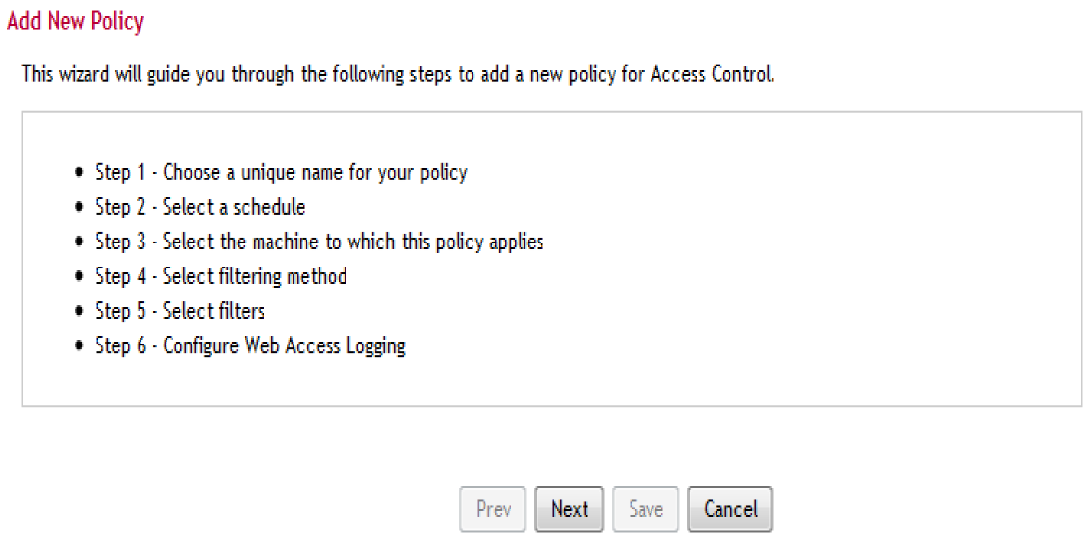
Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes
effective and permanent.

3.6.2 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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.7 Access Control

The Access Control section allows you to control access in and out of 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 like P2P utilities or games.



Add New Policy

This wizard will guide you through the following steps to add a new policy for Access Control.

- Step 1 - Choose a unique name for your policy
- Step 2 - Select a schedule
- Step 3 - Select the machine to which this policy applies
- Step 4 - Select filtering method
- Step 5 - Select filters
- Step 6 - Configure Web Access Logging

3.7.1 Access Control

Enable: Toggle whether *access control* is *Enabled* or *Disabled*.

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.

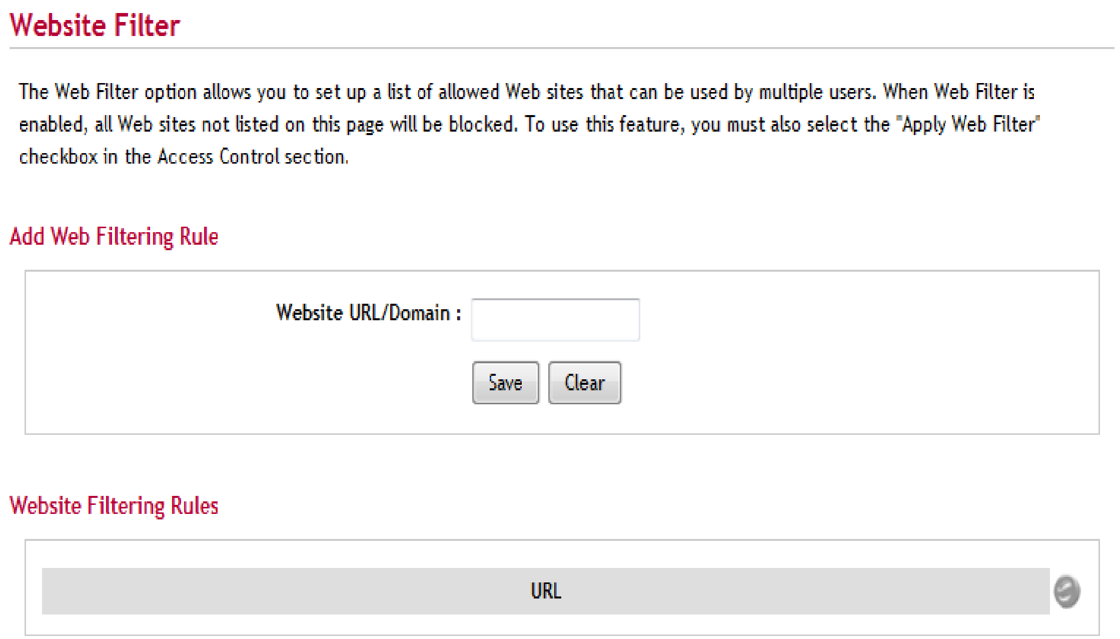
Add Policy: Click this button to start creating a new access control policy. The Policy Wizard guides you through the steps of defining each access control policy. A policy is the "Who, What, When, and How" of access control -- whose computer will be affected by the control, what internet addresses are 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.

3.7.2 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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.7.3 WEB Filter

This section is where you add the Web sites to be used for **Access Control**. The Web sites listed here are used when the *Web Filter* option is enabled in **Access Control**.



Website Filter

The Web Filter option allows you to set up a list of allowed Web sites that can be used by multiple users. When Web Filter is enabled, all Web sites not listed on this page will be blocked. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

Add Web Filtering Rule

Website URL/Domain :

Website Filtering Rules

URL

3.7.4 Add/Edit Web Site

This is where you can add Web sites to the **Allowed Web List**. The **Allowed Web 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 (such as **google.com**). Enter the most inclusive domain name. For instance, entering dlink.com will give you access to www.dlink.com and support.dlink.com.
Do not enter the **http://** preceding the URL.
Note: Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all of the web sites used to construct a page. For example, to access my.yahoo.com, you must enable access to yahoo.com, yimg.com, and doubleclick.net.

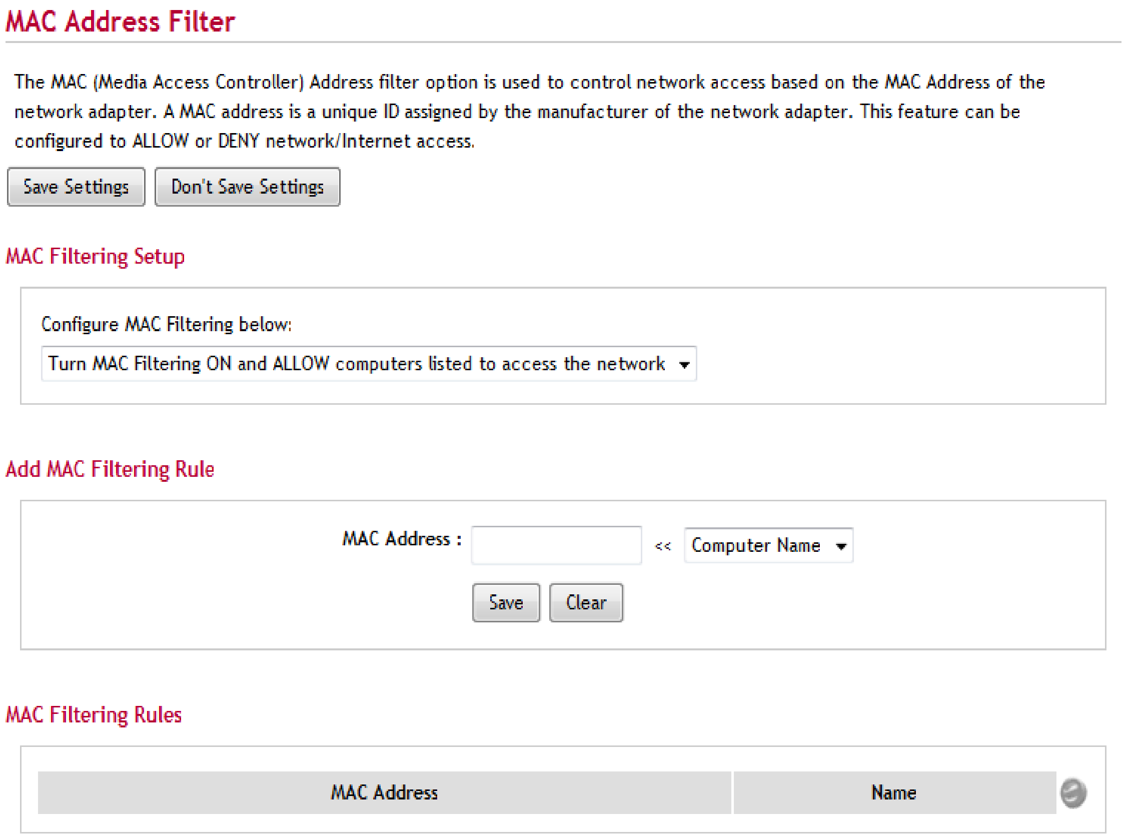
Save: Saves the new or modified *Allowed Web Site* in the **Allowed Web Site List**. When you are done editing the settings, you must click the *Save Settings* button at the top of the page to make the changes effective and permanent.

3.7.5 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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.8 MAC Address Filter

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access for devices based on their MAC address.



MAC Address Filter

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

MAC Filtering Setup

Configure MAC Filtering below: Turn MAC Filtering ON and ALLOW computers listed to access the network

Add MAC Filtering Rule

MAC Address :

MAC Filtering Rules

MAC Address	Name

3.8.1 MAC Filtering Setup

Enable MAC Address Filter: When this is enabled, depending on the mode selected, computers are granted or denied network access based on their MAC address.

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

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.

3.8.2 Add/ Edit MAC Address

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

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

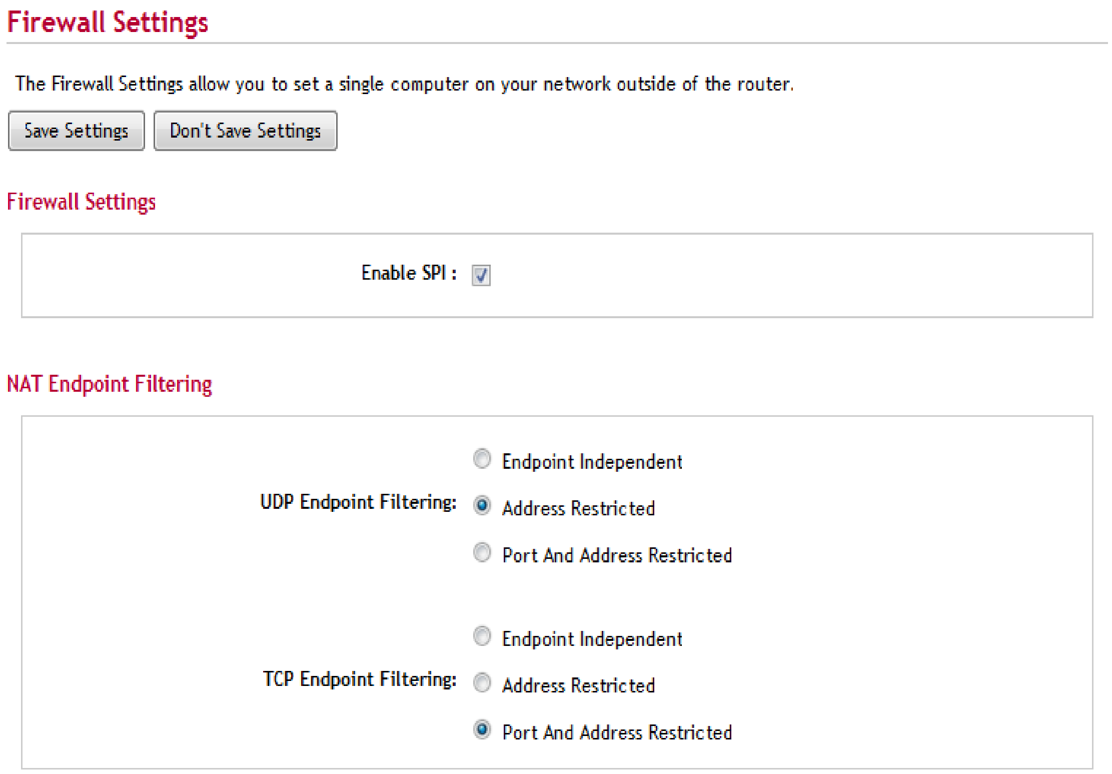
Save: Saves the new or modified MAC address in the MAC Address List. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

3.8.3 MAC Address List

This 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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.9 Firewall

A firewall protects your network from the outside world. The RGW208EN provides a tight firewall by virtue of the way NAT works. Unless you configure the router to the contrary, the NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attackers. However, some network applications cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control several ways of opening the firewall to address the needs of specific types of applications.



Firewall Settings

The Firewall Settings allow you to set a single computer on your network outside of the router.

Firewall Settings

Enable SPI : ☑

NAT Endpoint Filtering

UDP Endpoint Filtering:
○ Endpoint Independent
● Address Restricted
○ Port And Address Restricted

TCP Endpoint Filtering:
○ Endpoint Independent
○ Address Restricted
● Port And Address Restricted

3.9.1 Firewall Settings

Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. When SPI is enabled, the extra state information will be reported on the Status > Active sessions page.

Whether *SPI* is enabled or not, the router always tracks TCP connection states and ensures that each TCP packet's flags are valid for the current state.

3.9.2 NAT Endpoint Filtering

The NAT Endpoint Filtering options controls how the router's NAT manages incoming connection requests to ports that are already being used.

Endpoint Independent: Once a LAN-side application has created a connection through a specific port, the NAT will forward any incoming connection requests with the same port to the LAN-side application regardless of their origin. This is the least restrictive option, giving the best connectivity and allowing some applications (P2P applications in particular) to behave almost as if they are directly connected to the Internet.

Address Restricted: The NAT forwards incoming connection requests to a LAN-side host only when they come from the same IP address with which a connection was established. This allows the remote application to send data back through a port different from the one used when the outgoing session was created.

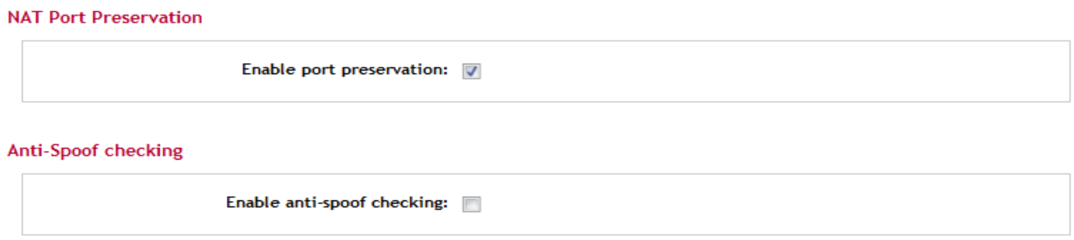
Port and Address Restricted: The NAT does not forward any incoming connection requests with the same port address as an already establish connection.

Note that some of these options can interact with other port restrictions. Endpoint Independent Filtering takes priority over inbound filters or schedules, so it is possible for an incoming session request related to an outgoing session to enter through a port in spite of an active inbound filter on that port. However, packets will be rejected as expected when sent to blocked ports (whether blocked by schedule or by inbound filter) for which there are no active sessions. Port and Address Restricted Filtering ensures that inbound filters and schedules work precisely, but prevents some level of connectivity, and therefore might require the use of port triggers, virtual servers, or port forwarding to open the ports needed by the application. Address Restricted Filtering gives a compromise position, which avoids problems when communicating with certain other types of NAT router (symmetric NATs in particular) but leaves inbound filters and scheduled access working as expected.

UDP Endpoint Filtering: Controls endpoint filtering for packets of the UDP protocol.

TCP Endpoint Filtering: Controls endpoint filtering for packets of the TCP protocol.

3.9.3 Various



NAT Port Preservation

Enable port preservation: ☑

Anti-Spoof checking

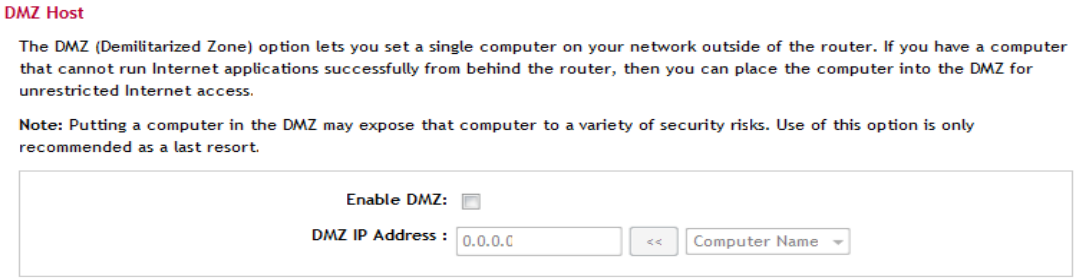
Enable anti-spoof checking: □

NAT Port Preservation: NAT Port preservation (on by default) tries to ensure that, when a LAN host makes an Internet connection, the same LAN port is also used as the Internet visible port. This ensures best compatibility for internet communications. Under some circumstances it may be desirable to turn off this feature.

Anti-Spoof checking: Enabling this option can provide protection from certain kinds of "spoofing" attacks. However, enable this option with care. With some modems, the WAN connection may be lost when this option is enabled. In that case, it may be necessary to change the LAN subnet to something other than 192.168.0.x (192.168.2.x, for example), to re-establish the WAN connection.

3.9.4 DMZ Host

The *DMZ (Demilitarized Zone)* option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the *DMZ* for unrestricted Internet access.



DMZ Host

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

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.

Enable DMZ: ☐

DMZ IP Address : 0.0.0.0 << Computer Name

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

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

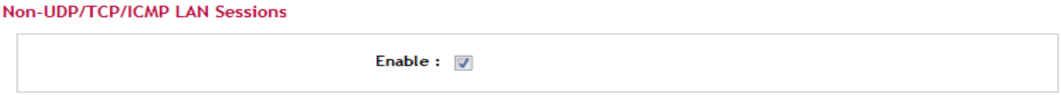
DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it’s IP address automatically using *DHCP*, be sure to make a *DHCP reservation* on the *Basic -> DHCP* page so that the IP address of the *DMZ machine* does not change.

After you’ve completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

3.9.5 Non-UDP/ TCP/ IMCP LAN Sessions

When a LAN application that uses a protocol other than UDP, TCP, or ICMP initiates a session to the Internet, the router's NAT can track such a session, even though it does not recognize the protocol. This feature is useful because it enables certain applications (most importantly a single VPN connection to a remote host) without the need for an *Application Layer Gateway*.

Note that this feature does not apply to the DMZ host (if one is enabled). The DMZ host always handles these kinds of sessions.



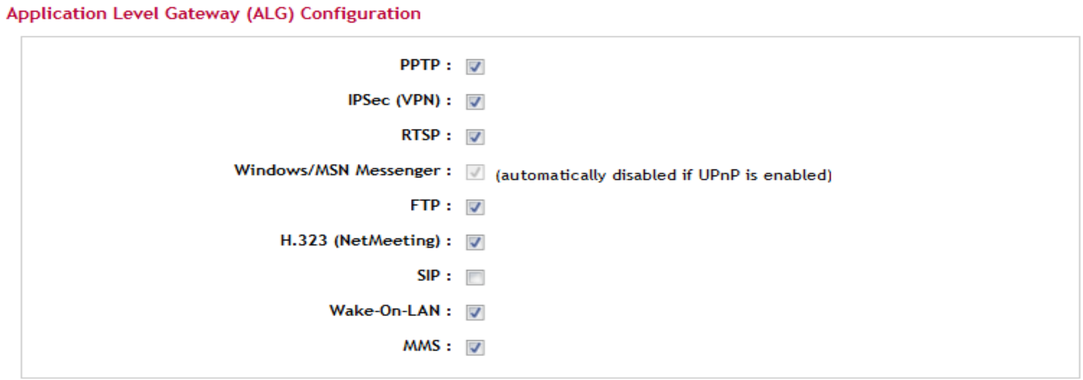
Non-UDP/TCP/ICMP LAN Sessions

Enable : ☑

Enable: Enabling this option enables single VPN connections to a remote host. (But, for multiple VPN connections, the appropriate VPN ALG must be used.) Disabling this option, however, only disables VPN if the appropriate VPN ALG is also disabled.

3.9.6 Application Level Gateway (ALG) Configuration

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.



Application Level Gateway (ALG) Configuration

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

Windows/MSN Messenger : ☑ (automatically disabled if UPnP is enabled)

FTP : ☑

H.323 (NetMeeting) : ☑

SIP : □

Wake-On-LAN : ☑

MMS : ☑

PPTP: Allows multiple machines on the LAN to connect to their corporate networks using PPTP protocol. When the PPTP ALG is enabled, LAN computers can establish PPTP VPN connections either with the same or with different VPN servers. When the PPTP ALG is disabled, the router allows VPN operation in a restricted way -- LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server.

IPSec (VPN): Allows multiple VPN clients to connect to their corporate networks using IPSec. Some VPN clients support traversal of IPSec through NAT. This option may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try disabling this option.
Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

Note that L2TP VPN connections typically use IPSec to secure the connection. To achieve multiple VPN pass-through in this case, the IPSec ALG must be enabled.

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/ MSN Messenger: Supports use on LAN computers of Microsoft Windows Messenger (the Internet messaging client that ships with Microsoft Windows) and MSN Messenger. 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.

H.323 (NetMeeting): Allows H.323 (specifically 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.

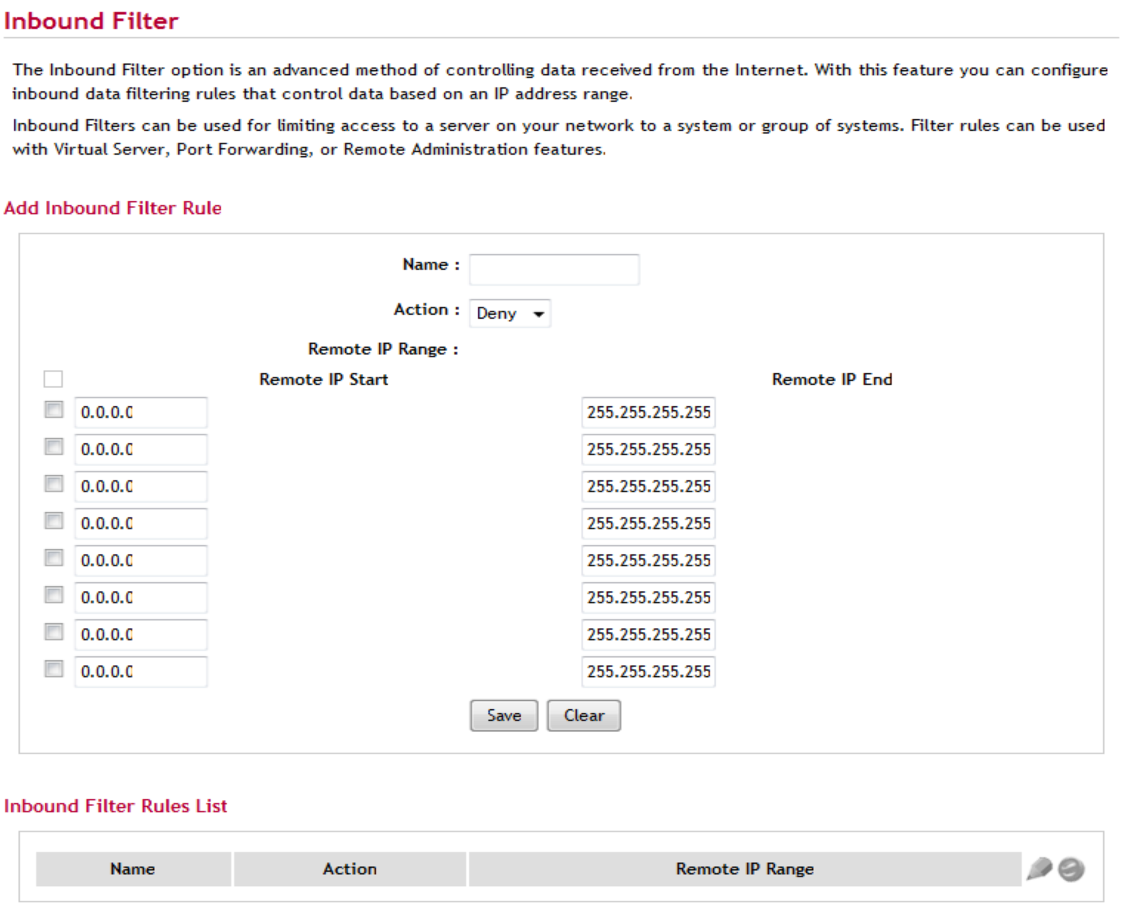
SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning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

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

3.10 Inbound filter

The Inbound Filters 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 an IP address range.
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.



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 an IP address range.

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, Port Forwarding, or Remote Administration features.

Add Inbound Filter Rule

Name :

Action : Deny

Remote IP Range :

□	Remote IP Start	Remote IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255

Inbound Filter Rules List

Name	Action	Remote IP Range

3.10.1 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.

Remote 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 rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the *Save Settings* button at the top of the page to make the changes effective and permanent.

3.10.2 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. After you've completed all modifications or deletions, you must click the *Save Settings* button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to *Reboot the Device* or *Continue*. If you need to make additional settings changes, click *Continue*. If you are finished with your configuration settings, click the *Reboot the Device* button.

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

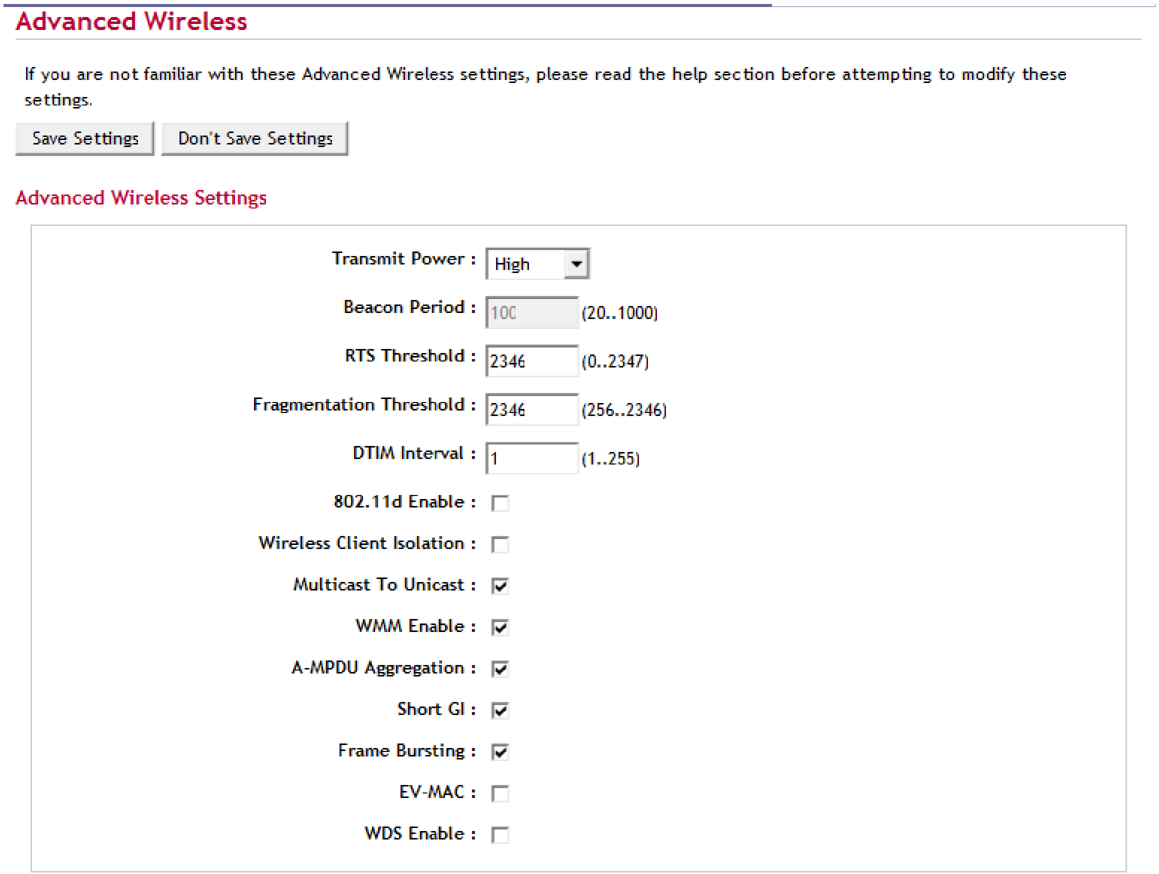
Allow All: Permit any WAN user to access the related capability.

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

3.11 Advanced Wireless

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.

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. Values that are not a multiple of 4, are forced to a multiple of 4.



Advanced Wireless

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

Advanced Wireless Settings

Transmit Power :	High	
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
802.11d Enable :	□	
Wireless Client Isolation :	□	
Multicast To Unicast :	☑	
WMM Enable :	☑	
A-MPDU Aggregation :	☑	
Short GI :	☑	
Frame Bursting :	☑	
EV-MAC :	□	
WDS Enable :	□	

RTS Threshold: When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value of 2346 bytes.

Fragmentation Threshold: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value of 2346 bytes. Setting the Fragmentation value too low may result in poor performance.

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".

Wireless Client Isolation: Enabling Wireless Client Isolation (also known as L2 Isolation) prevents associated wireless clients from communicating directly with each other by using low-level (link layer) protocols and without passing through the router.

Multicast To Unicast: When multiple wireless clients are receiving streaming media, enabling this option can provide better performance in some cases by transforming each multicast packet into multiple unicast packets. (Broadcast packets are still sent out as broadcast packets.) If you experience interoperability problems when the AP is sending streaming media to some legacy wireless clients, try turning this option off.

WMM Enable: Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

A-MPDU Aggregation: Aggregation of wireless packets based on MAC protocol data units is a technique for maximizing performance. This option should normally remain enabled.

Short GI: Using a short (400ns) guard interval can increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

Frame Bursting: Selecting this option can increase wireless throughput, but can also decrease performance of neighboring APs.

Extra Wireless Protection: Extra protection for neighboring 11b wireless networks. Turn this option off to reduce the adverse effect of legacy wireless networks on 802.11ng performance. This option is available only when 802.11 Mode is set to an 11n Only option. (Refer to the Basic → Wireless page.)

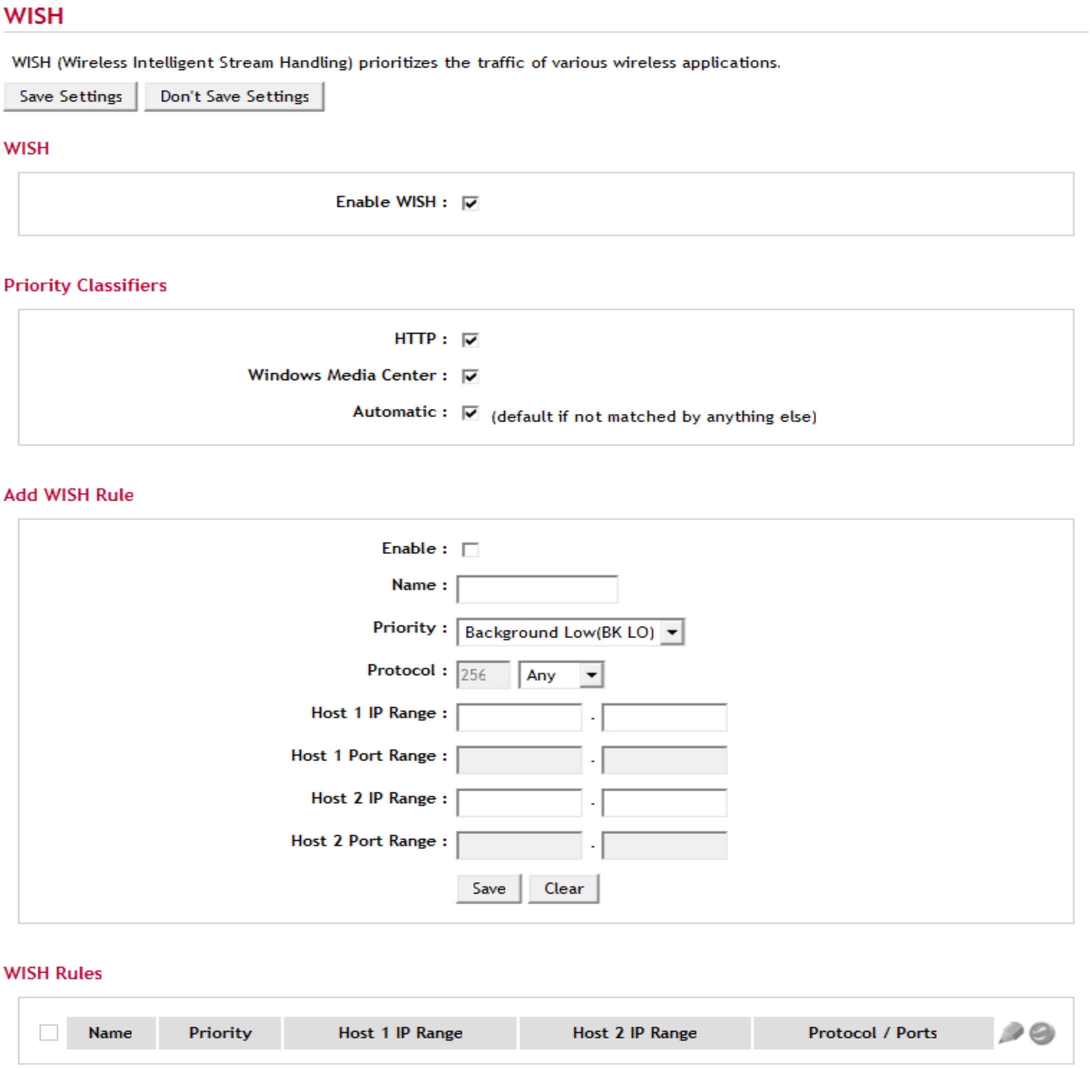
EV-MAC: Enable EV-MAC option for superior experience of wireless video streaming.

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. Make sure the APs are configured with same channel number.

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. Enter a MAC address for each of the other APs that you want to connect with WDS.

3.12 WISH

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.



WISH

WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications.

WISH

Enable WISH : ☑

Priority Classifiers

HTTP : ☑

Windows Media Center : ☑

Automatic : ☑ (default if not matched by anything else)

Add WISH Rule

Enable : □

Name :

Priority : Background Low(BK LO)

Protocol : 256 Any

Host 1 IP Range : -

Host 1 Port Range : -

Host 2 IP Range : -

Host 2 Port Range : -

WISH Rules

□	Name	Priority	Host 1 IP Range	Host 2 IP Range	Protocol / Ports

Enable WISH: Enable this option if you want to allow WISH to prioritize your traffic.

3.12.1 Priority Classifiers

HTTP: Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

Windows Media Center: Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

Automatic: When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

3.12.2 Add/Edit WISH Rule

A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities, and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

Enable: Specifies whether the entry will be active or inactive.

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

Priority: The priority of the message flow is entered here. Four priorities are defined:
BK: Background (least urgent).
BE: Best Effort.
VI: Video.
VO: Voice (most urgent).

Protocol: The protocol used by the messages.

Host 1 IP Range: The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

Host 1 Port Range: The rule applies to a flow of messages for which host 1's port number is within the range set here.

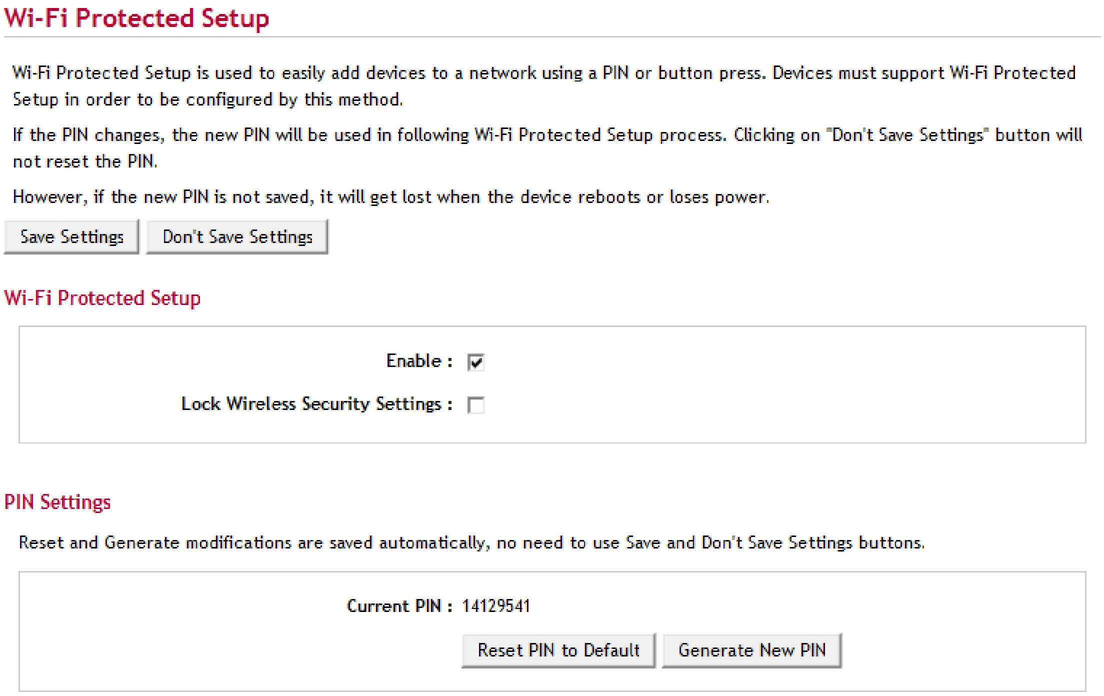
Host 2 IP Range: The rule applies to a flow of messages for which the other computer's IP address falls within the range set here.

Host 2 Port Range: The rule applies to a flow of messages for which host 2's port number is within the range set here.
Save/Update

3.12.3 WISH Rules

This section lists the defined WISH Rules. Click the Enable checkbox at the left to directly activate or de-activate the entry. An entry can be changed by clicking the Edit icon or can be deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Edit WISH Rule" section is activated for editing.

3.13 Wi-Fi Protected Setup



Wi-Fi Protected Setup

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

Wi-Fi Protected Setup

Enable : ☑

Lock Wireless Security Settings : □

PIN Settings

Reset and Generate modifications are saved automatically, no need to use Save and Don't Save Settings buttons.

Current PIN : 14129541

3.13.1 Wi-Fi Protected Setup

Enable: Enable the Wi-Fi Protected Setup feature.
Lock Wireless Security Settings: Locking the wireless security settings prevents the settings from being changed by any new external registrar using its PIN. Devices can still be added to the wireless network using Wi-Fi Protected Setup. It is still possible to change wireless network settings with Manual Wireless Network Setup, Wireless Network Setup Wizard, or an existing external WLAN Manager Registrar.

3.13.2 PIN Settings

A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator ("admin" account) can change or reset the PIN.

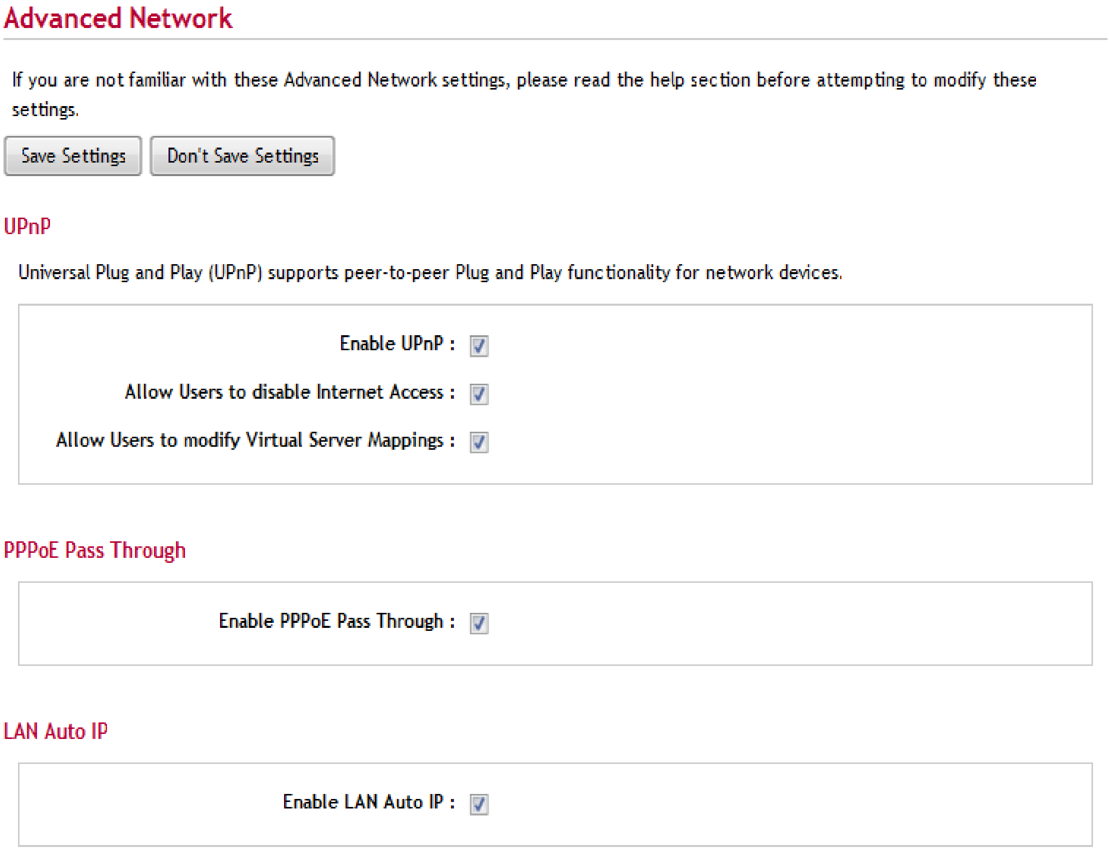
Current PIN: Shows the current value of the router's PIN.

Reset PIN to Default: Restore the default PIN of the router.

Generate New PIN: Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.

3.14 Advanced Network

This section contains advanced network options.



Advanced Network

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

UPnP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP : ☑

Allow Users to disable Internet Access : ☑

Allow Users to modify Virtual Server Mappings : ☑

PPPoE Pass Through

Enable PPPoE Pass Through : ☑

LAN Auto IP

Enable LAN Auto IP : ☑

3.14.1 UPnP

UPnP is short for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software.

Enable UPnP: If you need to use the *UPnP* functionality, you can enable it here.

Allow Users to disable Internet Access: Allow Users to disable Internet Access Disabling this option prevents UPnP clients from terminating the WAN connection.

Allow Users to modify Virtual Server Mappings: Disabling this option prevents UPnP clients from adding, modifying, deleting, or disabling virtual server entries.

3.14.2 PPPoE Pass Through

This option controls whether LAN computers can act as PPPoE clients and negotiate PPP sessions through the router over the WAN ethernet link.

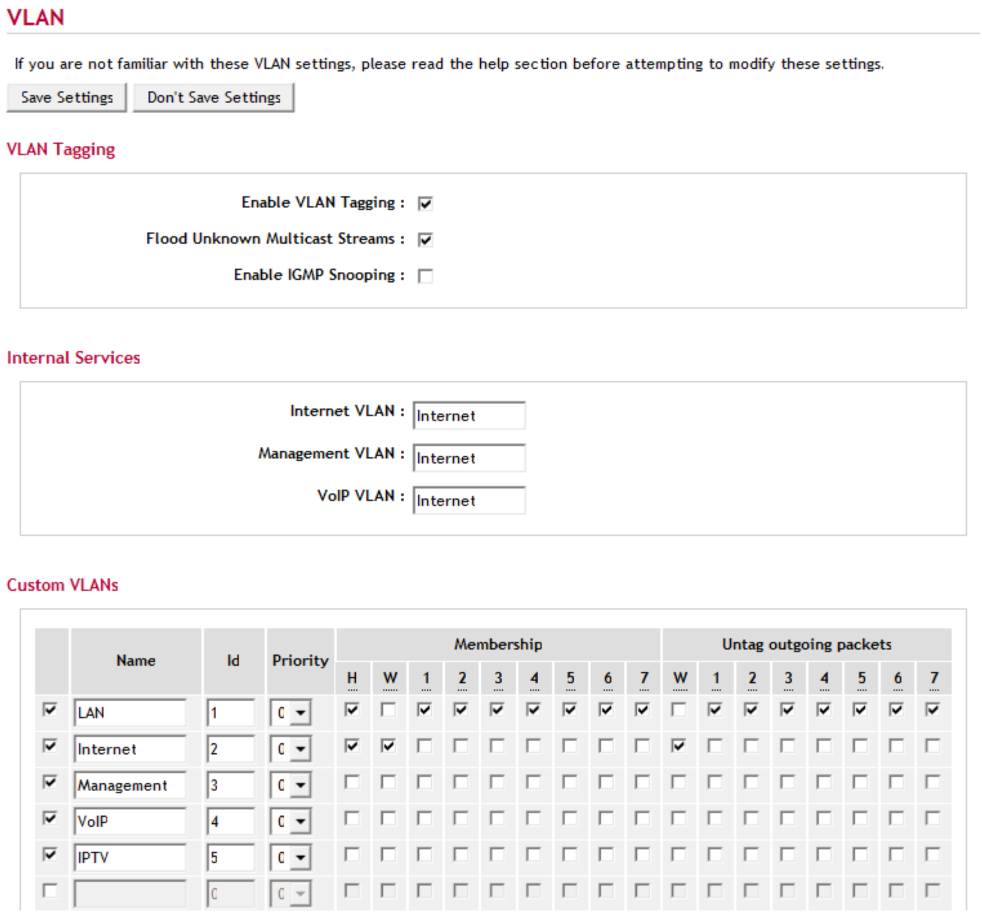
Enable PPPoE Pass Through: Enabling this option allows LAN computers to act as PPPoE clients. Disabling this option prevents LAN computers from establishing PPPoE pass-through connections.

3.14.3 LAN Auto IP

Enables the router to automatically generate its LAN-side IP address and communicate with other LAN computers that also implement auto-IP, even when the router's DHCP server function is disabled.

Enable LAN Auto IP: This option should normally remain enabled.

3.15 VLAN



VLAN

If you are not familiar with these VLAN settings, please read the help section before attempting to modify these settings.

VLAN Tagging

Enable VLAN Tagging : ☑

Flood Unknown Multicast Streams : ☑

Enable IGMP Snooping : □

Internal Services

Internet VLAN : Internet

Management VLAN : Internet

VoIP VLAN : Internet

Custom VLANs

	Name	Id	Priority	Membership									Untag outgoing packets							
				H	W	1	2	3	4	5	6	7	W	1	2	3	4	5	6	7
☑	LAN	1	0	☑	□	☑	☑	☑	☑	☑	☑	☑	□	☑	☑	☑	☑	☑	☑	☑
☑	Internet	2	0	☑	☑	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□
☑	Management	3	0	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
☑	VoIP	4	0	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
☑	IPTV	5	0	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
□		0	0	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

3.15.1 VLAN Tagging

Enable WAN VLAN Tagging: This turns on VLAN functionality.

Flood Unknown Multicast Streams: Useful description goes here.

Enable IGMP Snooping: Useful description goes here.

3.15.2 Internal Services

Here you can assign what VLAN the router services will use. The names enter here should have a matching entry in the VLANs table.

Internet VLAN: This selects the VLAN used for internet access.

Management VLAN: This selects the VLAN used for remote management.

VoIP VLAN: This selects the VLAN used for VoIP connections.

3.15.3 Custom VLANs

This is a list of user defined VLANs.

Name: This is the name of the VLAN which you can use to reference it by in Internal Services and VLAN to SSID mapping.

Id: This is the unique identifer for the VLAN. This will be the id the packets belong to the VLAN will be tagged with.

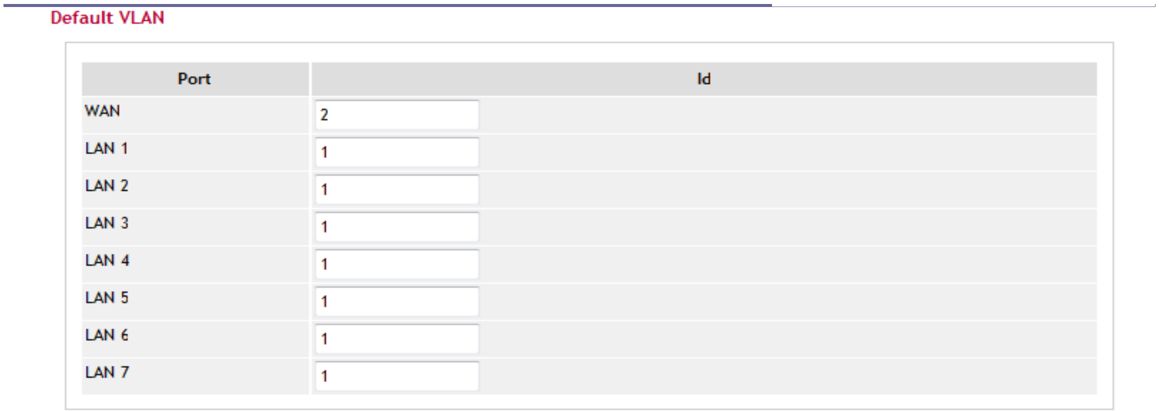
Priority: This is the priority packets sent from the VLAN.

Membership: This is the list of ports which is a member of the VLAN.

Untag ports: This is the ports which should not have the VLAN id tagged on the outgoing packets.

3.15.4 Default VLAN

This is a list of the default VLAN for the different ports.



Default VLAN

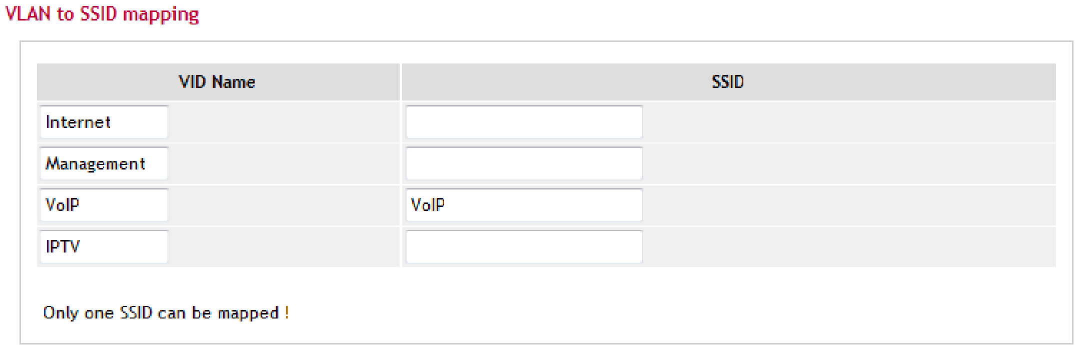
Port	Id
WAN	2
LAN 1	1
LAN 2	1
LAN 3	1
LAN 4	1
LAN 5	1
LAN 6	1
LAN 7	1

Port: This is the port the setting is applied to.

Id: This is the default VLAN id for the port. Incoming untagged packets will be given this id.

3.15.5 VLAN to SSID mapping

This allows to map a VLAN to an SSID.



VLAN to SSID mapping

VID Name	SSID
Internet	
Management	
VoIP	VoIP
IPTV	

Only one SSID can be mapped !

VID Name: The name of the VLAN you want to map.

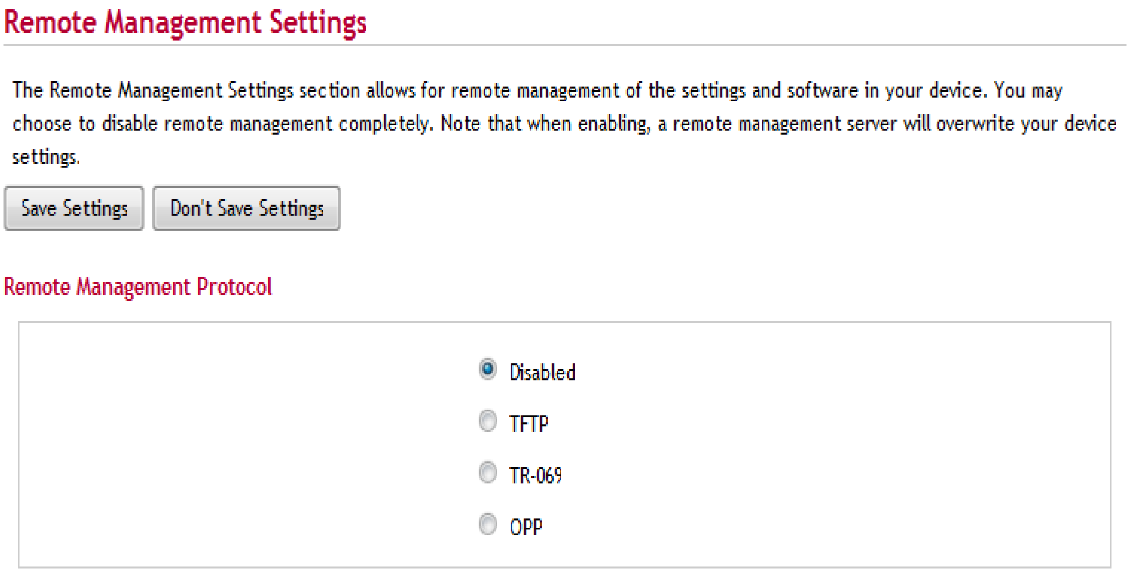
SSID: The SSID you want to map to the VLAN.

3.16 Provisioning

NB! These settings should never be touched by a regular end user (customer).

The provisioning section is used to configure the provisioning backend of the device. The primary responsibility of provisioning is to ensure quality and bug-free firmware. The integrated provisioning client will periodically check for any updates made by the server. The secondary responsibility is to provide automatic configuration for the device to establish connection with the service it belongs to. Such configurations are either network and connectivity type configurations (Example: NTP, STUN, SIP, service credentials etc) or application type configurations (Example: Priority level, Log level etc). This will involve things like access rights and privileges to ensure the security of a service provider's resources and user privacy. As a tertiary responsibility, it tries to reduce the amount of custom configuration by using group control, limiting single unit control, and special setups resulting in a radical decrease in the total number of configurations needed. Lastly, and most importantly, provisioning is used to reduce the service support burden for both the service provider and the end customer, enabling massive deployment of quality VoIP services.

NB! Any changes you make on any of these pages covered in this manual, may be overridden by provisioning if provisioning is enabled.



Remote Management Settings

The Remote Management Settings section allows for remote management of the settings and software in your device. You may choose to disable remote management completely. Note that when enabling, a remote management server will overwrite your device settings.

Remote Management Protocol

● Disabled
○ TFTP
○ TR-069
○ OPP

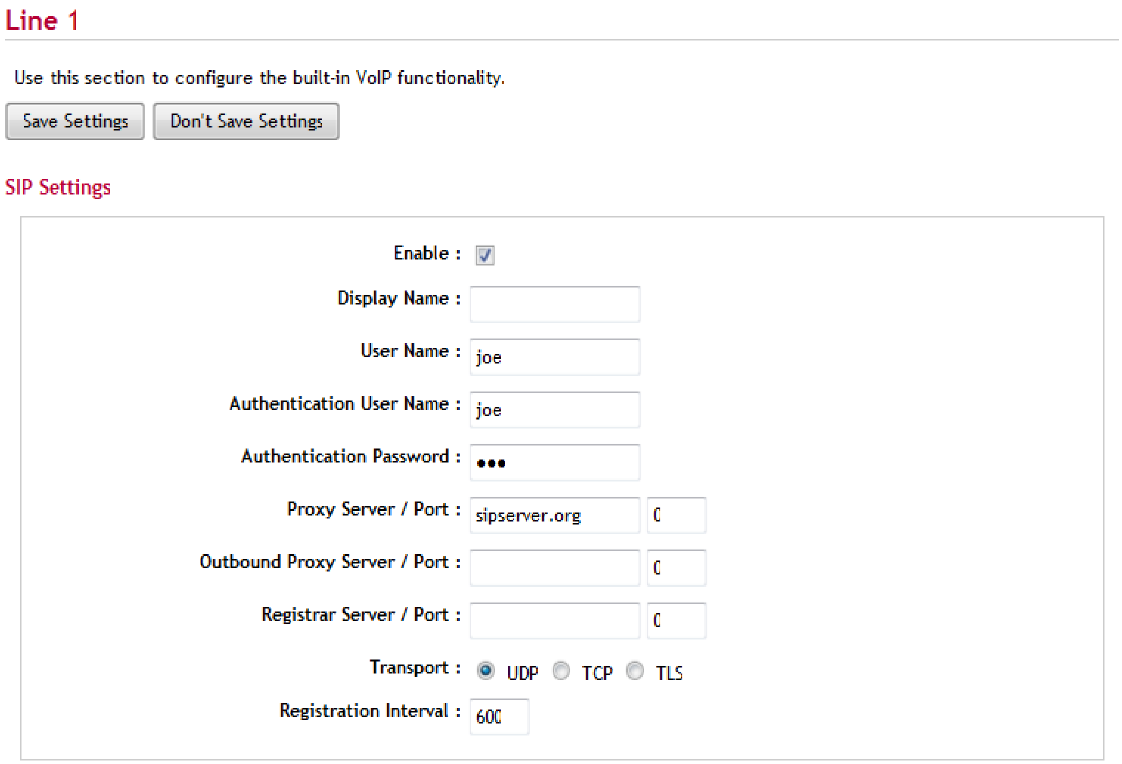
3.16.1 Three provisioning protocols

The device supports three provisioning protocols. TR-069 is the industry standard, while TFTP is the ‘old’ standard. OPP (Owera Provisioning Protocol) is a proprietary protocol developed by Owera. The settings here will enable the device to connect to a provisioning server and be provided with both configuration and firmware, as the provider seems fitting.

4 VoIP

SIP is the protocol used for opening, sustaining and closing IP telephony calls. In this section you can configure the built-in SIP functionality.

Note! Only the Line 1 SIP account settings is shown



Line 1

Use this section to configure the built-in VoIP functionality.

SIP Settings

Enable :	☑
Display Name :	
User Name :	joe
Authentication User Name :	joe
Authentication Password :	•••
Proxy Server / Port :	sipserver.org / 0
Outbound Proxy Server / Port :	/ 0
Registrar Server / Port :	/ 0
Transport :	● UDP ○ TCP ○ TLS
Registration Interval :	600

4.1 Line 1

The following descriptions also apply to the second SIP account (for setting up a second telephone service/ number).

4.1.1 SIP Settings

Enable this account: Enable/ Disable current account (account 1 or account 2).

Display Name: Enter display name. When you call someone, this is what will show on their display. Typically, this will be your public phone number.

User Name: Enter user name for current account (account 1 or account 2). Typically the same as **Authentication User**.

Authentication User: Enter Authentication User name for current account (account 1 or account 2). This is your user name with your service provider.

Authentication Password: Enter the password associated with the Authentication User for the current account (account 1 or account 2).

Proxy Server: Enter the URL or IP address of the desired SIP Server.

Proxy Port: Enter the specific port to connect to on the SIP Server, or use 0 (zero) for default.

Outbound Proxy Server: Enter the URL or IP address of the desired SIP Proxy. If you do not have an outbound proxy, do not enter anything for the **Registrar Server** either.

Outbound Proxy Port: Enter the specific port to connect to on the SIP Proxy, or use 0 (zero) for default.

Registrar Server: Enter the URL or IP address of the desired SIP Registrar.

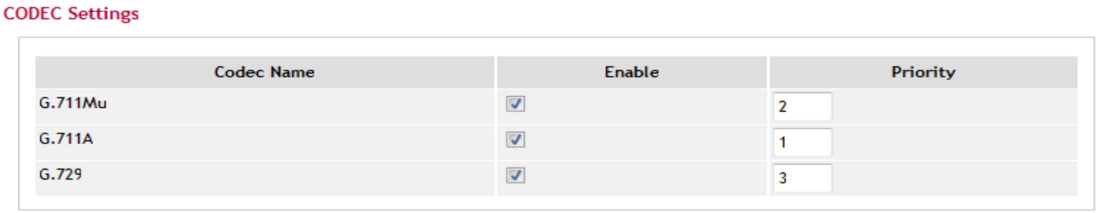
Registrar Port: Enter the specific port to connect to on the SIP Registrar, or use 0 (zero) for default.

Transport: Use this option to tell the SIP server, upon connection registration, whether you prefer inbound traffic on *UDP (User Datagram Protocol)* or on *TCP (Transmission Control Protocol)*. Default is UDP.

Registration Interval: Enter value (in seconds) for re-registering with the SIP server.

*Note! The value is set similar to the value the Service Provider specifies. However, the actual re-registering time will be **Registration Interval** divided by 2.*

4.1.2 Codec Settings



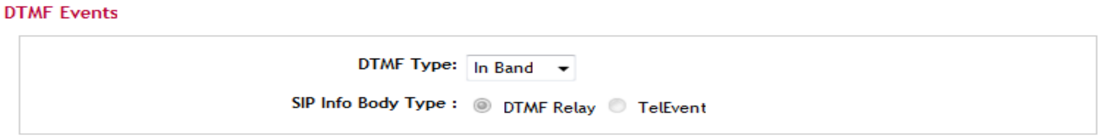
CODEC Settings

Codec Name	Enable	Priority
G.711Mu	☑	2
G.711A	☑	1
G.729	☑	3

Codec Priority: Set the priority of the different codecs relative to each other.

4.1.3 DTMF Events

These settings determine the communication protocol used between the RGW208EN and the SIP-server.



DTMF Events

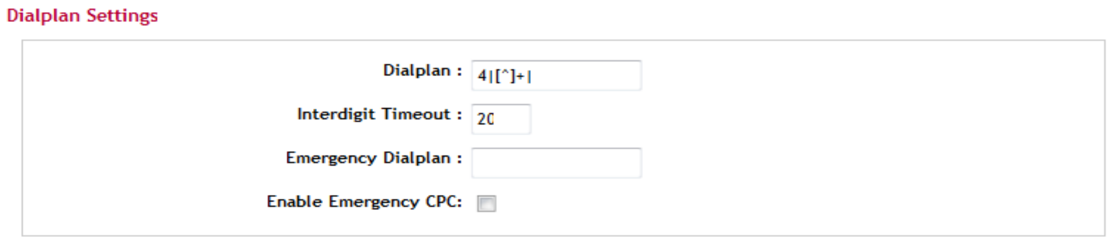
DTMF Type: In Band

SIP Info Body Type : ● DTMF Relay ○ TelEvent

DTMF type: Select type of *Dual-Tone Multi-Frequency (DTMF).* Please refer to RFC 2833 to gain an understanding of the IETF specified recommendations. Industry standard is RFC2833, InBand is the old protocol which may work if RFC2833 doesn't.

SIP INFO body type: Set whether *SIP INFO body type* should be *DTMF-Relay* or *Telephone-Event*. Default is *DTMF-Relay*. This determines the format of SIP INFO sent through a session. Please refer to RFC 2833 to gain an understanding of the IETF specified recommendations.

4.1.4 Dialplan Settings



Dialplan Settings

Dialplan : 4|[^]+|

Interdigit Timeout : 20

Emergency Dialplan :

Enable Emergency CPC: □

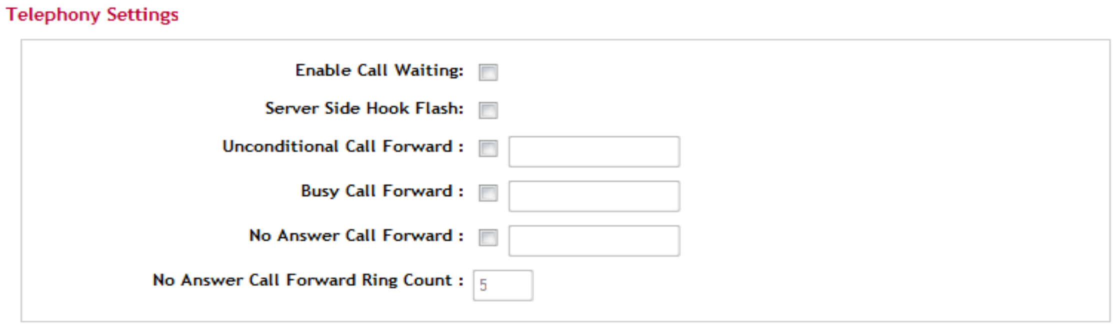
Dial plan: Enter a valid dial plan for your local environment (this is typically preconfigured by your Service Provider).

Interdigit Timeout: The time in seconds between key presses. If you exceed this timeout, the number entered so far will be dialed.

Emergency Dialplan: The area you live in might have special regulations when handling emergency numbers. These numbers are defined in this dialplan. If you are in doubt, do not change the default value.

Enable Emergency CPC: When in an emergency call, this prevents disruption of the line between you and the emergency center. If you are in doubt, do not change the default value.

4.1.5 Telephony Settings



Telephony Settings

Enable Call Waiting: □

Server Side Hook Flash: □

Unconditional Call Forward : □

Busy Call Forward : □

No Answer Call Forward : □

No Answer Call Forward Ring Count : 5

Enable Call Waiting: Enable/ Disable the *Call Waiting* feature. This feature lets you accept multiple calls simultaneously, placing the calls currently unattended to on hold.

Send Hook Flash: Enable/ Disable the *Hook Flash* button functionality on the phone.

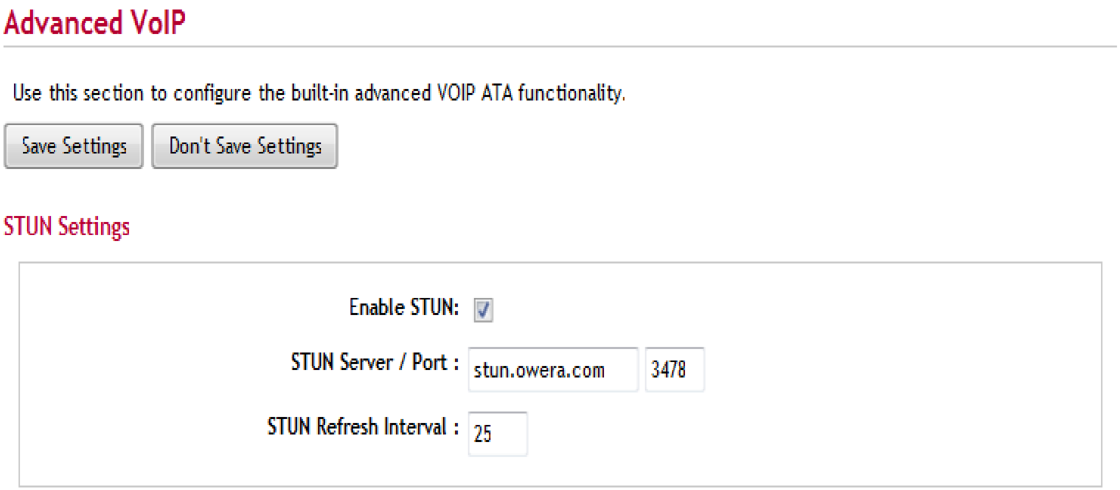
Unconditional Call Forward: An incoming call will be forwarded to this address in all cases. Your phone will not ring.

Busy Call Forward: If you are in a call and do not accept an incoming call (either call waiting is turned off, you deny the incoming call or you don't accept it), the call will be forwarded to this address.

No Answer Call Forward: If you do not pick up your phone, an incoming call will be forwarded to the address entered here after a timeout.

4.2 Advanced

4.2.1 STUN Settings



Advanced VoIP

Use this section to configure the built-in advanced VOIP ATA functionality.

STUN Settings

Enable STUN: ☑

STUN Server / Port : stun.owera.com 3478

STUN Refresh Interval : 25

STUN (Simple Traversal of UDP through NATs) is a network protocol used to set up UDP communication between two hosts, where one or both hosts are behind NAT routers.

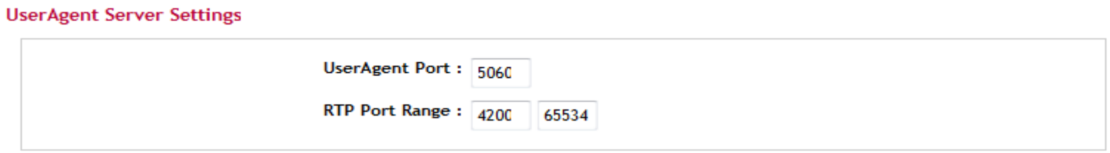
Enable STUN: Enable/ Disable the STUN Client. Note the **STUN Refresh** option below.

STUN Server: Enter the URL or IP address of the desired STUN server.

STUN Server Port: Enter the specific port to connect to the STUN server on.

STUN Refresh: Enter the refresh interval for connecting with STUN server. Note that if the value 0 (zero) is entered, **STUN is also disabled** even if **Enable STUN** is set/toggled.

4.2.2 User Agent Server Settings



UserAgent Server Settings

UserAgent Port : 5060

RTP Port Range : 4200 65534

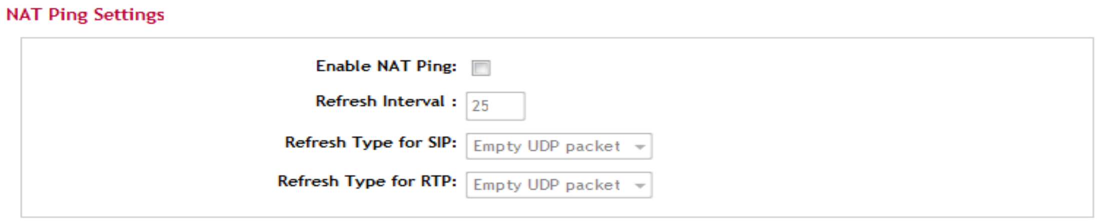
UserAgent Port: Defaults to 5060

Local RTP port range (min – max): Enter the port range for reception of RTP media. The device will increment the port number with 2 for each RTP session. Enter 0 (zero) in either field for automatic assignment.

4.2.3 NAT Ping Settings

The NAT Ping client communicates with the SIP server at a specified interval, keeping the connection to the SIP server open. This is useful if the RGW208EN connects to the SIP server through an upstream NAT router, either on your local network, or in some cases at your ISP.

Note: The SIP server must support this feature in order for it to work. Using a STUN client is therefore more common.



NAT Ping Settings

Enable NAT Ping: □

Refresh Interval : 25

Refresh Type for SIP: Empty UDP packet

Refresh Type for RTP: Empty UDP packet

Enable NAT PING: Enable/ Disable the *NAT ping client*. Note the **NAT PING Refresh** option below.

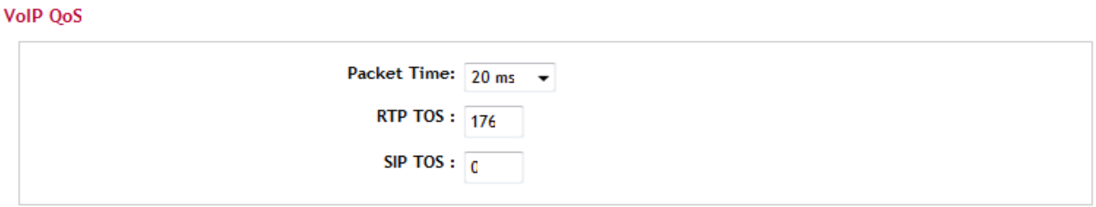
NAT PING Refresh: Enter the refresh interval for communicating with the SIP server. Note that if the value 0 (zero) is entered, **NAT ping is also disabled** even if **Enable NAT PING** is set/ toggled.

Refresh Type for SIP: None disables NAT Ping for SIP. Empty UDP packet enables sending of empty UDP packets to the SIP server. SIP Ping message enables sending of SIP Ping messages, and performing SIP Re-Register on failure (used with some Nortel servers).

Refresh Type for RTP: None disables NAT Ping for RTP. Empty UDP packet enables sending of empty UDP packets to the remote RTP peer.

4.2.4 VoIP QoS

This section contains advanced options for configuring *Quality of Service (QoS).*



VoIP QoS

Packet Time: 20 ms

RTP TOS : 176

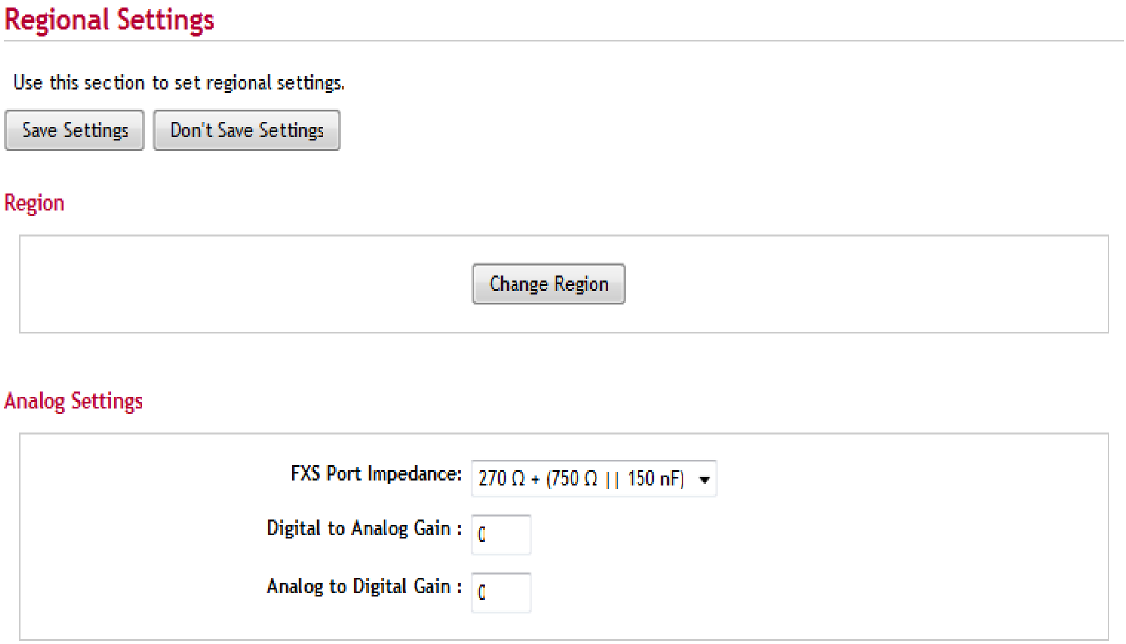
SIP TOS : 0

Packet Time: How often packets are sent by the codec. This is highly critical and you should not change the default value.

RTP TOS value: Select the *Type of Service (ToS)* value to assign to outbound RTP packets. This value determines the priority the packets will be given at routers between you and your recipient, if any. The value should either be given to you by your SIP service provider or leave them as set per default. You might have unexpected results if you change these values at will.

SIP TOS value: Select the *Type of Service (ToS)* value to assign to outbound SIP packets. This value determines the priority the packets will be given at routers between you and your recipient, if any. The value should either be given to you by your SIP service provider or leave them as set per default. You might have unexpected results if you change these values at will.

4.3 Regional Settings



Regional Settings

Use this section to set regional settings.

Region

Analog Settings

FXS Port Impedance: 270 Ω + (750 Ω || 150 nF)

Digital to Analog Gain : 0

Analog to Digital Gain : 0

4.3.1 Region

By changing the region (country), many settings on this page will be set automatically.

4.3.2 Analog Settings

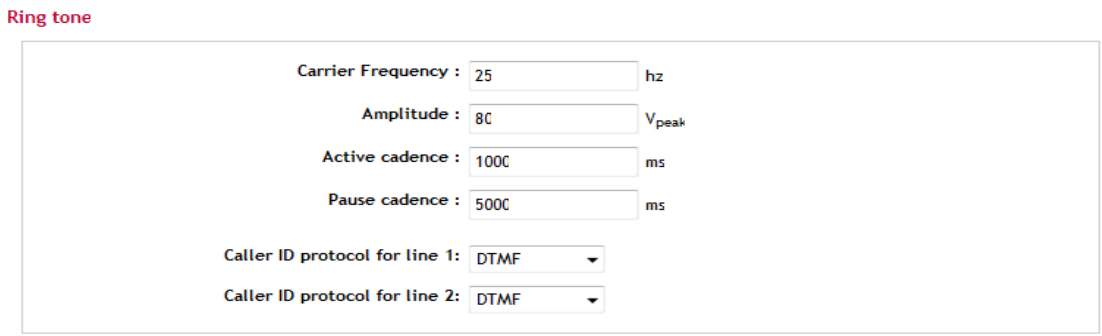
FXS Port Impedance:

Digital to Analog Gain:

Analog to Digital Gain:

4.3.3 Ring tone

This contains setting for the ring tone.



Ring tone

Carrier Frequency :	25	hz
Amplitude :	80	V_{peak}
Active cadence :	1000	ms
Pause cadence :	5000	ms
Caller ID protocol for line 1:	DTMF	
Caller ID protocol for line 2:	DTMF	

Carrier Frequency: The carrier frequency of the ring tone.

Amplitude: The amplitude in V_{peak} of the ring tone.

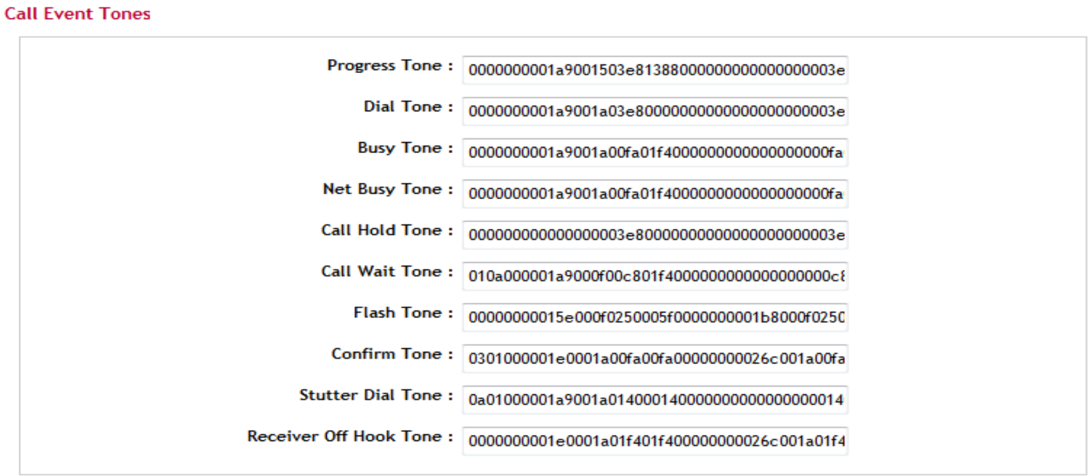
Active cadence: How long the active part of the ring tone will last, in ms.

Pause cadence: How long the silent part of the ring tone will last, in ms.

Caller ID protocol for line 1&2: Depending upon the phone connected the ATA, the protocol for showing the numbers in the phone display varies. FSK ETSI is the industry standard (used by most modern phones), while DTMF is the old standard which might work for older phones.

4.3.4 Call Event Tones

This is the tones for the different events. This is in a binary format and should not be edited by hand. Use the Change Region button if you want another set of tones.



Call Event Tones

Progress Tone :	0000000001a9001503e81388000000000000000000003e
Dial Tone :	0000000001a9001a03e8000000000000000000000003e
Busy Tone :	0000000001a9001a00fa01f4000000000000000000fa
Net Busy Tone :	0000000001a9001a00fa01f4000000000000000000fa
Call Hold Tone :	000000000000000003e8000000000000000000000003e
Call Wait Tone :	010a000001a9000f00c801f40000000000000000000c8
Flash Tone :	00000000015e000f0250005f0000000001b8000f0250
Confirm Tone :	0301000001e0001a00fa00fa00000000026c001a00fa
Stutter Dial Tone :	0a01000001a9001a0140001400000000000000000014
Receiver Off Hook Tone :	0000000001e0001a01f401f400000000026c001a01f4

Progress Tone: This tone will be played while you are waiting for the receiver to pick up the phone.

Dial Tone: This tone informs you that everything is ready and you can start dialing.

Busy Tone: This tone will be played if the receiver is already in a call.

Net Busy Tone: This tone will be played if there is something wrong with the connection.

Call Hold Tone: This tone will be played if your call has been placed on hold.

Call Wait Tone: This tone will be played if there is an incoming call while you're already in a call.

Flash Tone: Useful description goes here.

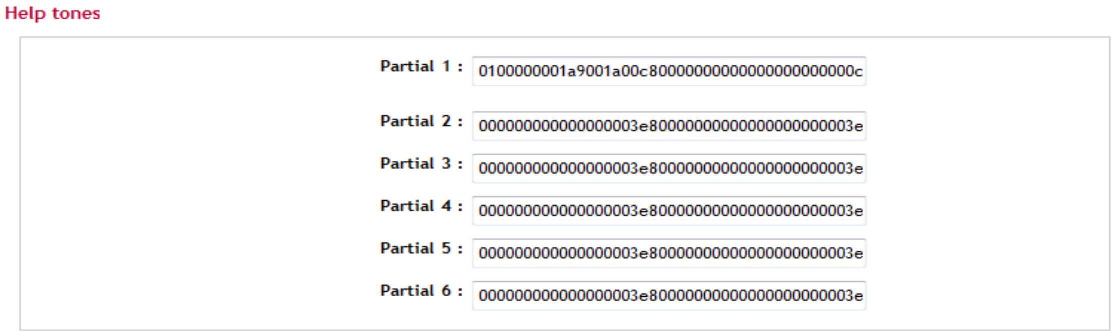
Confirm Tone: Useful description goes here.

Stutter Dial Tone: This tone will be played if there is any special conditions applied to the call.

Receiver Off Hook Tone: This tone will be played if the phone is left off hook for longer periods of time.

4.3.5 Help Tones

This is the some extra tones which is used to build up larger ring tones. You probably do not want to edit them.



Help tones

Partial 1 : 0100000001a9001a00c80000000000000000000000c

Partial 2 : 000000000000000003e80000000000000000000003e

Partial 3 : 000000000000000003e80000000000000000000003e

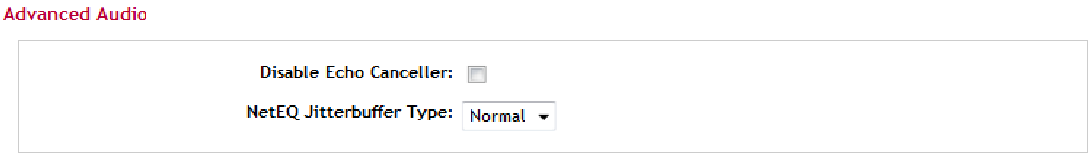
Partial 4 : 000000000000000003e80000000000000000000003e

Partial 5 : 000000000000000003e80000000000000000000003e

Partial 6 : 000000000000000003e80000000000000000000003e

4.3.6 Advanced Audio

This section contains advanced options for configuring audio settings and quality.
Advanced Audio



Advanced Audio

Disable Echo Canceller: □

NetEQ Jitterbuffer Type: Normal ▾

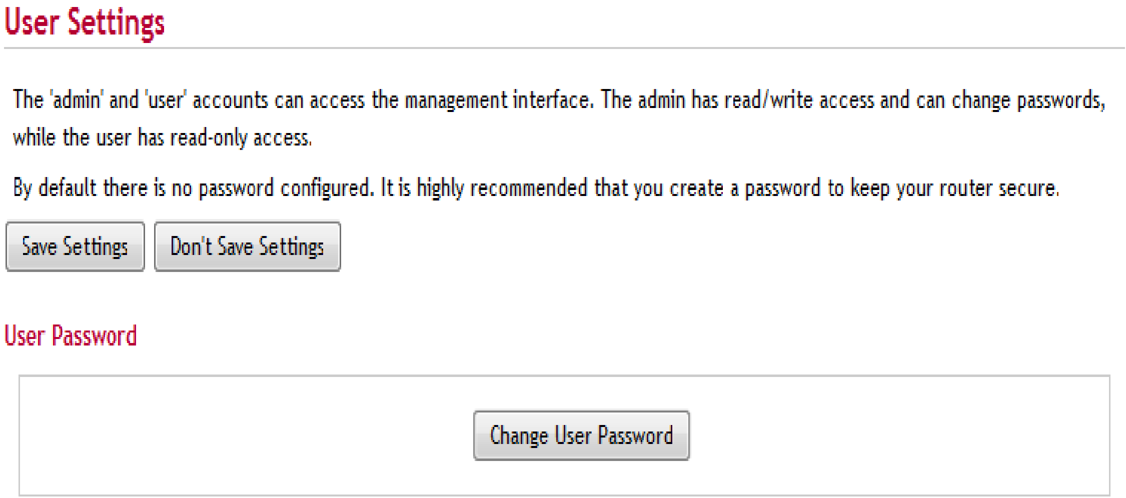
Disable Echo Canceller: This will disable the echo canceller.

NetEQ Jitterbuffer Type: Choose between Normal, Off and Fax.

5 Tools

The Tools section contains options for configuring router passwords, timezone settings, logging functions, schedules and other system parameters.

5.1 User



User Settings

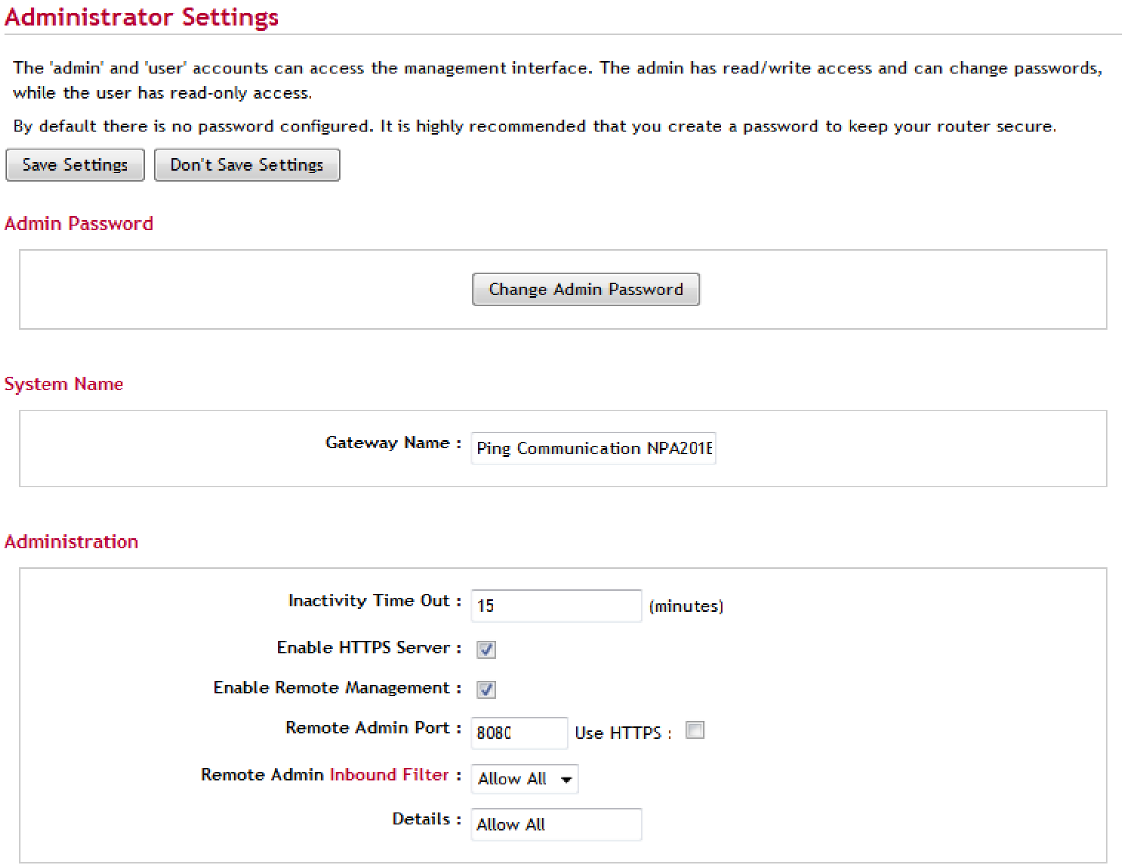
The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

User Password

Here you can set a password for the *User* user. The *User* user has read only access and may not change the passwords in the device.

5.2 Admin



Administrator Settings

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

Admin Password

System Name

Gateway Name : Ping Communication NPA201E

Administration

Inactivity Time Out : 15 (minutes)

Enable HTTPS Server : ☑

Enable Remote Management : ☑

Remote Admin Port : 8080 Use HTTPS : □

Remote Admin Inbound Filter : Allow All

Details : Allow All

5.2.1 Admin Password

Here you can set a password for the *Admin* user. The *Admin* user has full read/ write access to change the passwords in the device.

Password: Enter a password that will grant access to the Web-based management interface. (Note. Should not be used if testing and trying out the device. Use only if necessary)

5.2.2 System name

Gateway Name: The name of the router can be set here. Default value is *Owera VoIP-Gateway.*

5.2.3 Administration

This section contains options for configuring management and remote management for the device, secure or otherwise.

Inactivity Time Out: The number of minutes without activity before the web session on this interface is closed.

Enable HTTPS Server: If you want a secure connection to this web interface, enable this option.

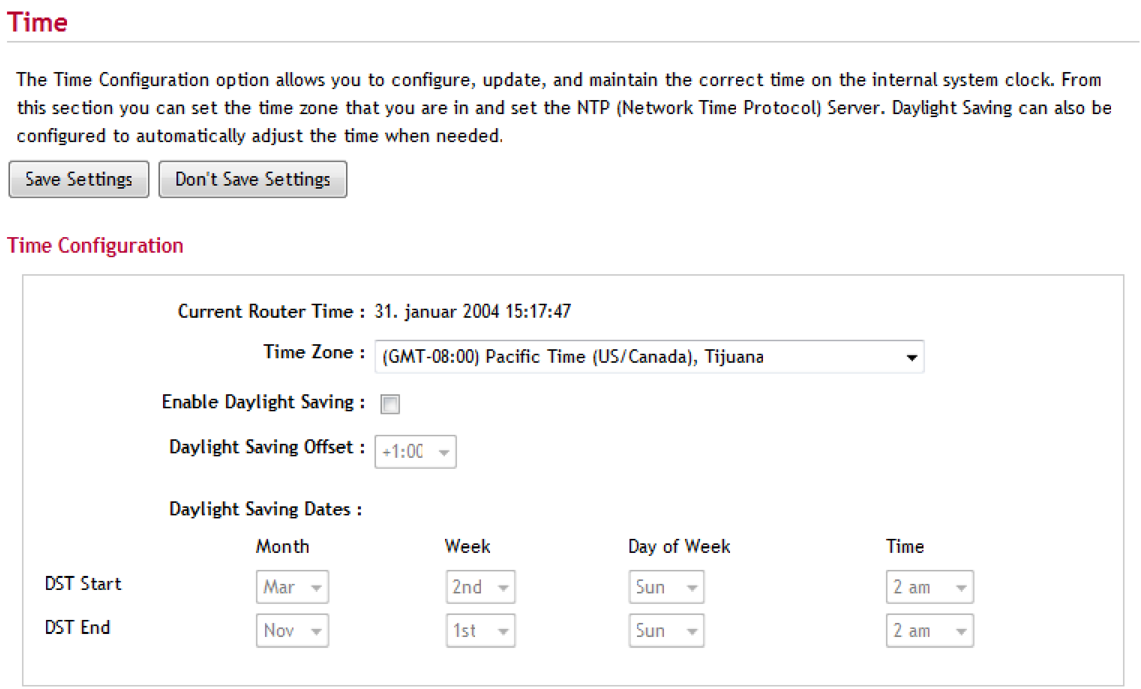
Enable Remote Management: If you want to reach this web interface from WAN side, enable this option.

Remote Admin Port: Decide which port to access the web interface

Remote Admin Inbound Filter: Specify a filter (which can be created under Advanved -> Inbound Filter) to control access to the web interface.

5.3 Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.



Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time Configuration

Current Router Time : 31. januar 2004 15:17:47

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Enable Daylight Saving : □

Daylight Saving Offset : +1:0C

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Mar	2nd	Sun	2 am
DST End	Nov	1st	Sun	2 am

Time Configuration

Current Router Time: This field displays the time currently maintained by the router. If this is not correct, use the following options to configure it correctly.

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

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

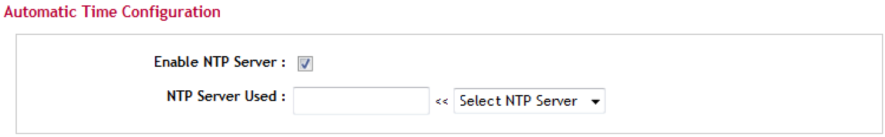
Daylight Saving Offset: Select the time offset if your location observes daylight saving time.

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."

Automatic Time Configuration

This section contains options for configuring the router's *Network Time Server* functionality.



Automatic Time Configuration

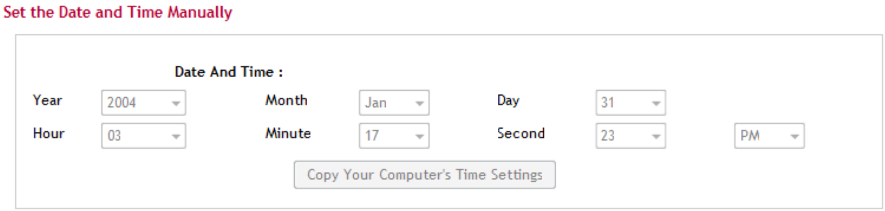
Enable NTP Server : ☑

NTP Server Used : << Select NTP Server

Enable NTP Server: Select this option if you want to synchronize the router's clock 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.

Set the Date and Time



Set the Date and Time Manually

Date And Time :

Year	2004	Month	Jan	Day	31	
Hour	03	Minute	17	Second	23	PM

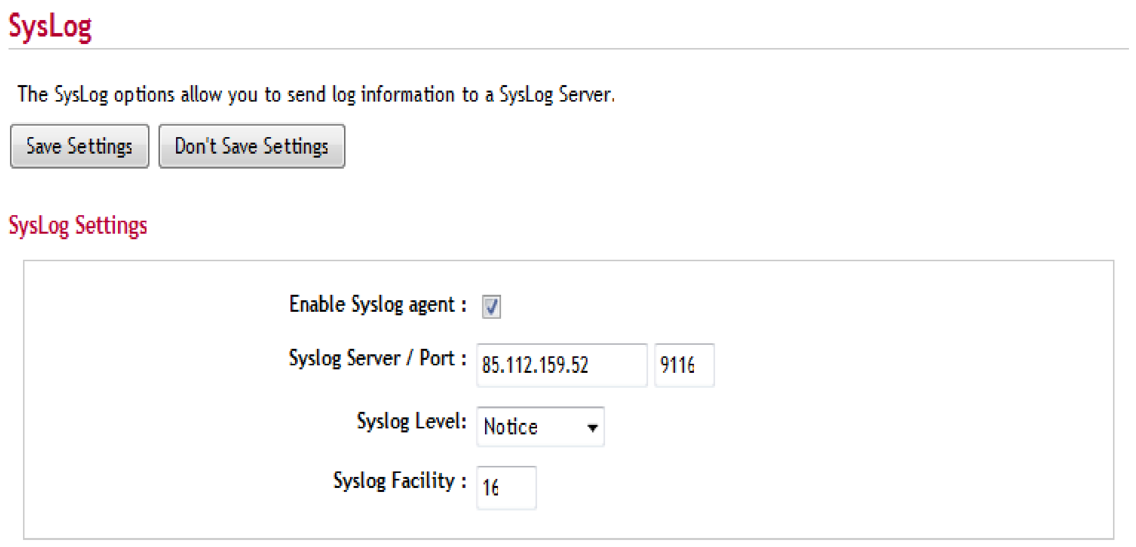
Copy Your Computer's Time Settings

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 (Note: Be sure the computer’s time is set correctly).

Note: If the router loses power for any reason, it cannot keeps its clock running and will not have the correct time when it is started again. To maintain the 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.

5.4 Syslog

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



SysLog

The SysLog options allow you to send log information to a SysLog Server.

SysLog Settings

Enable Syslog agent : ☑

Syslog Server / Port : 85.112.159.52 9116

Syslog Level: Notice

Syslog Facility : 16

Enable Syslog Agent: Enable this option to output the router logs to a Syslog Server.

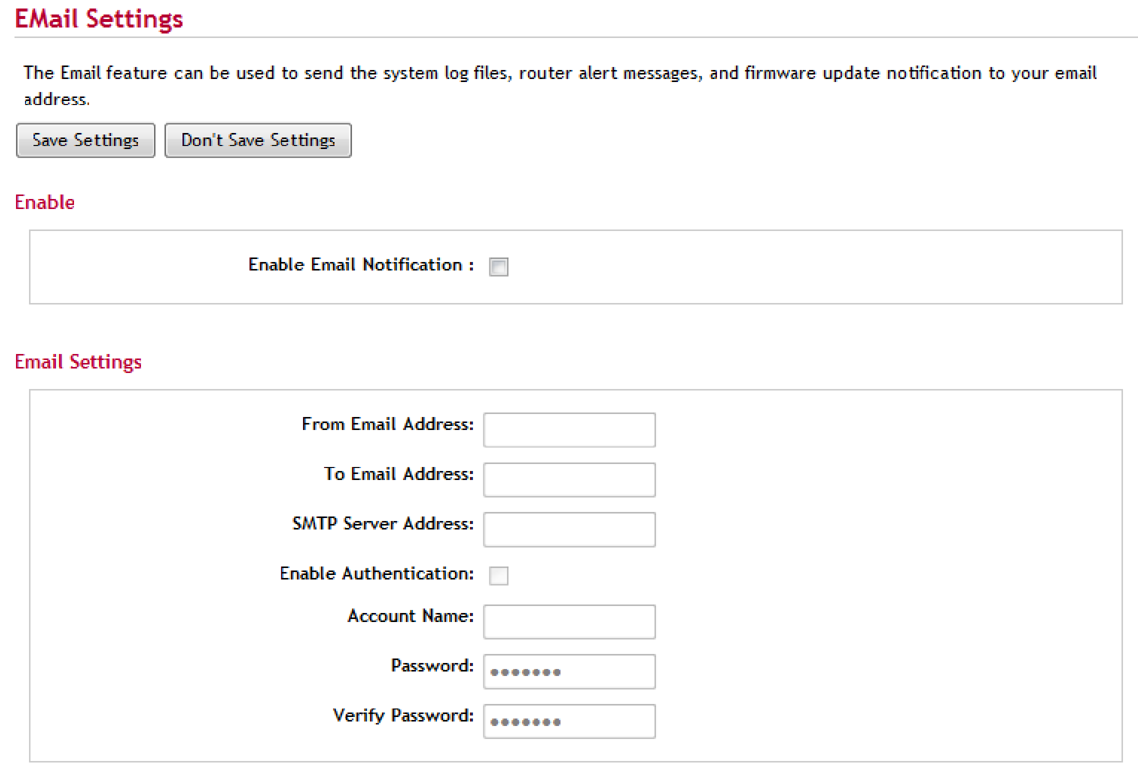
Syslog Server IP Address/Port: Enter the LAN IP address of the Syslog Server and the port number.

Syslog Level: Decide the lowest level to trigger a syslog message to be sent to the server. Setting the log level to DEBUG will cause a massive amount of log messages to the server.

Syslog Facility: Leave this field to 16, only to be changed if testing a Syslog Server.

5.5 Email settings

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



EMail Settings

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

Enable

Enable Email Notification : □

Email Settings

From Email Address:

To Email Address:

SMTP Server Address:

Enable Authentication: □

Account Name:

Password: •••••••

Verify Password: •••••••

5.5.1 Email Settings

Enable Email Notification: When this option is enabled, router activity logs are e-mailed to a designated email address, displaying the following parameters.

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.

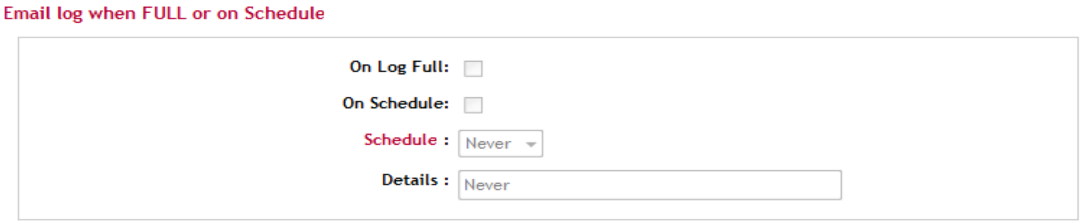
Enable Authentication: If your SMTP server requires authentication, select this option.

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 for verification.

Email Log When Full or on Schedule



Email log when FULL or on Schedule

On Log Full:	□
On Schedule:	□
Schedule :	Never
Details :	Never

On Log Full: When this option is selected, logs will be sent via email when the log is full.

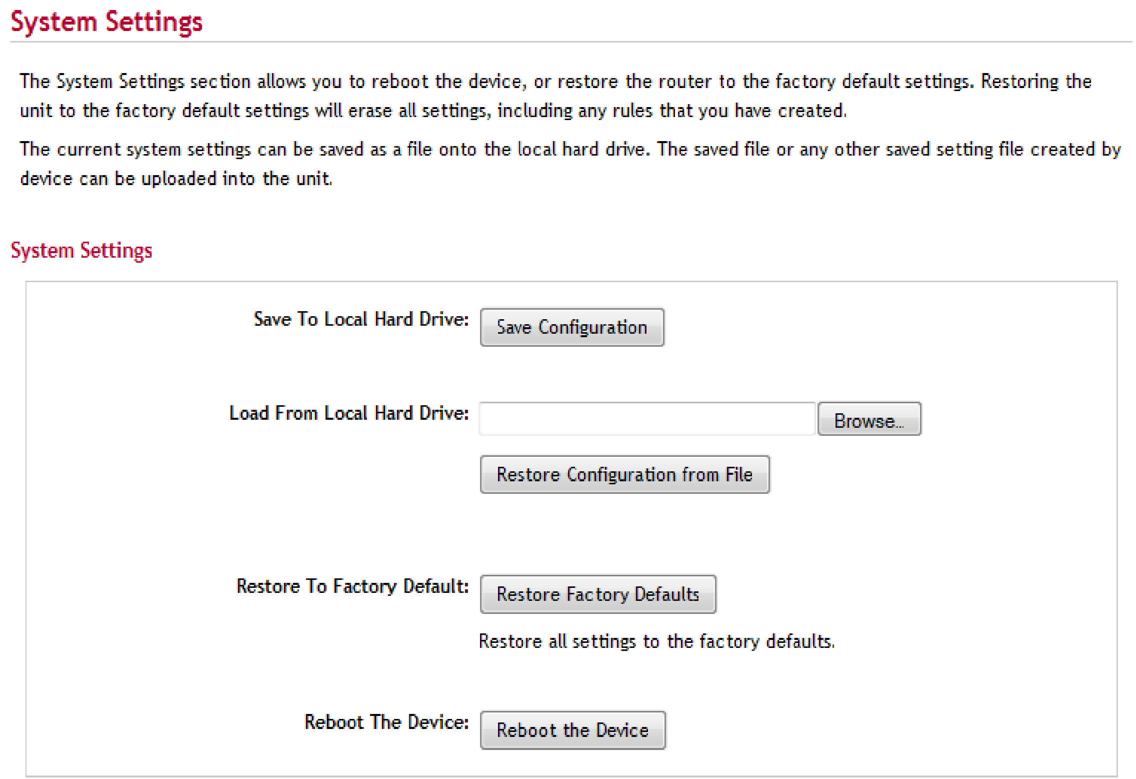
On Schedule: Selecting this option will send the logs via email according to a schedule.

Schedule: This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to Tools > Schedules.

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 additional emails to be sent.

5.6 System

The System Settings section allows you to reboot the device or 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've created.



System Settings

The System Settings section allows you to reboot the device, or 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.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

System Settings

Save To Local Hard Drive:
Save Configuration
Load From Local Hard Drive:
Browse...
Restore Configuration from File
Restore To Factory Default:
Restore Factory Defaults

Restore all settings to the factory defaults.

Save Settings To Local Hard Drive: 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.

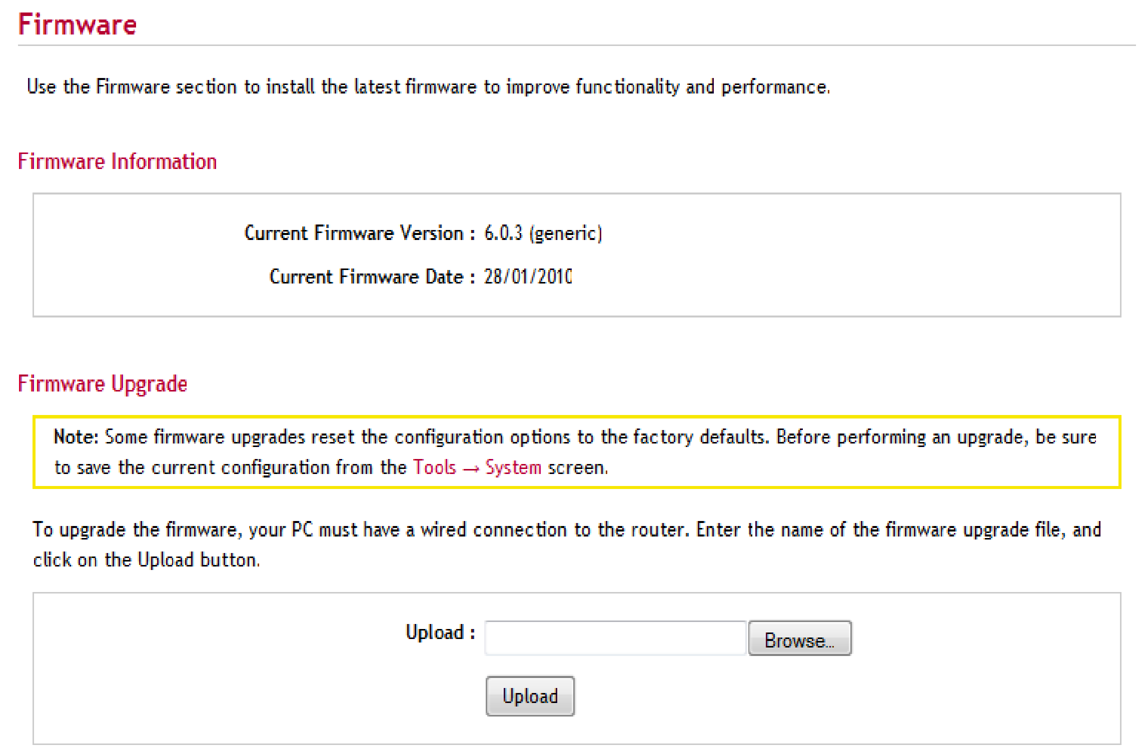
Load From Local Hard Drive: Use this option to restore previously saved router configuration settings.

Restore all Settings to the Factory Defaults: This option will restore all configuration settings back to the factory defaults. Any settings that have not been saved will be lost. If you want to save your router configuration settings, use the **Save Settings** option above.

Reboot the Device: This will restart the router. Useful for restarting when you are not near the device.

5.7 Firmware

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



Firmware

Use the Firmware section to install the latest firmware to improve functionality and performance.

Firmware Information

Current Firmware Version : 6.0.3 (generic)

Current Firmware Date : 28/01/2010

Firmware Upgrade

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the Tools → System screen.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

To upgrade the firmware, follow these steps:

1. Click the **Browse** button to locate the RGW208EN 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 can take another minute or more.
4. Confirm updated firmware revision on status page.

5.7.1 Firmware Information

This section displays the Current Firmware Version and the Latest Firmware Version. To verify the latest firmware version, the gaming router checks the Internet.

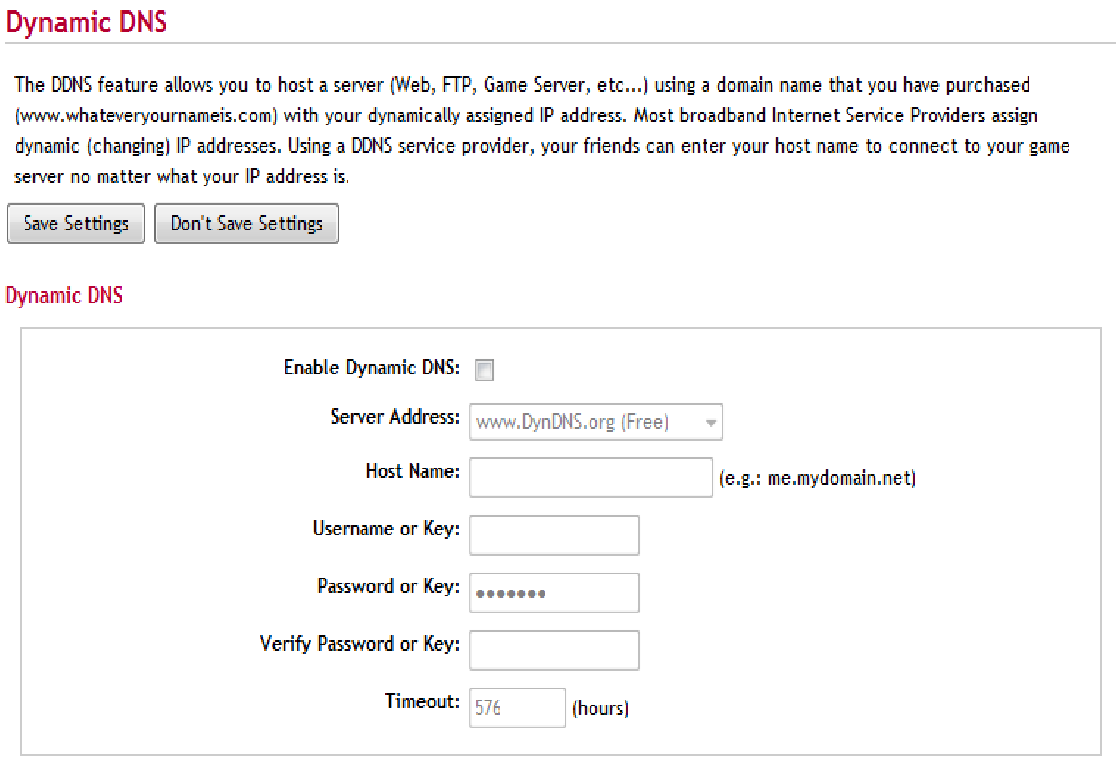
5.7.2 Firmware Upgrade

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the *Tools* -> *System* 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.

5.8 Dynamic DNS

The DDNS 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. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.



Dynamic DNS

The DDNS 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. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Dynamic DNS

Enable Dynamic DNS:	□
Server Address:	www.DynDNS.org (Free)
Host Name:	(e.g.: me.mydomain.net)
Username or Key:	
Password or Key:	•••••••
Verify Password or Key:	
Timeout:	576 (hours)

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, fully qualified. For example: `myhost.mydomain.net`

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.

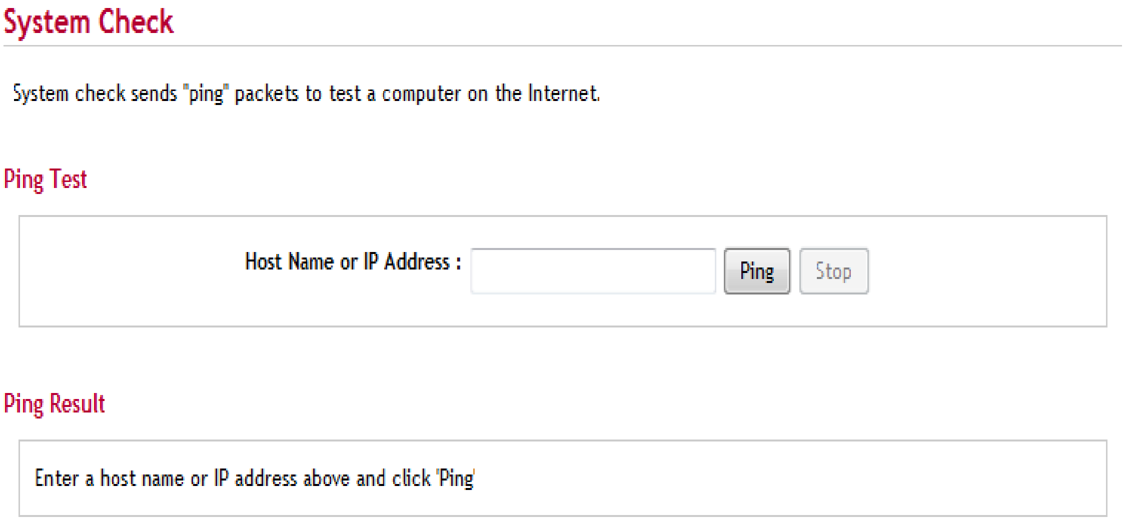
Timeout: The time between periodic updates to the Dynamic DNS, if your dynamic IP address has not changed. The timeout period is entered in hours.

Note: 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: 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 a virtual server.*

5.9 System Check

This section contains options to *Ping* a host.



System Check

System check sends "ping" packets to test a computer on the Internet.

Ping Test

Host Name or IP Address :

Ping Result

Enter a host name or IP address above and click 'Ping'

5.9.1 Ping Test

"Ping" is an Internet utility function that sends a series of short messages to a target computer and reports the results. You can use it to test whether a computer is running, and to get an idea of the quality of the connection to that computer, based on the speed of the responses.

Host Name or IP Address: Enter the IP address or the fully qualified host name of the target computer.

Ping: Start Pinging the specified host.

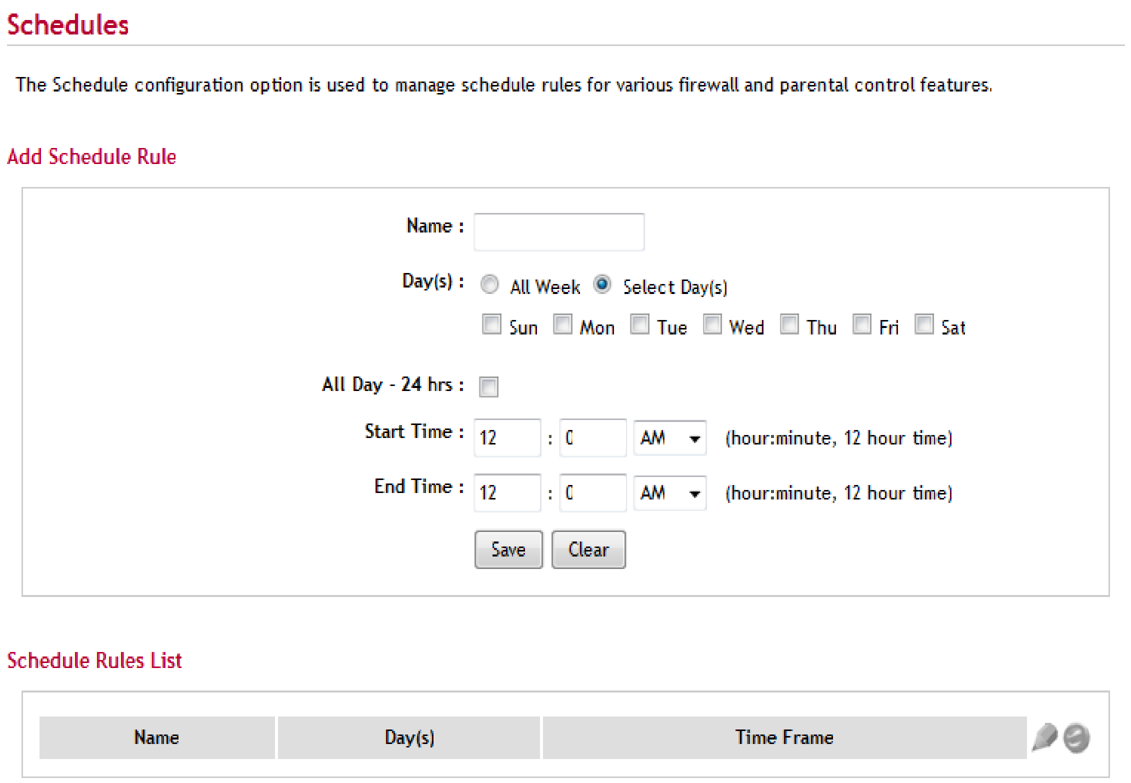
Stop: The host is Pinged repeatedly until you press this button.

5.9.2 Ping Result

The results generated by the *Ping Test* will be displayed continuously here.

5.10 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.



Schedules

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

Add Schedule Rule

Name :	
Day(s) :	○ All Week ● Select Day(s) □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day - 24 hrs :	□
Start Time :	12 : 0 AM (hour:minute, 12 hour time)
End Time :	12 : 0 AM (hour:minute, 12 hour time)
	Save Clear

Schedule Rules List

Name	Day(s)	Time Frame

5.10.1 Add/Edit Schedule Rule

Schedule 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: Select this option if you want this schedule in effect all day for the selected day(s).

Start Time: If you do not use the **All Day** option, enter the desired 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 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 used for email events.

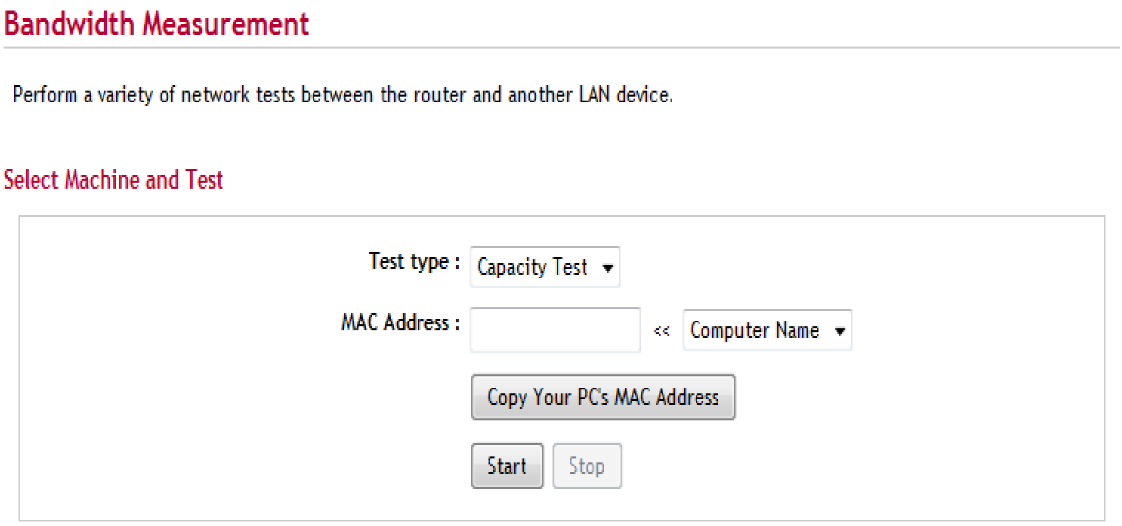
Save: Saves the new or modified *Schedule* in the **Schedule Rules List**. When you are done editing the settings, you must click the *Save Settings* button at the top of the page to make the changes effective and permanent.

5.10.2 Schedule Rules List

This 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. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

5.11 Bandwidth

The Bandwidth Measurement page uses the Link Layer Topology and Discover (LLTD) protocol to measure the bandwidth between the access point and LAN or WLAN devices that support LLTD. LLTD support is included in many end-point devices, including PCs, Xbox, Ubicom based digital picture frames, Ubicom based routers, etc.



Bandwidth Measurement

Perform a variety of network tests between the router and another LAN device.

Select Machine and Test

Test type : Capacity Test

MAC Address :

Test Type:

Capacity Test: Uses packet transit time to measure the latency introduced between packets, and uses that information to estimate the available bandwidth. The test transmits small packets at wide intervals to minimize competition with other LAN traffic.

Flood Test: Transmits an increasingly large number of packets to find the point at which the network starts to drop packets, then backs off and provides an estimate of the packet rate that is just below the maximum and does not introduce packet loss. This test will actually compete with other traffic on the LAN.

MAC Address: Enter the MAC Address of the LAN machine you want to use for testing. You can also choose the LAN machine from the drop-down list of known machines, or you can select the machine you are currently using by clicking the button Copy Your Machine's MAC Address. Make sure that the selected LAN machine supports the LLTD protocol.

Start: Start running the test. The router exchanges packets with the machine whose MAC Address you specified. The test will fail if the target machine does not support the LLTD protocol.

Stop: The test runs until you stop it. Let the test run for a few minutes. When the results seem to have stabilized, click this button to end the test.

Results When you start the test, the results appear in this area of the screen.

Reference Values: The first several bars in the results table are the reference values against which you can compare the measured results. Each bar represents the typical bandwidth usage of a specific type of media stream.

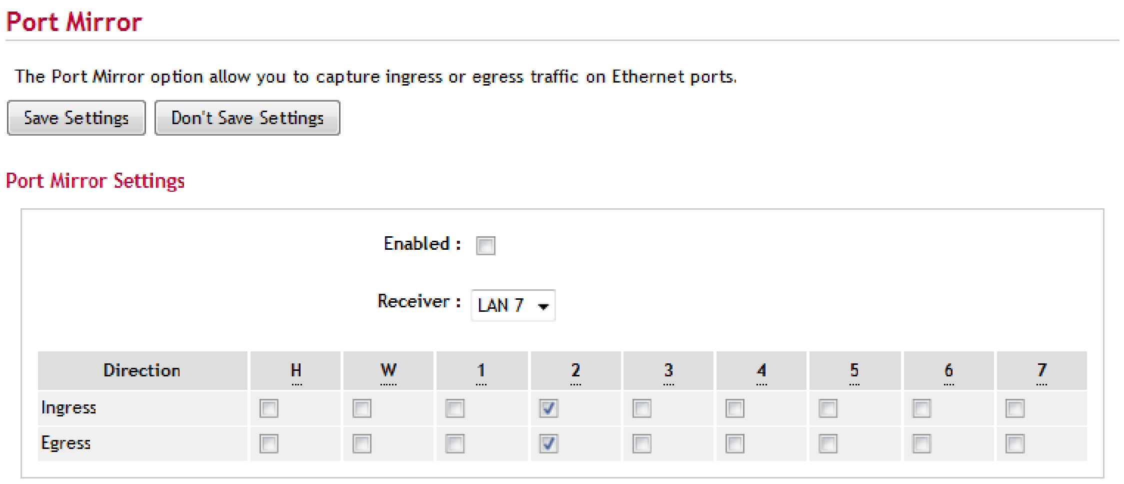
Digital Music
Internet VOD (Video on Demand)
Satellite TV (Standard definition)
HDTV Broadcast
Measured Results

Compare the measured results to the reference values to discover what kinds of media can travel over this link without degradation.

Link Capacity: The bar shows the measured capacity of the link between the access point and the specified LAN machine, using the same scale as the reference bars.

Link Drop Rate: The Flood Test also displays the measured drop rate. The Link Drop Rate is a measure of packets that are lost when the Flood Test tries to increase the volume of packets beyond the capacity of the link. The changing values of Link Drop Rate serve as an indicator of test activity.

5.12 Mirror



Port Mirror

The Port Mirror option allow you to capture ingress or egress traffic on Ethernet ports.

Port Mirror Settings

Enabled : ☐

Receiver : LAN 7

Direction	H	W	1	2	3	4	5	6	7
Ingress	☐	☐	☐	☑	☐	☐	☐	☐	☐
Egress	☐	☐	☐	☑	☐	☐	☐	☐	☐

The Port Mirror option allows you to capture ingress or egress traffic on Ethernet ports.

Enabled: Enables the port mirror.

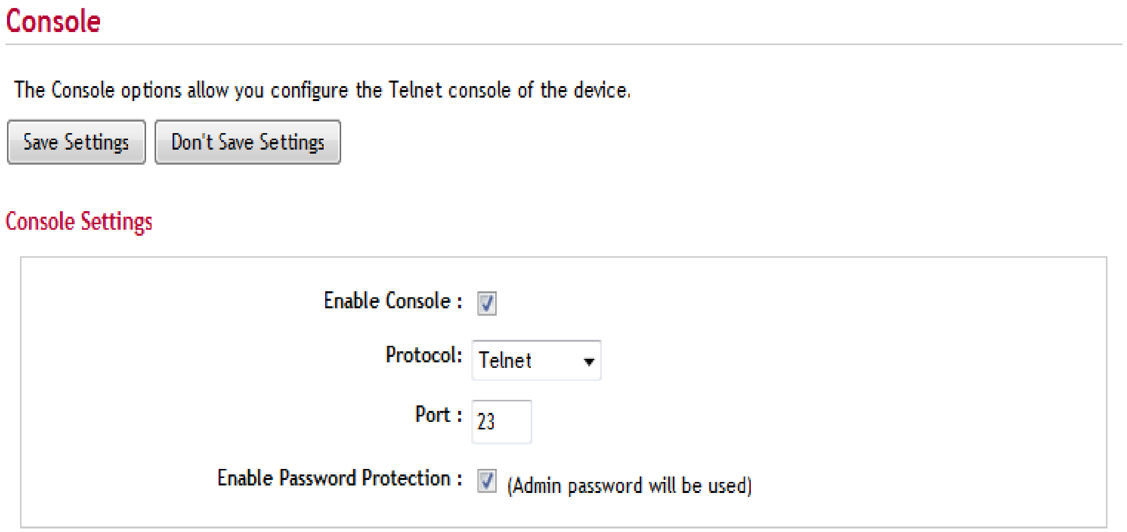
Receiver: The port which the captured data gets sent to.

Ingress: Capture the incoming packets from the selected port.

Egress: Capture the outgoing packets from the selected port.

The letter H is short Host, which is internal traffic in the router. This is only useful for debugging. The letter W is short for WAN, so you can mirror in/out to the internet. The digits 1-7 denotes the LAN-ports.

5.13 Console



Console

The Console options allow you configure the Telnet console of the device.

Console Settings

Enable Console : ☑

Protocol: Telnet

Port : 23

Enable Password Protection : ☑ (Admin password will be used)

The Console options allow you configure the Telnet console of the device.

Enabled Console: Enables the console server.
Protocol: Here you can choose between regular Telnet and encrypted Telnet/TLS.
Port: This is the port the console server will listen to.
Enable Password Protection: Enabling this will make the server ask for a password. This will correspond to the password used for the Admin account on the web interface.

Example:

Command Line

```
telnet-ssl -z ssl 192.168.0.1
```

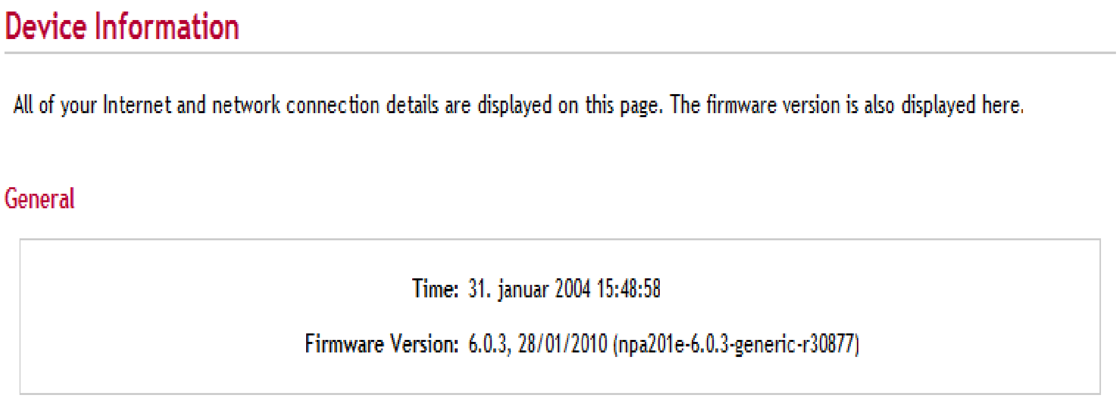
Output

```
Welcome to Foobar

Enter 'h [command]' or 'help [command]' for command info.

help, h - This help menu
version - Version
call    - Console dialing menu
system  - System menu
media   - Media / Voice / RTP menu
ua      - SIP UserAgent menu
eth     - Ethernet menu
fxs     - FXS menu
prov    - Provisioning menu
hw      - Hardware access
reboot  - Reboot the system
rstcfg  - Restore default configuration
quit, q - Quit console
>
```

6 Status

The Status items are mainly informational.

6.1 Device Info



Device Information

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

General

Time: 31. januar 2004 15:48:58

Firmware Version: 6.0.3, 28/01/2010 (npa201e-6.0.3-generic-r30877)

All of your Internet and network connection details are displayed on the Device Info page. The firmware version is also displayed here.

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.

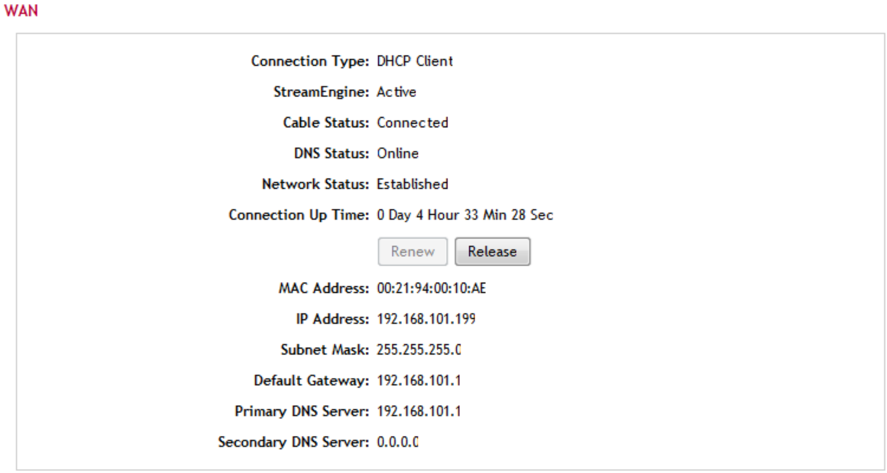
6.1.1 General

Time: Displays the time and date that the router is set to.

Firmware Version: Displays the currently loaded firmware version.

6.1.2 WAN

Displays information about your Internet connection. Depending on the WAN connection mode, you can take one of the following sets of actions:


WAN

Connection Type: DHCP Client

StreamEngine: Active

Cable Status: Connected

DNS Status: Online

Network Status: Established

Connection Up Time: 0 Day 4 Hour 33 Min 28 Sec

MAC Address: 00:21:94:00:10:AE

IP Address: 192.168.101.199

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.101.1

Primary DNS Server: 192.168.101.1

Secondary DNS Server: 0.0.0.0

Connection Type: The Internet connection type that is being used.

StreamEngine: Tells whether or not this feature is active

Cable Status: Displays whether the network cable is connected or disconnected.

Network Status: Displays whether the network has been established.

Connection Up Time: If a connection has been successfully established, this field displays how long the connection has been active.

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.

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.

MAC Address: The MAC address that is seen over the Internet.

IP Address: The IP address being used on the WAN port.

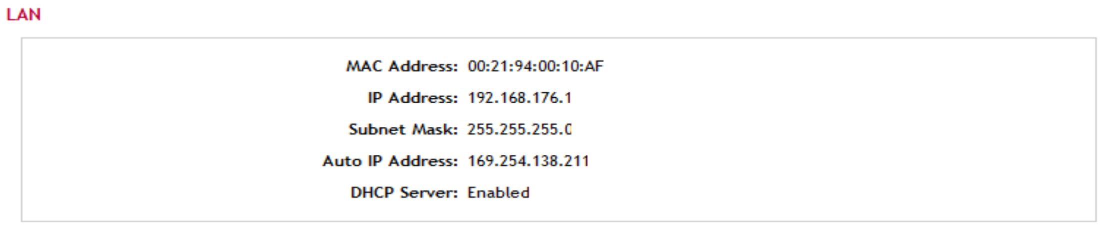
Subnet Mask: The subnet mask used on the WAN port.

Default Gateway: The default gateway of the WAN port.

Primary DNS Server: The Primary DNS Server address.

Secondary DNS Server: The Secondary DNS Server address.

6.1.3 LAN



LAN

MAC Address: 00:21:94:00:10:AF

IP Address: 192.168.176.1

Subnet Mask: 255.255.255.0

Auto IP Address: 169.254.138.211

DHCP Server: Enabled

MAC Address: The MAC address displayed for your local area network.

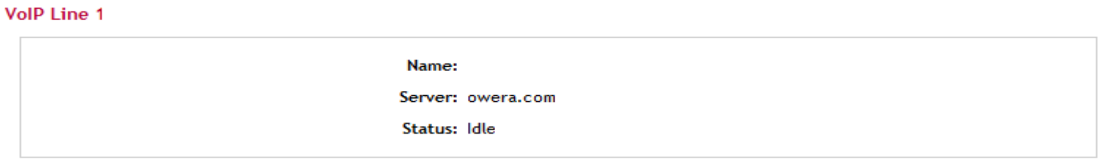
IP Address: The IP address of the router on your local area network.

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

Auto IP Address: If no IP address is assigned to this device, this IP address is used.

DHCP Server: Indicates if the router is acting as a DHCP server on the local area network.

6.1.4 VoIP Line Status

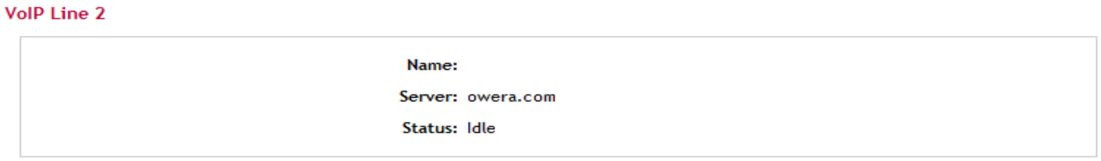


VoIP Line 1

Name:

Server: owera.com

Status: Idle



VoIP Line 2

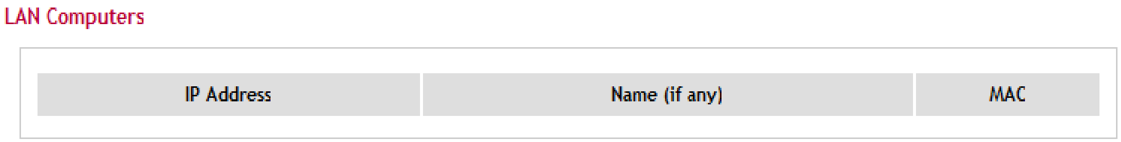
Name:

Server: owera.com

Status: Idle

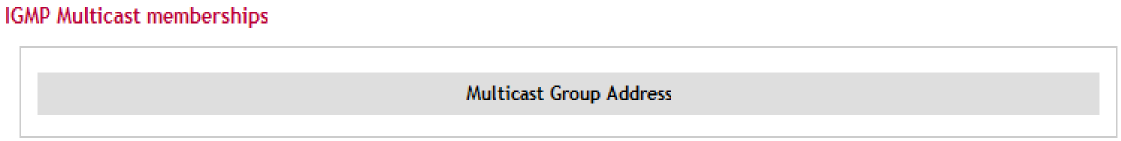
Show if the lines are enabled and/or in use. Idle status is when lines are active but not in use.

6.1.5 LAN Computers & IGMP Multicast memberships



LAN Computers

IP Address	Name (if any)	MAC



IGMP Multicast memberships

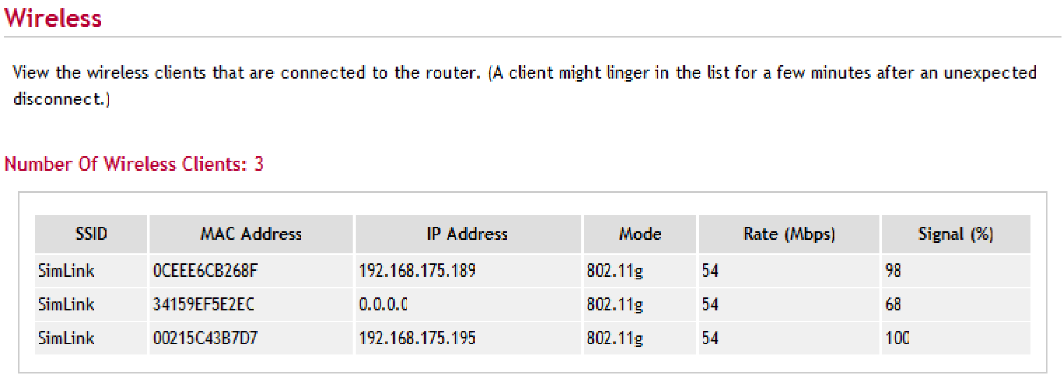
Multicast Group Address

This section 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.

If IGMP is enabled, this section shows all multicast groups of which any LAN devices are members.

6.2 Wireless

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)



Wireless

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

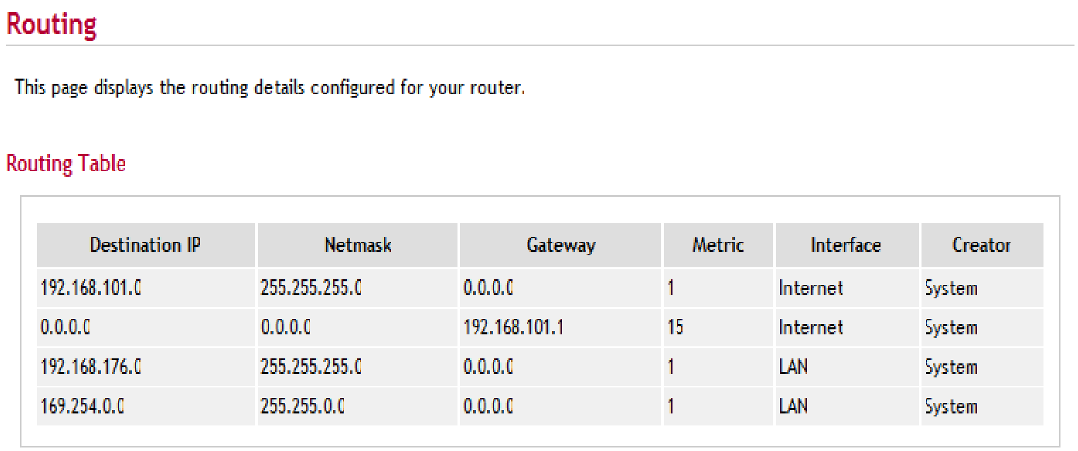
Number Of Wireless Clients: 3

SSID	MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)
SimLink	0CEEE6CB268F	192.168.175.189	802.11g	54	98
SimLink	34159EF5E2EC	0.0.0.0	802.11g	54	68
SimLink	00215C43B7D7	192.168.175.195	802.11g	54	100

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, 11g, or 11n for 802.11a, 802.11b, 802.11g, or 802.11n 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.

6.3 Routing

This page displays the routing details configured for the router.
A gateway value of 0.0.0.0 means there is no next hop. 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.



Routing

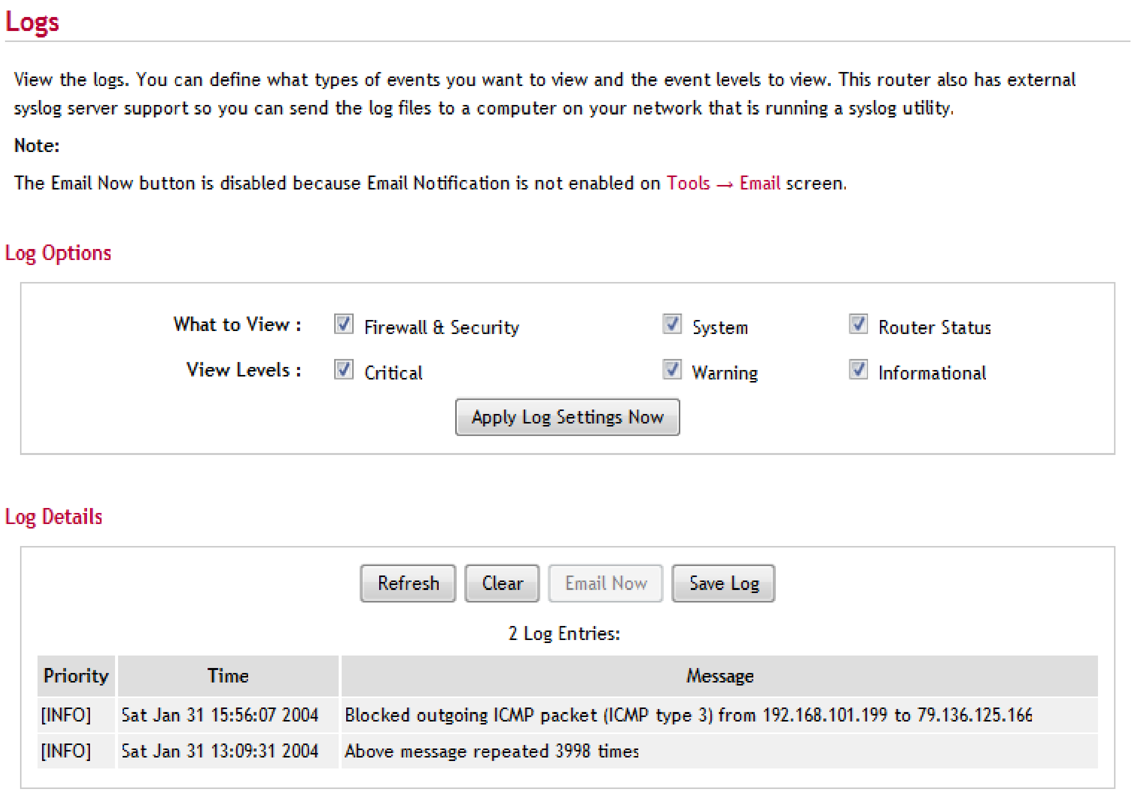
This page displays the routing details configured for your router.

Routing Table

Destination IP	Netmask	Gateway	Metric	Interface	Creator
192.168.101.0	255.255.255.0	0.0.0.0	1	Internet	System
0.0.0.0	0.0.0.0	192.168.101.1	15	Internet	System
192.168.176.0	255.255.255.0	0.0.0.0	1	LAN	System
169.254.0.0	255.255.0.0	0.0.0.0	1	LAN	System

6.4 Logs

The router automatically logs (records) events of possible interest in it's internal memory. If there isn't 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 the 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.



Logs

View the logs. You can define what types of events you want to view and the event levels 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.

Note:

The Email Now button is disabled because Email Notification is not enabled on Tools → Email screen.

Log Options

What to View : ☑ Firewall & Security ☑ System ☑ Router Status

View Levels : ☑ Critical ☑ Warning ☑ Informational

Log Details

2 Log Entries:

Priority	Time	Message
[INFO]	Sat Jan 31 15:56:07 2004	Blocked outgoing ICMP packet (ICMP type 3) from 192.168.101.199 to 79.136.125.166
[INFO]	Sat Jan 31 13:09:31 2004	Above message repeated 3998 times

6.4.1 Log Options

What to View: You can select the types of messages that you want to display from the log. Firewall & Security, System, and Router Status messages can be selected.

View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed from the log.

Apply Log Settings Now: Will filter the log results so that only the selected options appear.

6.4.2 Log Details

Refresh: Updates the log details on the screen so it displays any recent activity.

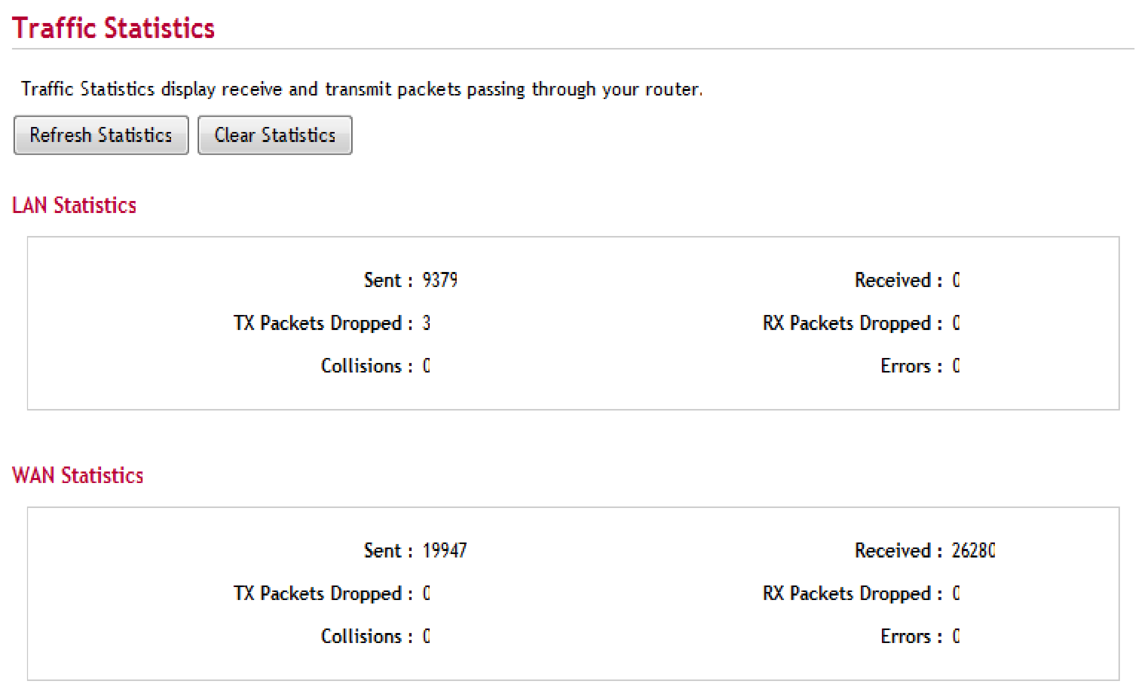
Clear: Clears all of the log contents.

Email Now: This option will send a copy of the router log to the email address configured in the *Tools > Email* screen.

Save Log: This option will save the router to a log file on your computer

6.5 Statistics

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



Traffic Statistics display receive and transmit packets passing through your router.

LAN Statistics

Sent : 9379
Received : 0
TX Packets Dropped : 3
RX Packets Dropped : 0
Collisions : 0
Errors : 0

WAN Statistics

Sent : 19947
Received : 26280
TX Packets Dropped : 0
RX Packets Dropped : 0
Collisions : 0
Errors : 0

Refresh Statistics: Updates the screen with the latest router statistics.

Clear Statistics: Clears all of the values on the screen.

6.5.1 LAN Statistics

Sent: The number of packets transmitted to the local area network.

Received: The number of packets received from the local area network.

TX Packets Dropped: The number of transmit packets dropped on the local area network.

RX Packets Dropped: The number of receive packets dropped on the local area network.

Collisions: The number of collisions on the local area network.

Errors: The number of errors occurring on the local area network.

6.5.2 WAN Statistics

Sent: The number of packets transmitted to the Internet.

Received: The number of packets received from the Internet.

TX Packets Dropped: The number of transmit packets sent to the WAN port that were dropped.

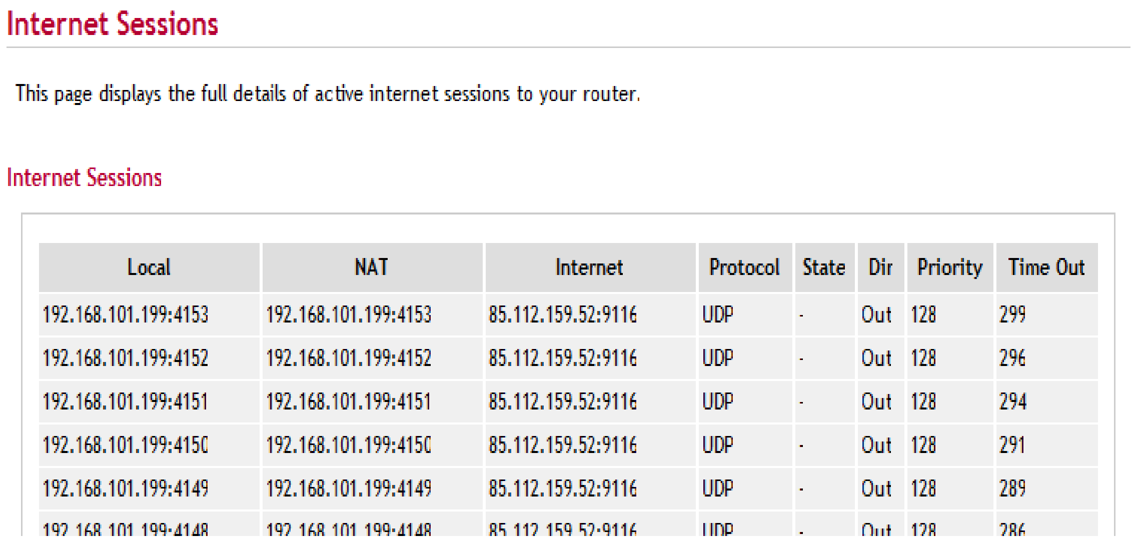
RX Packets Dropped: The number of receive packets sent to the WAN port that were dropped.

Collisions: The number of collisions involving packets intended for the WAN port.

Errors: The number of errors occurring with packets intended for the WAN port.

6.6 Internet 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.



Internet Sessions

This page displays the full details of active internet sessions to your router.

Internet Sessions

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out
192.168.101.199:4153	192.168.101.199:4153	85.112.159.52:9116	UDP	-	Out	128	299
192.168.101.199:4152	192.168.101.199:4152	85.112.159.52:9116	UDP	-	Out	128	296
192.168.101.199:4151	192.168.101.199:4151	85.112.159.52:9116	UDP	-	Out	128	294
192.168.101.199:4150	192.168.101.199:4150	85.112.159.52:9116	UDP	-	Out	128	291
192.168.101.199:4149	192.168.101.199:4149	85.112.159.52:9116	UDP	-	Out	128	289
192.168.101.199:4148	192.168.101.199:4148	85.112.159.52:9116	UDP	-	Out	128	286

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

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

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

Protocol: The communications protocol used for the conversation.

State: State for sessions that use the TCP protocol.

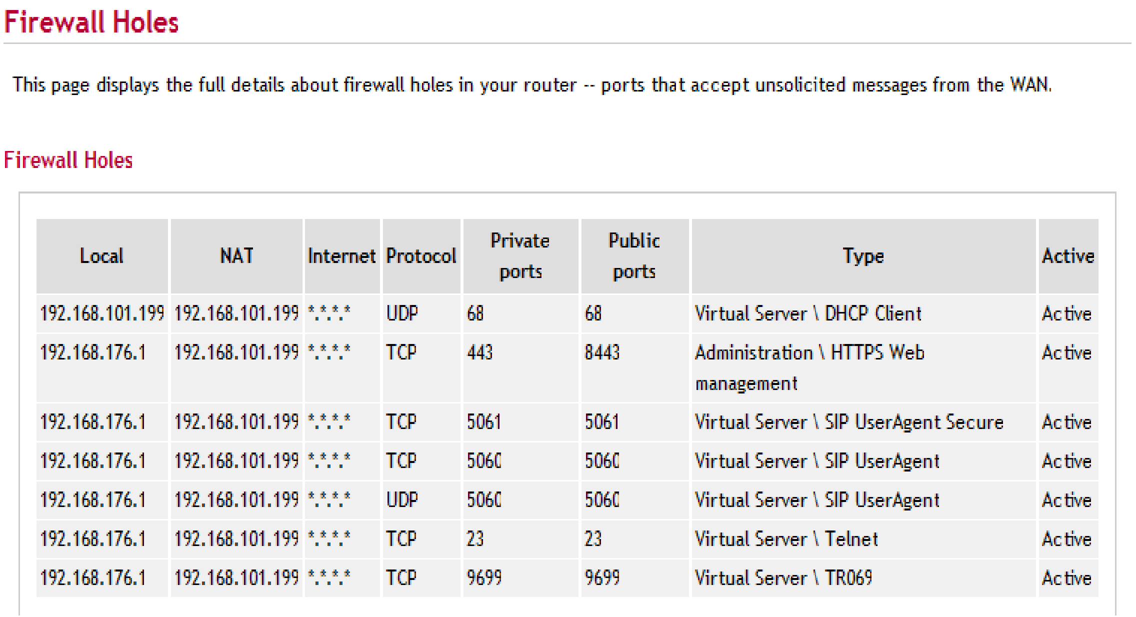
- NO: None -- This entry is used as a placeholder for a future connection that may occur.
- SS: SYN Sent -- One of the systems is attempting to start a connection.
- EST: Established -- the connection is passing data.
- FW: FIN Wait -- The client system has requested that the connection be stopped.
- 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:
Out - Initiated from LAN to WAN.
In - Initiated from WAN to LAN.

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

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.
300 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

6.7 Firewall Holes



Firewall Holes

This page displays the full details about firewall holes in your router -- ports that accept unsolicited messages from the WAN.

Firewall Holes

Local	NAT	Internet	Protocol	Private ports	Public ports	Type	Active
192.168.101.199	192.168.101.199	*.*.*.*	UDP	68	68	Virtual Server \ DHCP Client	Active
192.168.176.1	192.168.101.199	*.*.*.*	TCP	443	8443	Administration \ HTTPS Web management	Active
192.168.176.1	192.168.101.199	*.*.*.*	TCP	5061	5061	Virtual Server \ SIP UserAgent Secure	Active
192.168.176.1	192.168.101.199	*.*.*.*	TCP	5060	5060	Virtual Server \ SIP UserAgent	Active
192.168.176.1	192.168.101.199	*.*.*.*	UDP	5060	5060	Virtual Server \ SIP UserAgent	Active
192.168.176.1	192.168.101.199	*.*.*.*	TCP	23	23	Virtual Server \ Telnet	Active
192.168.176.1	192.168.101.199	*.*.*.*	TCP	9699	9699	Virtual Server \ TR069	Active

An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer. You can view current sessions on the Internet Sessions page. Normally, all connections are started by a LAN-side computer that initiates a session with an Internet-side (WAN-side) computer. Connections from LAN to WAN are always allowed, when possible and in accordance with any policies you set.

If an WAN-side computer attempts to start a connection with a LAN-side computer, that connection attempt will, under normal circumstances, be blocked by the "firewall", and a record of the attempt will be written in the Log.

However, certain useful kinds of Internet sessions are normally initiated from WAN-side computers. To allow connections to be started by WAN-side computers, a "hole" must be created in the firewall.

Firewall holes can be created by several means. You can explicitly create holes with Virtual Server, Port forwarding, and Gaming rules, for example. Also, UPnP devices and LAN-side computers can ask for a hole to be created -- typically the case with peer-to-peer programs, such as Bit Torrent, and IM programs, such as Windows Live Messenger Service -- but there are many other types. The router itself can even create holes for its own use.

The firewall holes page shows currently open holes. It shows you the types of connections that can be started by Internet computers. It also shows the LAN-side computer that will receive any connection started by an Internet computer.

Local: The IP address of the LAN-side computer that will receive packets started by an Internet computer on this connection.

NAT: If the router has more than one WAN-side IP address, the connection attempts are limited to the address shown. An entry of "*.*.*.*" means any IP address.

Internet: An IP address entry means that only that IP address can start a connection. An entry of "*.*.*.*" means any IP address. A policy-name entry means that the connection is limited to that policy.

Protocol: The internet protocol that this connection is allowed to use.

Private Ports: The LAN-side ports used for the connection.

Public Ports: The WAN-side ports used for the connection.

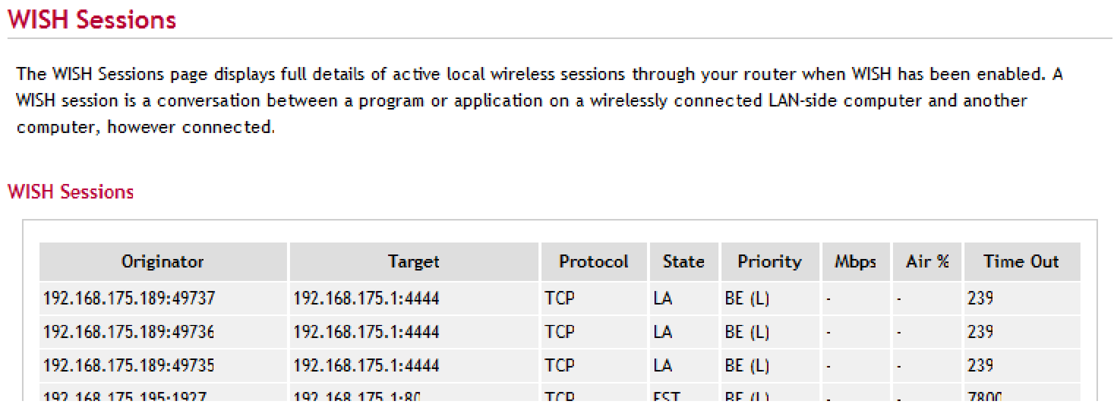
Type: Specifies both how the hole was created and what the hole is used for. For example, "Virtual server \ SMTP" shows that the hole was created as a virtual server rule for the Simple Mail Transfer Protocol..

Active: For holes that are created by scheduled rules, shows whether the rule is currently scheduled.

WISH Sessions

6.8 WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wireless connected LAN-side computer and another computer, however connected.



WISH Sessions

The WISH Sessions page displays full details of active local wireless sessions through your router when WISH has been enabled. A WISH session is a conversation between a program or application on a wirelessly connected LAN-side computer and another computer, however connected.

WISH Sessions

Originator	Target	Protocol	State	Priority	Mbps	Air %	Time Out
192.168.175.189:49737	192.168.175.1:4444	TCP	LA	BE (L)	-	-	239
192.168.175.189:49736	192.168.175.1:4444	TCP	LA	BE (L)	-	-	239
192.168.175.189:49735	192.168.175.1:4444	TCP	LA	BE (L)	-	-	239
192.168.175.195:1927	192.168.175.1:80	TCP	EST	BE (L)	-	-	7800

Originator: The IP address and, where appropriate, port number of the computer that originated a network connection.

Target: The IP address and, where appropriate, port number of the computer to which a network connection has been made.

Protocol: The communications protocol used for the conversation.

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.

Priority: The priority given to packets sent wireless over this conversation by the WISH logic. The priorities are:

- BK: Background (least urgent).
- BE: Best Effort.
- VI: Video.
- VO: Voice (most urgent).

Mbps: Useful description goes here

Air%: Useful description goes here

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.

300 seconds

UDP connections.

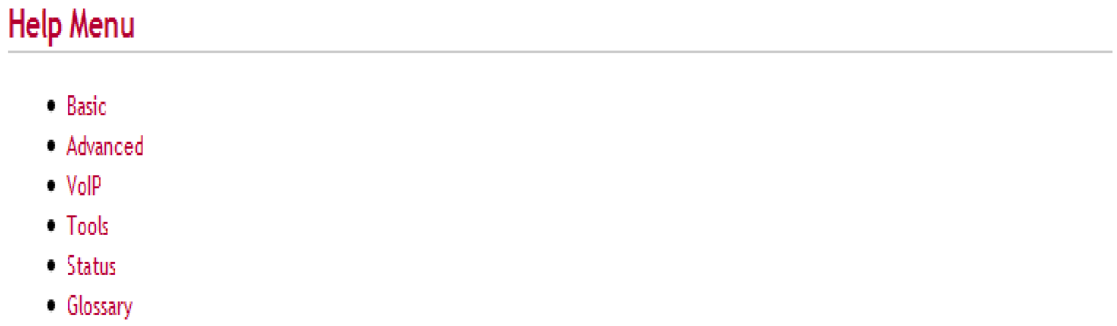
240 seconds

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

7800 seconds

Established or closing TCP connections.

7 Help



Help Menu

- Basic
- Advanced
- VoIP
- Tools
- Status
- Glossary

The help section replicates all the menu choices in the web interface. Each section provides roughly the same information as this manual.

The Service Provider is free to add a detailed Help Section.