



Broadband Router

Model #: RI408

Firmware Version: 4.0.16.1.44.11

User Manual

Ver 1.0

Solutions for the Digital Life™

Table of Contents

1	Introduction	1
	Package Contents	1
	Minimum System Requirements	2
	Features	2
	Getting to Know the Router	3
2	Connecting the Router	7
	Setting Up the Router	7
	Computer Network Configuration	11
	Home Screen	13
3	Configuring My Network Settings	15
	Accessing My Network	15
	Using My Network	16
4	Using Network Connections	23
	Network (Home/Office)	24
	Ethernet Connection	30
	Broadband Ethernet Connection	33
	WAN PPPoE	39
5	Configuring the Router's Security	45
	General	47
	Access Control	49
	Port Forwarding	52
	DMZ (Demilitarized Zone) Host	54
	Port Triggering	55
	Remote Administration	56
	Website Blocking	58
	Static NAT	60
	Advanced Filtering	61
	Security Log	65
6	Using Parental Controls	73
	Activating Parental Controls	73
	Creating a Filtering Policy	74
	Advanced Options	78
	Statistics	79

7	Using Advanced Settings	81
	About	83
	Configuration File	83
	Restart	84
	Restoring Default Settings	84
	Diagnostics	85
	MAC Cloning	86
	System Settings	87
	Universal Plug and Play (UPnP)	92
	Firmware Upgrade	93
	Scheduler Rules	96
	Date and Time	98
	Users	99
	ARP (Address Resolution Protocol) Table	101
	Routing	101
	Network Objects	103
	Firmware Restore	105
	Dynamic DNS	105
	IP Address Distribution	107
	DNS Server	111
	Remote Administration	113
	Protocols	114
8	Monitoring the Router	117
	Monitoring Connections	117
	Traffic Monitoring	118
	System Log	119
	Router Status	119
9	Troubleshooting	121
A	Quality Of Service	125
	Traffic Priority	125
	Traffic Shaping	129
B	Specifications	139
	General	139
	LED Indicators	139
	Environmental	140
	Notices	141
	Regulatory Compliance Notices	141
	Modifications	141

Introduction

1

Thank you for purchasing the Actiontec Broadband Router. The Router features eight Ethernet ports, making it one of the most versatile routers available. If you want to take your home or office networking to the next level, the Actiontec Broadband Router is sure to be one of the keys to your success.



Package Contents

- ♦ Actiontec Broadband Router
- ♦ Black Power cord
- ♦ Yellow cable (Ethernet, 6 ft.)
- ♦ White cable (Ethernet, 10 ft.)
- ♦ Quick Start Guide
- ♦ Installation Guide
- ♦ User Manual CD
- ♦ Wall-mount template
- ♦ Vertical stand
- ♦ Warranty

Minimum System Requirements

- Computer with Ethernet capability
 - Microsoft Windows 98SE, Me, 2000, or XP; Mac OS 9 or greater; Linux/BSD, Unix
 - Internet Explorer 5.0 or higher; Netscape Navigator 7.0 or higher
 - TCP/IP network protocol installed on each computer
-

Features

- Integrated wired networking with 8-port 10/100 Mbps Ethernet switch
- Enterprise-level security, including :
 - Fully customizable firewall with Stateful Packet Inspection
 - Content filtering with URL-keyword based filtering, parental control, customizable filtering policies per computer, and E-mail notification
 - Denial of service protection against IP spoofing attacks, intrusion and scanning attacks, IP fragment overlap, ping of death, and fragmentation attacks
 - Event logging
 - Intrusion detection
 - MAC address filtering
 - NAT
 - DMZ hosting
 - Access control
 - ICSA certified
- Other Features
 - DHCP server option
 - DHCP server/PPPoE server auto-detection
 - DNS server
 - LAN IP and WAN IP address selection
 - MAC address cloning

Port forwarding

PPPoE support

QoS support (end to end layer 2/3) featuring Diffserv, 802.1p/q prioritization, configurable upstream/downstream traffic shaping, random early detection and pass-through of WAN-side DSCPs, PHBs, and queuing to LAN-side devices

Remote management and secured remote management using HTTPS

Reverse NAT

Static NAT

Static routing

Time zone support

VLAN multicast support

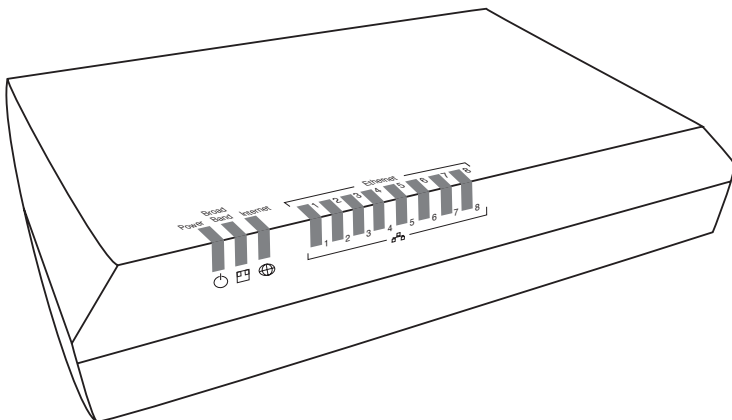
VPN IPSec (VPN passthrough only)

Getting to Know the Router

This section contains a quick description of the Router's lights (LEDs), ports, etc. The Router features several indicator lights on its front panel, and a series of ports and switches on its rear panel.

Front Panel

The front panel of the Router features 11 indicator lights: Power, Broadband, Internet, and Ethernet (8).



Power Light

The Power light displays the Router's current status. If the Power light glows steadily green, the Router is receiving power and fully operational. When the Power light flashes rapidly, the Router is initializing. If the Power light is not illuminated or glows red when the Power cord is plugged in and the Power switch is turned on, the Router has suffered a critical error and technical support should be contacted.

Broadband Light

The Broadband light illuminates when the Router is connected to a the Internet via Ethernet. If flashing, data traffic is passing across the port.

Internet Light

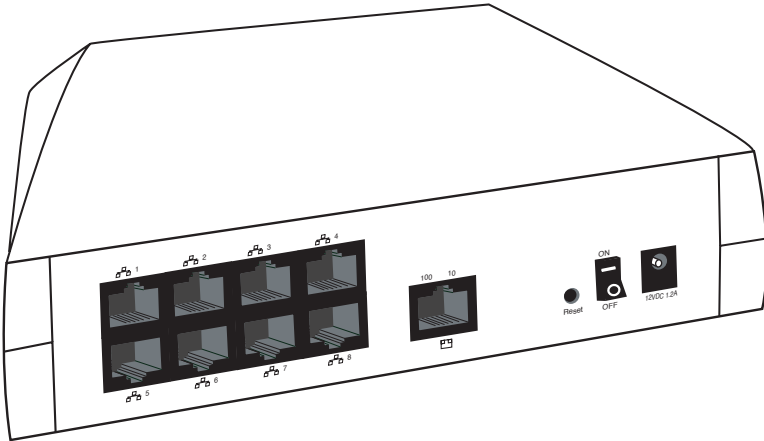
When the Internet light glows steadily green, the Router is connected to the ISP (Internet Service Provider). If it glows amber, there is a physical connection to the ONT (Optical Network Terminator), but authentication has not taken place (i.e., no IP address is present).

Ethernet Lights (1 - 8)

The Ethernet lights illuminate when the Router is connected to a local network via one or more of its Ethernet ports. If flashing, data traffic is passing across the port(s).

Rear Panel

The rear panel of the Router features ten ports (Ethernet [8], Broadband, and Power), as well as a Reset button and Power switch.



Ethernet Ports (8)

The Ethernet ports connect devices to the Router via Ethernet cables to create a local area network (LAN). The Ethernet ports are 10/100 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

Broadband Port

The Broadband port connects the Router to the ISP using an Ethernet cable.

Reset Button

To restore the Router's factory default settings, press and hold the Reset button for approximately ten seconds. The reset process will start about ten seconds after releasing the button. When the Router resets, all the lights on the front panel turn off, and then the lights start flashing. The Router has completed its reset process when the Power light glows steadily green.



Caution: Do not unplug the Power cord from the Router during the reset process. Doing so may result in the loss of the Router's configuration information. If this occurs, reset the Router again.

Power Switch

The Power switch powers the Router on and off.

Power Port

The Power port connects the Router to an electrical wall outlet via the Power cord.



Caution: Do not unplug the Power cord from the Router during the reset process. Doing so may result in the loss of the Router's configuration information. If this occurs, reset the Router again.

Connecting the Router

2

Connecting a computer or local network to the Broadband Router is a simple procedure, varying slightly depending on the computer's operating system, and designed to seamlessly integrate the Router with the computer or local network. Moreover, zero-configuration is attained when taking advantage of Universal Plug-and-Play support in Windows XP.

The Windows default network settings dictate that in most cases, the setup procedure described in the "Computer Network Configuration" will be unnecessary. For example, the default DHCP setting in Windows 2000 is "client," requiring no further modification.

However, Actiontec advises following the setup procedure described below to verify all communication parameters are valid and the physical cable connections are correct.

Setting Up the Router

There are three parts to setting up the Router: Connecting the Cables, Configuring the Router, and Connecting Other Computers.


Connecting the Cables



Note: If a different router was being used, disconnect it. Remove all the old router components, including power supplies and cables, since they will not work with the Broadband Router.

1. Get the Router and black Power cord from the box.
2. Plug the black Power cord in the black port on the back of the Router and then into a power outlet.
3. Turn the Router on.
4. Make sure the Power light on the front of the Router is glows steadily green.
5. Plug the yellow Ethernet cable from the box into one of the eight yellow Ethernet ports on the back of the Router.

6. Make sure the computer is powered on, then plug the other end of the yellow Ethernet cable into an Ethernet port on the computer.
7. Make sure at least one of the Ethernet LAN lights on the front of the Router glows steadily green. This may take a few moments.
8. Get the white Ethernet cable from the box and plug one end in the white port on the back of the Router.
9. Plug the other end of the white Ethernet cable into the high-speed Ethernet jack.
10. Make sure the WAN light on the front of the Router glows steadily green.

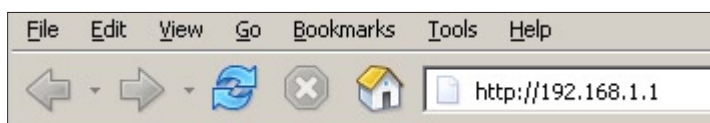
 **Note:** If the WAN light does not illuminate, make sure the Ethernet cable is connected properly at both ends.

Configuring the Router

1. Open a web browser on the computer connected to the Router. In the “Address” text box, type:

http://192.168.1.1

then press **Enter** on the keyboard.



2. The “Login” screen appears. Enter the default user name (admin) and password (password) in the appropriate text boxes, then click **OK**.



3. The “Login Setup” screen appears. Select a new user name and password and enter them in the appropriate text boxes (the password must be entered twice, for validation purposes). Write the new user name and password down on a piece of paper and keep it in a safe place, since they will be needed to access the Router’s MegaControl Panel™ in the future.



Login Setup

We now require you to change your default login User Name and Password. Please select a new login User Name and Password and type it into the appropriate fields below, then click OK.

User Name:

New Password:

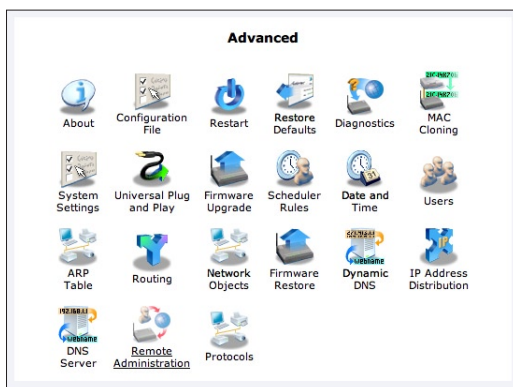
Retype New Password:

4. The “Home” screen of the MegaControl Panel appears. Make sure the green light is displayed in the “Network Status” section of the screen.



5. Make sure the “Ethernet Status” in the “Broadband Connection” section displays “Connected,” as shown in the figure above.

- Click **Advanced** at the top of the Home screen. The “Advanced” screen appears.



- Click **Date and Time**. The “Date and Time” screen appears.

Date and Time

Localization

Local Time: Jan 1, 2003 21:26:10

Time Zone: Eastern_Time (GMT-05:00)

Daylight Saving Time

☒ Enabled

Start: Mar 28 00 : 00

End: Oct 28 01 : 00

Offset: 60 Minutes

Automatic Time Update

☒ Enabled

Time Of Day (TOD)

Protocol: ☒ Network Time Protocol (NTP)

Update Every: 24 Hours [Sync Now](#)

Time Server	Action
ntp.actiontec.com	Add Remove Refresh
Add	Remove Refresh

Status: Got time update from server, Last Update: Fri Apr 14 13:27:45 2006

Press the **Refresh** button to update the status.

[OK](#) [Apply](#) [Cancel](#) [Clock Set](#) [Refresh](#)

- In the “Localization” section of the screen, select the correct time zone from the “Time Zone” drop-down list, then click **OK** at the bottom of the screen.

The Router is now configured.

Connecting Other Computers

The Router can connect to other computers via Ethernet. To do this:

1. Get an Ethernet cable and plug one end into one of the open yellow Ethernet ports on the back of the Router.
2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.
3. Make sure the corresponding LAN light on the front of the Router glows steadily green.
4. Repeat these steps for each computer to be connected to the Router .

Computer Network Configuration

Each network interface on the computer should either be configured with a statically defined IP address and DNS address, or instructed to automatically obtain an IP address using the Network DHCP server. The Router is set up, by default, with an active DHCP server, and Actiontec recommends leaving this setting as is.

Configuring a Computer to Use Dynamic IP Addressing

To configure a computer to use dynamic IP addressing:

Windows XP

1. Select **Network Connections** in the Control Panel.
2. Right-click **Ethernet Local Area Connection**, then click **Properties**.
3. In the “General” tab, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. The “Internet Protocol (TCP/IP) Properties” window appears.
5. Click the “Obtain an IP address automatically” radio button.
6. Click the “Obtain DNS server address automatically” radio button.
7. Click **OK** to save the settings.

Windows 2000/98/Me

1. Select **Network and Dialing Connections** in the Control Panel.
2. Right-click on the Ethernet connection's icon, then click **Properties**.
3. Select **Internet Protocol (TCP/IP)** component, then click **Properties**.
4. The "Internet Protocol (TCP/IP) Properties" window appears.
5. Click the "Obtain an IP address automatically" radio button.
6. Click the "Obtain DNS server address automatically" radio button.

Windows NT

1. Click **Network** in the Control Panel. The "Network" window appears.
2. In the "Protocol" tab, select **Internet Protocol (TCP/IP)** then click **Properties**.
3. In the "IP Address" tab, click the "Obtain an IP address automatically" radio button.
4. In the "DNS" tab, verify no DNS server is defined in the "DNS Service Search Order" text box and no suffix is defined in the "Domain Suffix Search Order" text box.

Linux

1. Login into the system as a super-user, by entering "su" at the prompt.
2. Type "ifconfig" to display the network devices and allocated IPs.
3. Type "pump -i <dev>," where <dev> is the network device name.
4. Type "ifconfig" again to view the newly allocated IP address.
5. Make sure no firewall is active on device <dev>.

Home Screen

After logging into the Router's MegaControl Panel (see “Configuring the Router” at the beginning of this chapter), the “Home” screen appears.



The Home screen has a “Main Menu” that occupies the top of the screen. Below that, the screen is divided into three columns: “Network Status,” “My Network,” and “Entertainment/General Information.” w.

Main Menu

The “Main Menu” contains links to all of the configuration options of the Router: **Network Connections** (chapter 4), **Security** (chapter 5), **Parental Control** (chapter 6), **Advanced** (chapter 7), **System Monitoring** (chapter 8), and **Quality of Service** (appendix A).

Network Status

This section displays the status of the Router's network and Internet connection. A green light signifies the Router is connected; a yellow light means the Router is attempting to connect; and a red light signifies the Router's connection is down.

Broadband Connection

The "Broadband Connection" section of Network Status displays the state of the Router's broadband connection ("Connected" or "Disconnected").

My Network

The "My Network" section of the Home screen displays the connection type, name, IP address, and MAC (Media Access Control) address of all devices connected to the Router's network. The icon associated with the device will be displayed normally (signifying an active device) or shaded (signifying the device has not been active for at least 60 seconds). The user can also configure the basic settings of each device by clicking on its icon. These settings are described in more detail in chapter 3, "Configuring My Network Settings."

Entertainment/General Information

This section contains links to various Verizon Web sites, and other informational links. Clicking on the flashing icon above "Go to Internet Now" connects the user to the home page configured on the user's web browser.

Configuring My Network Settings

3

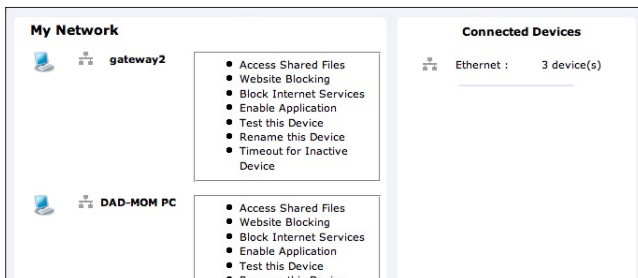
Once the Broadband Router is physically connected and the MegaControl Panel's Home screen is displayed in a web browser, a list of the devices connected to the Router's network appears in the "My Network" section of the screen. From here, some basic network settings can be configured.

Accessing My Network

To access My Network, click on the "My Network" icon:



The "My Network" screen appears:



On the far right side of the screen, in the "Connected Devices" section, is a list of the devices currently connected to the network, listed by connection type and number. The center of the screen contains the "My Network" section, which displays each device connected to the network, and a series of configuration settings.

Using My Network

Various settings can be accessed for a particular device from the My Network column, as explained below.

Access Device

For devices that can be accessed (such as Internet cameras and networked hard drives), locate it in the My Network column, then click **Access Devices** to use the device over the network.

Access Shared Files

To access the shared folders on a particular device, locate the device in the My Network column, then click **Access Shared Files**. A list of shared files appears on the screen.


Website Blocking

Website blocking is used to prevent a device on the network from accessing particular websites on the Internet. To set up website blocking on a networked device, locate the device in the My Network column, then click **Website Blocking**. The “Blocked Website” screen appears.



1. Enter the website address (IP or URL) to block on the network (all pages within the website will also be blocked). If the website address has multiple IP addresses, the Router will resolve all additional addresses and automatically add them to the restrictions table.
2. To apply website blocking to a single computer or group of computers on the network, select them from the “Networked Computer/Device” drop-down list.

3. If website blocking needs to be active all the time, select “Always” from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times select “Specify Schedule” and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).

 **Note:** Make sure the Router’s date and time settings for your time zone are set correctly.

4. Click **OK** to add the website to the table. The previous screen appears while the Router attempts to find the site. “Resolving...” appears in the “Status” column while the site is being located.
5. If the site is successfully located, “Resolved” appears in the Status column. If not, “Hostname Resolution Failed” appears. Click **Refresh** to update the status if necessary. If the Router fails to locate the website, do the following:
 - Use a web browser to verify the website is available. If it is, the website address was entered incorrectly. See “Modifying a Website Address,” below.
 - If the website is not available, return to the Website Blocking screen at a later time and click **Resolve Now** to verify the website can be found and blocked by the Router.

Block Internet Services


Internet services blocking is used to prevent a device on the network from accessing particular services on the Internet, such as receiving E-mail or downloading from FTP sites. To set up Internet services blocking on a networked device, locate the device in the My Network column, then click **Block Internet Services**. The “Add Access Control Rule” screen appears.




The screenshot shows a dialog box titled "Add Access Control Rule". It has three dropdown menus: "Networked Computer / Device" with "Any" selected, "Protocol" with "Any" selected, and "When should this rule occur?" with "Always" selected. At the bottom, there are "OK" and "Cancel" buttons.

1. If this access control rule applies to all networked devices, select “Any” from the “Networked Computer/Device” list box. If this rule applies to certain devices only, select “Specify Address” and click **Add**. Then, add a network object (for more details about adding network objects, see the “Advanced Settings” chapter of this manual).

2. Select the Internet protocol to be blocked from the “Protocol” drop-down list.
3. If this rule will be active all the time, select “Always” from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times select “Specify Schedule” and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).


 **Note:** Make sure the Router’s date and time settings for your time zone are set correctly.

4. Click **OK** to save the changes. The Access Control screen will display a summary of the access control rule.

 **Note:** To block a service that is not included in the list select “Specify Protocol” from the Protocol drop-down menu. The “Edit Service” screen appears. Define the service, then click **OK**. The service will then be automatically added to the top section of the “Add Access Control Rule” screen, and will be selectable.

The user may disable an access control and the service made available without having to remove the service from the Access Control table. This may be useful to make the service available only temporarily, with the expectation that the restriction will be reinstated later.

- To temporarily disable an access control clear the check box next to the service name.
- To reinstate the restriction at a later time select the check box next to the service name.
- To remove an access restriction from the Access Control table click the Remove button for the service. The service will be removed from the Access Control table.

 **Note:** When web filtering is enabled, HTTP services cannot be blocked by access control.

Enable Application

Activating “Enable Application” (also known as port forwarding) allows the network to be exposed to the Internet in certain limited and controlled ways, enabling some applications to work from the local network (game, voice, and chat applications, for example), as well as allowing Internet access to servers in the network. To set this up on a networked device, locate the device in the My Network column, then click **Enable Applications**. The “Port Forwarding” screen appears.

Networked Computer / Device	Network Address	Public IP Address	Protocols	WAN Device	Status	Action
Add						

Port Forwarding
Expose computers/devices on the network to external Internet users.

OK **Apply** **Cancel** **Resolve Now** **Refresh**

1. Click **Add**. The “Add Port Forwarding Rule” screen appears.

Add Port Forwarding Rule

☐ Specify Public IP Address

Networked Computer / Device: Specify Address

Protocol: Specify Protocol **Add**

WAN Device: All WAN Devices


Forward to Port: Same as Incoming Port

When should this rule occur? Always

OK **Cancel**

2. Enter the local IP address or the host name of the computer providing the service in the “Networked Computer/Device” text box. Note that only one local network computer can be assigned to provide a specific service or application.
3. Select the Internet protocol to be provided from the “Protocol” drop-down list.
4. To select a port to forward communications to (this is optional), select “Specify” from the “Forward to Port” drop-down list, then, in the text box that appears, enter the port number. If no port is identified, select “Same as Incoming Port.”

5. If this port will be active all the time, select “Always” from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times select “Specify Schedule” and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).
6. Click **OK** to save the changes.

 **Note:** Some applications, such as FTP, TFTP, PPTP, and H323, require the support of special specific Application Level Gateway (ALG) modules to work inside the local network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure they reach their intended destinations. The Router is equipped with a robust list of ALG modules, enabling maximum functionality in the local network.

The ALG is automatically assigned based on the destination port.

Test This Device

Selecting “Test This Device” generates a new screen that displays information about the device, and also allows the user to test the connectivity of the device. To test a networked device, locate the device in the My Network column, then click **Test This Device**. The “Device Information” screen appears.

Device Information

This screen provides a detailed breakdown for this device.

Device:	gateway2
IP Address:	192.168.1.2
Subnet Mask:	255.255.255.0
Network Connection:	Bridge
Lease Type:	Dynamic
Port Forwarding Services:	None
Windows Shared Folders:	\\gateway2.home\

To test if this device is connected to your broad band home router, click the "Test Connectivity" button.

Ping Test:

1. Click **Test Connectivity**. The “Diagnostics” screen appears.

The screenshot shows a web interface titled "Diagnostics". Under the heading "Ping (ICMP Echo)", there is a table of results:

Destination:	www.yahoo.com	Go
Number of pings:	4	
Status:	Test Succeeded	
Packets:	4/4 transmitted, 4/4 received, 0% loss	
Round Trip Time:	Minimum = 16 ms Maximum = 39 ms Average = 22 ms	

Below the table, it says "Press the **Refresh** button to update the status."

At the bottom are two buttons: "Close" and "Refresh".

2. Click **Go**. The Router runs a ping test, and the results are displayed in the Diagnostics screen.

Rename This Device

To rename a networked device, locate the device in the My Network column, then click **Rename This Device**. The “Rename Device” screen appears.

The screenshot shows a web interface titled "Rename Device". Below the title is a subtitle: "This Page allows you to change the name of this device, and how it is identified on your network".

There are three main sections:

- Current Device Name:** A text box containing "gateway2".
- New Name:** A text box for entering a new name. Above it is the instruction: "To rename this device, type the new Device Name below and click OK".
- New Icon:** A drop-down menu showing "Desktop/Laptop" and a small laptop icon. Above it is the instruction: "To assign an icon to this device, select from the drop-down box below and click OK".

At the bottom are two buttons: "OK" and "Back".

Enter the new name of the device in the “New Name” text box and, if needed, select a new icon for the device from the “New Icon” drop-down list.

Timeout for Inactive Device

The amount of time a device continues to be displayed on the network after it has been disconnected is configured in the “Timeout for Inactive Device” screen. To display the screen, click **Timeout for Inactive Device**.



The screenshot shows a web-based configuration interface titled "Timeout for Inactive Device". The text explains that after a device is removed from the router, the setting below is the time frame that it will take for the device to no longer be displayed on the network. It instructs the user to select a desired time frame and click the Apply button. Below this text is a "Timeout:" label followed by a dropdown menu currently set to "5 min". At the bottom of the form are two buttons: "OK" and "Back".

Timeout for Inactive Device

After a device is removed from the router, the setting below is the time frame that it will take for the device to no longer be displayed on the network. This page allows you to change the time out setting.

Please select the desired time frame then click the Apply button for the settings to take affect.

Timeout: 5 min ▼


OK Back

Select the timeout period from the “Timeout” drop-down list. After the device has been disconnected for this amount of time, it will no longer be displayed in the “My Network” column.

Using Network Connections

4











The Broadband Router supports various local area network (LAN) and wide area network (WAN, on Internet) connections via Ethernet. The Network Connection screens of the Router's MegaControl Panel are used to configure the various parameters of the Router's network and Internet connections, and create new connections.

 **Caution:** The settings covered in this chapter should be configured by experienced network technicians only.

To access the Router's network connections, click **Network Connections** at the top of the Home screen. The "Network Connections" screen appears.

Network Connections

NOTE: Ignore the WAN PPPOE Status unless you are a PPPOE customer.














Rule Name	Status	Action
 Network (Home/Office)	Connected	 
 Broadband Connection (Ethernet)	Down	 
 WAN PPPOE	Disabled	 
Add		

Full Status Detect Broadband Connection Advanced >>

Click **Advanced** to expand the screen and display all connection entries.

Network Connections

NOTE: Only advanced technical users should use this feature.

Rule Name	Status	Action
 Network (Home/Office)	Connected	 
 Ethernet	Connected	 
 Broadband Connection (Ethernet)	Down	 
 WAN PPPOE	Disabled	 
Add		

Full Status Detect Broadband Connection Basic <<

To select a connection, click on its name. The rest of this chapter describes the different network connections available on the Router, as well as the connection types that can be created.

Network (Home/Office)

Select **Network (Home/Office)** in the Network Connections screen to generate the “Network (Home/Office) Properties” screen. This screen displays a list of the local network’s properties. The only modifications that can be made from this screen are disabling the connection (by clicking **Disable**) or renaming the connection (by entering a new name in the “Rule Name” text box).

Network (Home/Office) Properties

NOTE: Only advanced technical users should use this feature.

Disable

Rule Name: Network (Home/Office)

Status: Connected

Network: Network (Home/Office)

Underlying Device: Ethernet
Wireless Access Point
Coax

Connection Type: Bridge

MAC Address: 00:0f:b3:a2:d7:c6

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

IP Address Distribution: DHCP Server

Received Packets: 7138

Sent Packets: 794639

Time Span: 66:41:42

OK

Apply

Cancel

Settings



Note: When a network is disabled, its formerly underlying devices will not be able to get the DHCP address from the network interface to which they were connected.

The Network (Home/Office) connection is used to combine several network devices under one virtual network. For example, a home/office network can be created for Ethernet and other network devices.

Configuring the Home/Office Network

Click **Settings** in the “Network (Home/Office) Properties” screen to generate the “Configure Network (Home/Office)” screen.

General

The top part of the Configure Network (Home/Office) screen displays general communication parameters. Actiontec recommends not changing the default values in this section unless familiar with networking concepts.

Configure Network (Home/Office)	
NOTE: Only advanced technical users should use this feature.	
General	
Status:	Connected
When should this rule occur?:	Always
Network:	Network (Home/Office) ▾
Connection Type:	Bridge
Physical Address:	00:0f:b3:a2:d7:c6
MTU:	Automatic ▾ 1500
Internet Protocol	No IP Address ▾

Status Displays the connection status of the network.

When should this rule occur? Displays when the rule is active. To schedule rules, see the “Advanced Settings” chapter.

Network Select the type of connection being configured from the drop-down list (options: **Broadband Connection**, **Network [Home/Office]**, or **DMZ**).

Connection Type Displays the type of connection.

Physical Address Displays the physical address of the network card used for the network.

MTU MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. “Automatic” sets the MTU at 1500. Other choices include “Automatic by DHCP,” which sets the MTU according to the DHCP connection, and “Manual,” which allows the MTU to be set manually.

Internet Protocol

This section has three options: **No IP Address**, **Obtain an IP Address Automatically**, and **Use the Following IP Address**.





No IP Address Select this option if the connection will have no IP address. This is useful if the connection operates under a bridge.

Obtain an IP Address Automatically Select this option if the network connection is required by the ISP to obtain an IP address automatically. The server assigning the IP address also assigns a subnet mask address, which can be overridden by entering another subnet mask address.

Use the Following IP Address Select this option if the network connection uses a permanent (static) IP address, then the IP address and subnet mask address.

Bridge

The “Bridge” section of the Configure Network (Home/Office) screen is used to specify which networks can join the network bridge.

Bridge				
	Rule Name	Status	STP	Action
	Network (Home/Office)	Connected		
<input type="checkbox"/>	Broadband Connection (Ethernet)	Down	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	Ethernet	Connected	<input checked="" type="checkbox"/>	



Note: When a network is disabled, its formerly underlying devices inherit the network’s DHCP settings. For example, the removal of a network configured as DHCP client automatically configures the devices formerly constituting the network as DHCP clients, with the exact DHCP client configuration.

Click in the check box next to the particular network to specify it. Make sure there are no loops in the network configuration, and apply these settings in case the network consists of multiple switches, or other bridges apart from those created by the Router.

Status The “Status” column displays the connection status of a particular device.

STP Click in the device’s “STP” check box to enable Spanning Tree Protocol on the device. This protocol provides path redundancy while preventing undesirable loops in the network.

Action The “Action” column contains an icon that, when clicked, generates the configuration screen of the particular device.

DNS Server

Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. Specify such an address manually, according to the information provided by the ISP.

To manually configure DNS server addresses, select **Use the Following DNS Server Addresses**. Specify up to two different DNS server addresses, one primary, the other secondary.

DNS Server	
	Use the Following DNS Server Addresses ▾
Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

IP Address Distribution

The “IP Address Distribution” section of the Configure Network (Home/Office) screen is used to configure the Router’s Dynamic Host Configuration Protocol (DHCP) server parameters. DHCP automatically assigns IP addresses to network devices. If enabled, make sure to configure the network devices as “DHCP Clients.” There are three options in this section: **Disabled**, **DHCP Server**, and **DHCP Relay**.

Disabled Select this option if statically assigning IP addresses to the network devices.

DHCP Server To set up the network bridge to function as a DHCP server:


1. Select **DHCP Server**.
2. Enter the IP address at which the Router starts issuing addresses in the “Start IP Address” text boxes. Since the Router’s default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2.
3. Enter the end of the IP address range used to automatically issue IP addresses in the “End IP Address” text boxes.
4. Enter the subnet mask address in the “Subnet Mask” text boxes. The subnet mask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.



5. If Windows Internet Naming Service (WINS) is being used, enter the WINS server address in the “WINS Server” text boxes.
6. Enter the amount of time a network device will be allowed to connect to the Router with its currently issued dynamic IP address in the “Lease Time in Minutes” text box. Just before the time is up, the device’s user will need to make a request to extend the lease or get a new IP address.
7. Click in the “Provide Host Name If Not Specified by Client” check box to have the Router automatically assign network devices with a host name, in case a host name is not provided by the user.

DHCP Relay Select this option to have the Router function as a DHCP relay, and enter the IP address in the screen that appears.

IP Address Distribution According to DHCP Option 60

DHCP Option 60 is used to preset a general name for a product or product family, as well as set a specific IP range and priority level. In this way, one device and its traffic can be given higher priority over another device.

 **Note:** To use this feature, the device must output a vendor class ID for option 60 to assign it traffic priority.

IP Address Distribution According to DHCP Option 60(Vendor Class Identifier)			
Vendor Class ID	Dynamic IP Range	QoS	Action
IP-STB	192.168.1.100-192.168.1.150	5 - Medium	 

To add a new product or product family, click **New IP Range**. This generates the “DHCP Server Pool Settings” screen. Enter the vendor class identifier (provided by the manufacturer of the product), IP range, and priority level in the appropriate text boxes.

DHCP Server Pool Settings

DHCP Option 60 (Vendor Class Identifier):

Start IP Address:

End IP Address:

☒ Set Priority

Routing

The Router can be configured to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, while static routing specifies a fixed routing path to neighboring destinations.

There are two options in the “Routing” section of the Configure Network (Home/Office) screen: **Basic** or **Advanced**.

Basic Select this option for basic routing operation.

Advanced To set up the Router’s network bridge for advanced routing:

1. Select **Advanced** from the “Routing” drop-down menu.
2. Enter a device metric in the “Device Metric” text box. The device metric is a value used by the Router to determine whether one route is superior to another, considering parameters such as bandwidth and delay time.
3. Click in the “Default Route” check box to define this device as a the default route.
4. Click in the “Multicast - IGMP Proxy Internal” check box to activate multicasting.

Routing Table

Clicking **New Route** generates the “New Route” window, where a new route can be configured.

Internet Connection Firewall

Click in the “Enabled” check box to activate the Router’s firewall on the LAN Bridge connection. Actiontec does NOT recommend activating this feature.

Additional IP Addresses

Clicking **New IP Address** generates the “Additional IP Address Settings” screen, where additional IP addresses can be created to access the Router via the Network (Home/Office) connection.

Ethernet Connection

An Ethernet connection connects computers to the Router using Ethernet cables, either directly or via network hubs and switches. Click **Ethernet** in the Network Connections screen (if needed, click **Advanced** at the bottom of the screen to reveal the “Ethernet” link below “Network [Home/Office]”) to generate the “Ethernet Properties” screen. This screen displays a list of the connection’s properties. The only modifications that can be made from this screen are disabling the connection (by clicking **Disable**) or renaming the connection (by entering a new name in the “Rule Name” text box).

Ethernet Properties

NOTE: Only advanced technical users should use this feature.

Rule Name:	<input type="text" value="Ethernet"/>
Status:	Connected
Network:	Network (Home/Office)
Connection Type:	Ethernet
MAC Address:	00:0f:b3:a2:d7:c7
IP Address Distribution:	Disabled
Received Packets:	8967
Sent Packets:	615430
Time Span:	70:31:48











Note: If disabling the connection, the Router must be rebooted for the change to take effect.

Configuring the Ethernet Connection

Click **Settings** at the bottom-right of the Ethernet Properties screen to generate the “Configure Ethernet” screen.

Configure Ethernet

NOTE: Only advanced technical users should use this feature.

General				
Status:	Connected			
When should this rule occur?:	Always			
Network:	Network (Home/Office) ▼			
Connection Type:	Ethernet			
Physical Address:	00:0f:b3:a2:d7:c6			
MTU:	Automatic ▼	1500		
Internet Connection Firewall <input type="checkbox"/> Enabled				
Additional IP Addresses New IP Address				
8 Ports Ethernet Switch Show ▼				
Port	Status	PVID	VLANs	Action
Port 1	Connected 100 FD			
Port 2	Disconnected			
Port 3	Disconnected			
Port 4	Disconnected			
Port 5	Disconnected			
Port 6	Disconnected			
Port 7	Disconnected			
Port 8	Disconnected			

General

The top part of the Configure Ethernet screen displays general communication parameters. Actiontec recommends not changing the default values in this section unless familiar with networking concepts.

Status Displays the connection status of the Ethernet switch.

When should this rule occur? Displays when the rule is active. To schedule rules, see the “Advanced Settings” chapter.

Network Select the type of connection being configured from the drop-down list (**Network [Home/Office]**, **Broadband Connection**, or **DMZ**).

Connection Type Displays the type of connection.

Physical Address Displays the physical address of the network card used for the network.

MTU MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. “Automatic” sets the MTU at 1500. Other choices include “Automatic by DHCP,” which sets the MTU according to the DHCP connection, and “Manual,” which allows the MTU to be set manually.

Internet Connection Firewall

Click in the “Enabled” check box to activate the Router’s firewall on the Ethernet connection. Actiontec does NOT recommend activating this feature.

Additional IP Addresses

Clicking **New IP Address** generates the “Additional IP Address Settings” screen, where additional IP addresses can be created to access the Router via the Ethernet connection.

8 Ports Ethernet Switch

This section displays the connection status of the Router’s eight Ethernet ports.

8 Ports Ethernet Switch				
Show ▾				
Port	Status	PVID	VLANs	Action
Port 1	Connected 100 FD			
Port 2	Disconnected			
Port 3	Disconnected			
Port 4	Disconnected			
Port 5	Disconnected			
Port 6	Disconnected			
Port 7	Disconnected			
Port 8	Disconnected			

Clicking on a connection’s “Action” icon (in the column on the right) generates the “Port VLANs” screen, where ingress policies can be edited.

Port VLANs

Port 0 Settings

Ingress Policy:

Untagged (Do Not Add VLAN Header) ▾

Port VLANs IDs

VLAN ID	Egress Policy	Action
Add		

OK

Apply

Cancel

Broadband Ethernet Connection

A Broadband Ethernet connection connects the Router to the Internet using an Ethernet cable. Click **Broadband Connection (Ethernet)** from the Network Connections screen to generate the “Broadband Connection (Ethernet) Properties” screen. This screen displays a list of the connection’s properties. The only modifications that can be made from this screen are disabling the connection (by clicking **Disable**) or renaming the connection (by entering a new name in the “Rule Name” text box).

Broadband Connection (Ethernet) Properties

NOTE: Only advanced technical users should use this feature.

Disable

Rule Name:	Broadband Connection (Ethernet)
Status:	Down
Network:	Broadband Connection (Ethernet)
Connection Type:	Ethernet
MAC Address:	00:0f:b3:a2:d7:ca
IP Address Distribution:	Disabled
Received Packets:	0
Sent Packets:	0
Time Span:	70:10:59

OK

Apply

Cancel

Settings



Note: If disabling the connection, the Router must be rebooted for the change to take effect.

Configuring the Broadband Ethernet Connection

Click **Settings** at the bottom-right of the Broadband Connection (Ethernet) Properties window to generate the “Configure Broadband Connection (Ethernet)” screen.

Configure Broadband Connection (Ethernet)

NOTE: Only advanced technical users should use this feature.

General	
Status:	Down
When should this rule occur?:	Always
Network:	Broadband Connection ▾
Connection Type:	Ethernet
Physical Address:	00:0f:b3:a2:d7:c6
MTU:	Automatic ▾ 1500
Internet Protocol	No IP Address ▾
Internet Connection Firewall	<input checked="" type="checkbox"/> Enabled
Additional IP Addresses	New IP Address

OK
Cancel

General

The top part of the screen displays general communication parameters. Actiontec recommends not changing the default values in this section unless familiar with networking concepts.

Status Displays the status of the Ethernet connection (“Down,” “Connected,” etc.)

Schedule Displays when the rule is active. To configure rules, see the “Advanced Settings” chapter.

Network Select the type of connection being configured from the drop-down list (options: **Network (Home/Office)**, **Broadband Connection**, or **DMZ**).

Connection Type Displays the type of connection. Since this is an Ethernet Connection, “Ethernet” is displayed.

Physical Address Displays the physical address of the network card used for the network.

MTU MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. “Automatic, sets the MTU at 1500. Other choices include “Automatic by DHCP,” which sets the MTU according to the DHCP connection, and “Manual,” which allows the MTU to be set manually.

Internet Protocol

This section includes three options: **No IP Address**, **Obtain an IP Address Automatically**, and **Use the Following IP Address**.

No IP Address Select this option if the connection has no IP address. This is useful if the connection is operating under a bridge.

Obtain an IP Address Automatically Select this option if the ISP requires the connection to obtain an IP address automatically. The server assigning the IP address also assigns a subnet mask address, which can be overridden by clicking in the “Override Subnet Mask” check box and entering another subnet mask address. Additionally, the DHCP lease can be renewed and/or released by clicking on the appropriate “DHCP Lease” button.

Use the Following IP Address Select this option if the connection uses a permanent (static) IP address. The ISP should provide this address, along with a subnet mask address, default gateway address, and, optionally, primary and secondary DNS server addresses.

DNS Server

The Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. This connection can be configured to automatically obtain a DNS server address, or such an address can be specified manually, according to the information provided by the ISP.

To configure the connection to automatically obtain a DNS server address, select **Obtain DNS Server Address Automatically** from the “DNS Server” drop-down list. To manually configure DNS server addresses, select **Use the Following DNS Server Addresses**. Specify up to two different DNS server addresses, one primary, the other secondary.

IP Address Distribution

The “IP Address Distribution” section of the Configure Broadband Connection (Ethernet) screen is used to configure the Router’s Dynamic Host Configuration Protocol (DHCP) server parameters. DHCP automatically assigns IP addresses to network devices. If enabled, make sure to configure the network devices as “DHCP Clients.” There are three options in this section: **Disabled**, **DHCP Server**, and **DHCP Relay**.



Caution: Actiontec strongly recommends leaving this setting at “Disabled.”

Disabled Select this option if statically assigning IP addresses to the network devices.


DHCP Server To set up the Router to function as a DHCP server:



1. Select **DHCP Server**.
2. Enter the IP address at which the Router starts issuing addresses in the “Start IP Address” text boxes. Since the Router’s default IP address is 192.168.1.1, the Start IP Address must be 192.168.1.2 or higher.
3. Enter the end of the IP address range used to automatically issue IP addresses in the “End IP Address” text boxes.
4. Enter the subnet mask address in the “Subnet Mask” text boxes. The subnet mask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.
5. If a Windows Internet Naming Service (WINS) is being used, enter the WINS server address in the “WINS Server” text boxes.
6. Enter the amount of time a network device will be allowed to connect to the Router with its currently issued dynamic IP address in the “Lease Time in Minutes” text box. Just before the time is up, the device’s user will need to make a request to extend the lease or get a new IP address.
7. Click in the “Provide Host Name If Not Specified by Client” check box to have the Router automatically assign network devices with a host name, in case a host name is not provided by the user.

DHCP Relay Select this option to have the Router function as a DHCP relay, and enter the IP address in the screen that appears.

IP Address Distribution According to DHCP Option 60

DHCP Option 60 is used to preset a general name for a product or product family, as well as set a specific IP range and priority level. In this way, one device and its traffic can be given higher priority over another device.

 **Note:** To use this feature, the device must output a vendor class ID for option 60 to assign it traffic priority.

IP Address Distribution According to DHCP Option 60(Vendor Class Identifier)			
Vendor Class ID	Dynamic IP Range	QoS	Action
IP-STB	192.168.1.100-192.168.1.150	5 - Medium	 

To add a new product or product family, click **New IP Range**. This generates the “DHCP Server Pool Settings” screen. Set the device name, IP range, and priority level in the appropriate text boxes.

DHCP Server Pool Settings

DHCP Option 60 (Vendor Class Identifier):

Start IP Address:

End IP Address:

☒ Set Priority
 7-High

Routing

The Router can be configured to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, while static routing specifies a fixed routing path to neighboring destinations.

There are two options in the “Routing” section of the “Configure Broadband Connection (Ethernet)” screen: **Basic** or **Advanced**.

Basic Select this option for basic routing operation.

Advanced To set up the Router’s Broadband Ethernet connection for advanced routing:

1. Select **Advanced** from the Routing drop-down menu.
2. Enter a device metric in the “Device Metric” text box. The device metric is a value used by the Router to determine whether one route is superior to another, considering parameters such as bandwidth and delay time.

3. Click in the “Default Route” check box to define this device as a the default route.
4. Click in the “Multicast - IGMP Proxy Internal” check box to activate multi-casting.

Routing Table

Clicking **New Route** generates the “New Route” window, where a new route can be configured.

Internet Connection Firewall

Click in the “Enabled” check box to activate the Router’s firewall on the connection.

Additional IP Addresses

Clicking **New IP Address** generates the “Additional IP Address Settings” screen, where additional IP addresses can be created to access the Router via the connection.

WAN PPPoE

WAN Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards: Point-to-Point Protocol and Ethernet. PPPoE enables Ethernet networked computers to exchange information with computers on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

Click **WAN PPPoE** in the Network Connections screen to generate the “WAN PPPoE Properties” screen. This screen displays a list of the connection’s properties. The only modifications that can be made from this screen are disabling the connection (by clicking **Disable**) or renaming the connection (by entering a new name in the “Name” text box).

WAN PPPOE Properties

NOTE: Only advanced technical users should use this feature.

Enable	
Rule Name:	WAN PPPOE
Status:	Disabled
Network:	Broadband Connection
Underlying Device:	Broadband Connection (Ethernet)
Connection Type:	PPPoE
Service Name:	
User Name:	verizonfios

OK **Apply** **Cancel** **Settings**

Configuring the WAN PPPoE Connection

Click **Settings** in the WAN PPPoE Properties screen to generate the “Configure WAN PPPoE” screen.

Configure WAN PPPOE

NOTE: Only advanced technical users should use this feature.

General	
Status:	Disabled
When should this rule occur?:	Always
Network:	Broadband Connection ▼
Connection Type:	PPPoE
MTU:	Automatic ▼ 1492
Underlying Connection:	Broadband Connection (Ethernet) ▼
PPP	
Service Name (should be filled only if specified by provider): <input type="text"/>	
<input type="checkbox"/> On Demand (will attempt to connect only when packets are sent)	
Time Between Reconnect Attempts:	30 Seconds
PPP Authentication	
Login User Name (case sensitive):	verizonfios <input type="text"/>
Login Password:	***** <input type="password"/>
<input checked="" type="checkbox"/> Support Unencrypted Password (PAP)	
<input checked="" type="checkbox"/> Support Challenge Handshake Authentication (CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP (MS-CHAP)	
<input checked="" type="checkbox"/> Support Microsoft CHAP Version 2 (MS-CHAP v2)	
PPP Compression	
BSD:	Allow ▼
Deflate:	Allow ▼
Internet Protocol	
Obtain an IP Address Automatically ▼	
<input type="checkbox"/> Override Subnet Mask: 0 0 0 0	
DNS Server	
No DNS Server ▼	
Routing	
Basic ▼	
Internet Connection Firewall	
<input checked="" type="checkbox"/> Enabled	

General

The top part of the Configure WAN PPPoE screen displays general communication parameters. Actiontec recommends not changing the default values in this section unless familiar with networking concepts.

Status Displays the connection status of the WAN PPPoE connection. (“Down,” “Disabled,” “Connected,” etc.)

When should this rule occur? Displays when the rule is active. To schedule rules, see “Advanced Settings” chapter.

Network Select the type of connection being configured from the drop-down list (**Broadband Connection**, **Network (Home/Office)**, or **DMZ**).

Connection Type Displays the type of connection. Since this is PPPoE connection, “PPPoE” is displayed.

MTU MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. “Automatic,” sets the MTU at 1492. Other choices include “Automatic,” which sets the MTU according to the connection to the ISP, and “Manual,” which allows the MTU to be set manually.

Underlying Connection Specify the underlying connection above which the protocol initiates from the drop-down list, which displays all possible underlying devices.

PPP Configuration

Point-to-Point Protocol (PPP) is the most popular method for transporting packets between the user and the ISP.

Service Name Specify the networking peer’s service name, if provided by the ISP, in this text box.

On-Demand To use PPP on demand to initiate the point-to-point protocol session only when packets are actually sent over the Internet, click in this check box. This option should be active on a limited basis

Idle Time Before Hanging Up Enter the amount of idle time, in minutes, before the PPP session automatically ends .

Time Between Reconnect Attempts In this text box, specify the duration between PPP reconnect attempts, as provided by the ISP.

PPP Authentication

Point-to-Point Protocol (PPP) currently supports four authentication protocols: **Password Authentication Protocol (PAP)**, **Challenge Handshake Authentication Protocol (CHAP)**, and **Microsoft CHAP versions 1 and 2**. Select the authentication protocols the Router may use when negotiating with a PPTP server in this section. Select all the protocols if no information is available about the server's authentication methods. Note that encryption is performed only if Microsoft CHAP, Microsoft CHAP version 2, or both are selected.



Warning: The PPP Authentication settings should not be changed unless instructed to do so by Verizon.

Login User Name Enter the user name (provided by the ISP) in this text box.

Login Password Enter the password (provided by the ISP) in this text box.

Support Unencrypted Password (PAP) Password Authentication Protocol (PAP) is a simple, plain-text authentication scheme. The user name and password are requested by the networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.

Support Challenge Handshake Authentication (CHAP) Click in this check box to activate CHAP, a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.

Support Microsoft CHAP Click in this check box if communicating with a peer that uses Microsoft CHAP authentication protocol.

Support Microsoft CHAP Version 2 Select this check box if communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.

PPP Compression

The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner.

For each compression algorithm (**BSD** and **Deflate**), select one of the following from the drop-down list:

Reject Selecting this option rejects PPP connections with peers that use the compression algorithm. If Reject is activated, throughput may diminish.

Allow Selecting this option allows PPP connections with peers that use the compression algorithm.

Require Selecting this option insures a connection with a peer using the compression algorithm.

Internet Protocol

Select one of the following Internet Protocol options from the “Internet Protocol” drop-down list:

Obtain an IP Address Automatically This option is selected by default. Change only if required by the ISP. The server that assigns the Router with an IP address also assigns a subnet mask. Override the dynamically assigned subnet mask by selecting the “Override Subnet Mask” and entering a different subnet mask.

Use the Following IP Address Select this option to configure the Router to use a permanent (static) IP address. The ISP should provide this address.

DNS Server

The Domain Name System (DNS) is the method by which website or domain names are translated into IP addresses. The Router can be configured to automatically obtain a DNS server address, or the address can be entered manually, according to the information provided by the ISP.

To configure the connection to automatically obtain a DNS server address, select **Obtain DNS Server Address Automatically** from the “DNS Server” drop-down list. To manually configure DNS server addresses, select **Use the Following DNS Server Addresses** from the “DNS Server” drop-down list. Up to two different DNS server addresses can be entered (Primary and Secondary).

Routing

Select **Advanced** or **Basic** from the “Routing” drop-down list. If Advanced is selected, additional options appear, as listed below.

Routing Mode Select one of the following Routing modes:

- **Route** - Select this option to cause the Router to act as a router between two networks.

- **NAT** - Select this option to activate Network Address Translation (NAT), which translates IP addresses to a valid, public address on the Internet. NAT adds security, since the IP addresses of the devices on the network are not transmitted over the Internet. In addition, NAT allows many addresses to exist behind a single valid address. Use the NAT routing mode only if the local network consists of a single device, or collisions may occur if more than one device attempts to communicate using the same port.
- **NAPT** - Select this option to activate NAPT (Network Address and Port Translation), which refers to network address translation involving the mapping of port numbers and allows multiple machines to share a single IP address. Use NAPT if the local network contains multiple devices, a topology that necessitates port translation in addition to address translation.

Device Metric The device metric is a value used by the Router to determine whether one route is superior to another, considering parameters such as bandwidth, delay, and more.

Default Route Click in this check box to define the connection as a the default route.

Multicast - IGMP Proxy Default Click in this check box to enable the Router to issue IGMP (Internet Group Management Protocol) host messages on behalf of hosts the Router discovers through standard IGMP interfaces. IGMP proxy enables the routing of multicast packets according to the IGMP requests of local network devices asking to join multicast groups.

Routing Table

Clicking **New Route** generates the “New Route” window, where a new route can be configured.

Internet Connection Firewall

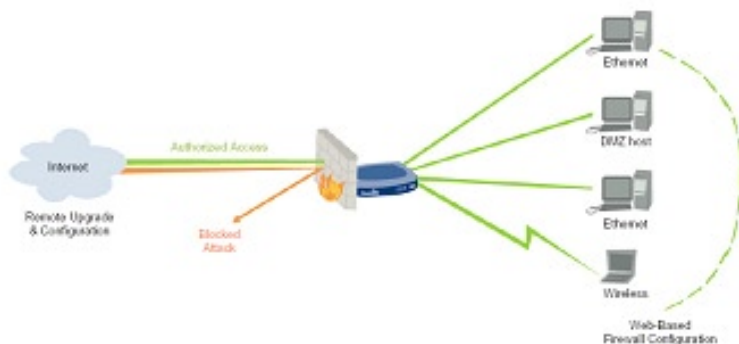
Click in the “Enabled” check box to activate the Router’s firewall on the WAN PPPoE connection.

Configuring the Router's Security

5

The Broadband Router's security suite includes comprehensive and robust security services: Stateful Packet Inspection, a firewall, user authentication protocols, and password protection mechanisms. These features allow users to connect their computers to the Internet and be protected from the security threats.

The Router's firewall is the cornerstone of the Router's security suite. It has been exclusively tailored to the needs of the residential/office user and is pre-configured to provide optimum security.



The firewall provides both the security and flexibility home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

Additional features, including surfing restrictions and access control, can also be configured locally through the Router's MegaControl Panel, or remotely by a service provider.

The firewall also supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. Specific input and output rules can be defined, the order of logically similar sets of rules can be controlled, and distinctions between rules that apply to Internet and local network devices can be made.

This chapter covers these Security features:

- **General** - select the security level for the firewall.
- **Access Control** - restrict access from the local network to the Internet.
- **Port Forwarding** - enable access from the Internet to specified services provided by computers on the local network.
- **DMZ Host** - configure a network host to receive all traffic arriving at the Router which does not belong to a known session.
- **Port Triggering** - define port triggering entries to dynamically open the firewall for some protocols or ports.
- **Remote Administration** - enable remote configuration of the Router from any Internet-accessible computer.
- **Website Blocking** - block network access to a certain hosts or websites on the Internet.
- **Static NAT** - allow multiple static NAT IP addresses to be designated to devices on the network.
- **Advanced Filtering** - control the firewall's settings and rules.
- **Security Log** - view and configure the security log.

General

The “General” screen is used to configure the Router’s basic security settings.



The firewall regulates the flow of data between the local network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through the Router) or rejected (barred from passing through the Router) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local network users access to required Internet services.

The firewall rules specify what types of services available on the Internet can be accessed from the local network and what types of services available in the local network can be accessed from the Internet. Each request for a service the firewall receives, whether originating in the Internet or from a computer in the local network, is checked against the firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, all subsequent data associated with this request (a “session”) will also be allowed to pass, regardless of its direction.


For example, when accessing a website on the Internet, a request is sent out to the Internet for this site. When the request reaches the Router, the firewall identifies the request type and origin (HTTP and a specific computer in the local network, in this case). Unless the Router is configured to block requests of this type from this computer, the firewall allows this request to pass out onto the Internet. When the website is returned from the web server, the firewall will associate it with this session and allow it to pass, regardless of whether HTTP access from the Internet to the local network is blocked or permitted.

Note that it is the origin of the request, not subsequent responses to this request, which determines whether a session can be established or not.

The Router features three pre-defined security levels: **Minimum**, **Typical**, and **Maximum**. The table below summarizes the behavior of the Router for each of the three security levels.

Security Level	Requests from the Internet (incoming traffic)	Requests from the local network (outgoing traffic)
Maximum Security	Blocked - No access to local network from Internet, except as configured in the Port Forwarding, DMZ host, and Remote Access screens.	Limited - Only commonly used services, such as web browsing and E-mail, are permitted.
Typical Security	Blocked - No access to local network from Internet, except as configured in the Port Forwarding, DMZ host, and Remote Access screens.	Unrestricted - All services are permitted, except as configured in the Access Control screen.
Minimum Security	Unrestricted - Permits full access from Internet to local network; all connection attempts permitted.	Unrestricted - All services are permitted, except as configured in the Access Control screen.

These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

 **Note:** Some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports if they cannot connect with their own default ports. When applying this behavior, these applications will not be blocked outbound, even at the Maximum Security level.

To configure the Router's security settings:

1. From the General screen, select a security level by clicking the appropriate radio button. Using the Minimum Security setting may expose the local network to significant security risks, and thus should only be used for short periods of time.

2. Check the “Block IP Fragments” box to protect the local network from a common type of hacker attack that uses fragmented data packets to sabotage the network. Note that VPN over IPSec and some UDP-based services make legitimate use of IP fragments. IP fragments must be allowed to pass into the local network to use these services.
3. Click **OK** to save changes.

Access Control

Access control is used to block specific computers within the local network (or even the whole network) from accessing certain services on the Internet. For example, one computer can be prohibited from surfing the Internet, another computer from transferring files using FTP, and the whole network from receiving incoming E-mail.


Access control defines restrictions on the types of requests that can pass from the local network out to the Internet, and thus may block traffic flowing in both directions. In the E-mail example given above, computers in the local network can be prevented from receiving E-mail by blocking their outgoing requests to POP3 servers on the Internet.

Access control also incorporates a list of preset services in the form of applications and common port settings.

Allow or Restrict Services

To view and allow/restrict these services:

1. Select **Access Control** from the left side of any Security screen. The “Access Control” screen appears.



















 **Note:** The “Allowed” section is only visible when the firewall is set to “Maximum.”

Access Control
Block Internet Services / Protocols like, E-mail or Internet access for any computer on your network.


Blocked

Networked Computer / Device	Network Address	Protocols	Status	Action
Add				

Allowed

Networked Computer / Device	Network Address	Protocols	Status	Action
<input checked="" type="checkbox"/> Any	Any	DHCP - UDP 67-68 -> 67	Active	 
<input checked="" type="checkbox"/> Any	Any	DNS - TCP 53 -> 53 TCP 1024-65535 -> 53 UDP 53 -> 53 UDP 1024-65535 -> 53	Active	 
<input checked="" type="checkbox"/> Any	Any	IMAP - TCP Any -> 143	Active	 
<input checked="" type="checkbox"/> Any	Any	SMTP - TCP Any -> 25	Active	 
<input checked="" type="checkbox"/> Any	Any	POP3 - TCP Any -> 110	Active	 
<input checked="" type="checkbox"/> Any	Any	HTTPS - TCP Any -> 443	Active	 
<input checked="" type="checkbox"/> Any	Any	HTTP - TCP Any -> 80	Active	 
<input checked="" type="checkbox"/> Any	Any	FTP - TCP Any -> 21	Active	 
<input checked="" type="checkbox"/> Any	Any	Telnet - TCP Any -> 23	Active	 
Add				

2. Click **Add** in the “Blocked” section of the screen. The “Add Access Control Rule” screen appears.

 **Note:** To block a service, click **Add** in the “Blocked” section of the Access Control screen. To allow outgoing traffic, click **Add** in the “Allowed” section of the screen.

Add Access Control Rule

Networked Computer / Device:

Protocol:

When should this rule occur?:

3. If this access control rule applies to all networked devices, select “Any” from the “Networked Computer/Device” list box. If this rule applies to certain devices only, select “Specify Address” and click **Add**. Then, add a network object (for more details about adding network objects, see the “Advanced Settings” chapter of this manual).
4. Select the Internet protocol to be allowed or blocked from the “Protocol” drop-down list.
5. If the rule will be active all the time, select **Always** from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times, select **Specify Schedule** and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).
6. Click **OK** to save the changes. The Access Control screen will display a summary of the new access control rule.



Note: To block a service not included in the list, select **Specify Protocol** from the Protocol drop-down menu. The “Edit Service” screen appears. Define the service, then click **OK**. The service will then be automatically added to the top section of the “Add Access Control Rule” screen, and will be selectable.

An access control can be disabled and the service made available without having to remove the service from the Access Control table. This may be useful to make the service available temporarily, with the expectation that the restriction will be reinstated later.

- To temporarily disable an access control, clear the check box next to the service name.
- To reinstate the restriction at a later time, select the check box next to the service name.
- To remove an access restriction from the Access Control table, click **Remove** for the service. The service will be removed from the Access Control table.

Port Forwarding

In its default state, the Router blocks all external users from connecting to or communicating with the network, making it safe from hackers who may try to intrude on the network and damage it. However, the network can be exposed to the Internet in certain limited and controlled ways to enable some applications to work from the local network (game, voice, and chat applications, for example) and to enable Internet access to servers in the network. Port forwarding (sometimes referred to as “local servers”) supports both of these functions.

To grant Internet users access to servers inside the local network, each service provided, as well as the computer providing it, must be identified. To do this:

1. Select **Port Forwarding** from the left side of any Security screen. The “Port Forwarding” screen appears.

Networked Computer / Device	Network Address	Public IP Address	Protocols	WAN Device	Status	Action
Add						

OK Apply Cancel Resolve Now Refresh

2. Click **Add**. The “Add Port Forwarding Rule” screen appears.

Add Port Forwarding Rule

☐ Specify Public IP Address

Networked Computer / Device: Specify Address

Protocol Specify Protocol

WAN Connection Type: All Broadband Devices

Forward to Port: Same as Incoming Port

When should this rule occur ? Always

OK Cancel

3. Enter the local IP address or the host name of the computer providing the service in the “Networked Computer/Device” text box, or select them from the drop-down list. Note that only one local network computer can be assigned to provide a specific service or application.

4. Select the Internet protocol to be provided from the “Protocol” drop-down list. To see all options, select **All Services**.
5. Select a WAN connection type from the “WAN Connection Type” drop-down list. Actiontec recommends selecting **All Broadband Devices**.
6. To select a port to forward communications to (this is optional), select **Specify** from the “Forward to Port” drop-down list, then, in the text box that appears, enter the port number. If no port is identified, select **Same as Incoming Port**.
7. If this port will be active all the time, select **Always** from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times, select **Specify Schedule** and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).
8. Click **OK** to save the changes.



Note: Some applications, such as FTP, TFTP, PPTP, and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the local network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. The Router is equipped with a robust list of ALG modules in order to enable maximum functionality in the local network. The ALG is automatically assigned based on the destination port.

How many computers can use a service or play a game simultaneously? Well, the answer may be a bit confusing. All the computers on the network can behave as clients and use a specific service simultaneously. Being a client means the computer within the network initiates the connection; for example, a computer on the network can open an FTP connection with an FTP server on the Internet. But only one computer on the network can operate as a server and respond to requests from computers on the Internet (outside the local network).

DMZ (Demilitarized Zone) Host

The DMZ host feature allows one device on the network to operate outside the firewall. Designate a DMZ host:

- To use an Internet service, such as an online game or video-conferencing program, not present in the Port Forwarding list and for which no port range information is available.
- To expose one computer to all services without restriction or security.



Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, consider the security implications and protect it if necessary.

To designate a local computer as a DMZ host:

1. Select **DMZ Host** from the left side of any Security screen. The “DMZ Host” screen appears.

2. Click in the “DMZ Host IP Address” check box, then enter the IP address of the computer to be designated as a DMZ host. Note that only one network computer can be a DMZ host at any time.
3. Click **OK**.

Click in the “DMZ Host IP Address” check box again to disable the DMZ host.

Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, inbound traffic is allowed to arrive at a specific network host using ports different than those used for the outbound traffic. The outbound traffic triggers which ports inbound traffic is directed.

For example, a gaming server is accessed using UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions. In this case, port triggering must be used, since it conflicts with the following default firewall settings:

- The firewall blocks inbound traffic by default.
- The server replies to the Router's IP, and the connection is not sent back to the host, since it is not part of a session.

To resolve the conflict, a port triggering entry must be defined, which allows inbound traffic on UDP port 3333, only after a network host generated traffic to UDP port 2222. This results in accepting the inbound traffic from the gaming server, and sending it back to the network host which originated the outgoing traffic to UDP port 2222.

To use port triggering:

1. Select **Port Triggering** from the left side of any Security screen. The "Port Triggering" screen appears.

Port Triggering
Trigger opening of ports for incoming data.

NOTE: Only advanced technical users should use this feature

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
<input checked="" type="checkbox"/> L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating	
<input checked="" type="checkbox"/> TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating	

Add

2. Select either "Specify Protocol" or "Show All Services" from the drop-down list next to "Add."

3. Click **Add**. An “Edit Service” screen appears.

Edit Service

Service Name:

Outgoing Trigger Ports		
Protocol	Server Ports	Action
New Trigger Ports		

Incoming Ports to Open		
Protocol	Opened Ports	Action
New Opened Ports		

3. Specify the port triggering entries by clicking **New Trigger Ports** and **New Opened Ports** and entering the protocol and protocol number in the succeeding screens. For example, to set up port triggering for the scenario laid out on the previous page, the service ports would be set to UDP and 2222, while the opened ports would be set to UDP and 3333.

Remote Administration

The Router can be accessed and controlled not only from within the local network, but also from the Internet using remote administration.

To access, select **Remote Administration** from the left side of any Security screen. The “Remote Administration” screen appears.

Remote Administration

Attention
 With Remote Administration enabled, your network will be a risk from outside attacks.

Allow Incoming Access to the Telnet Server

☐ Using Primary Telnet Port (23)

☐ Using Secondary Telnet Port (8023)

☐ Using Secure Telnet over SSL Port (992)

Allow Incoming Access to the MegaControl Panel

☐ Using Primary HTTP Port (80)

☐ Using Secondary HTTP Port (8080)

☐ Using Primary HTTPS Port (443)

☐ Using Secondary HTTPS Port (8443)

Diagnostic Tools

☒ Allow Incoming ICMP Echo Requests (e.g. pings and ICMP traceroute queries)

☐ Allow Incoming UDP Traceroute Queries

Telnet

Telnet is used to create a command-line session and gain access to all system settings and parameters using a text-based terminal. Select the Telnet port to be used by clicking in the appropriate check box, then click **OK**.

MegaControl Panel

MegaControl Panel is used to obtain access to the Router's MegaControl Panel and gain access to all settings and parameters, using a web browser. Both secure (HTTPS) and non-secure (HTTP) access is available. Select the port to be used by clicking in the appropriate text box, then click **OK**.



Note: Telnet and MegaControl Panel remote administration access may be used to modify or disable firewall settings. Local IP addresses and other settings can also be changed, making it difficult or impossible to access the Router from the local network. Therefore, remote administration access to Telnet or MegaControl Panel services should be activated only when absolutely necessary.

Diagnostic Tools

Diagnostic Tools are used for troubleshooting and remote system management by a user or the ISP.



Note: Encrypted remote administration is performed using a secure SSL connection, and requires an SSL certificate. When accessing the Router for the first time using encrypted remote administration, a warning appears regarding certificate authentication because the Router's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue. Even though this message appears, the self-generated certificate is safe, and provides a secure SSL connection.

Website Blocking

The Router can be configured to block specific websites, preventing access to them from computers on the local network. Restrictions can also be applied to a comprehensive, automatically updated table of sites to which access is not recommended. To view the table of websites currently being blocked, select **Website Blocking** in any Security screen. To activate website blocking, click in the “Enable Website Blocking” check box.

The screenshot shows the 'Website Blocking' configuration window. At the top, it says 'Block access to specific websites for specific computers or devices that are connected to the network.' Below this is a note: 'Note: To activate the Website Blocking Feature, please ensure to check the box next to Enable Website Blocking'. There is a checkbox labeled 'Enable Website Blocking'. Below the checkbox is a table with five columns: 'Networked Computer / Device', 'Network Address', 'Blocked Website', 'Status', and 'Action'. The first row of the table has an 'Add' button in the first column. Below the table, it says 'Press the Refresh button to update the data.' At the bottom, there are five buttons: 'OK', 'Apply', 'Cancel', 'Resolve Now', and 'Refresh'.

To add a new website to the table:

1. Click **Add**. The “Blocked Website” screen appears.

The screenshot shows the 'Blocked Website' configuration window. It says 'Enter the website that you wish to block:'. There is a text input field labeled 'Blocked Website:'. Below this is a dropdown menu labeled 'Networked Computer / Device' with 'Any' selected. Below that is another dropdown menu labeled 'When should this rule occur ?' with 'Always' selected. At the bottom, there are two buttons: 'OK' and 'Cancel'.

2. Enter the website’s address (IP or URL). All pages within the website will also be blocked. If the website address has multiple IP addresses, the Router will resolve all additional addresses and automatically add them to the restrictions table.
3. To apply website blocking to a single computer or group of computers on the network, select them from the “Networked Computer/Device” drop-down list.

4. If website blocking needs to be active all the time, select **Always** from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times, select **Specify Schedule** and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual).



Note: Make sure the Router's date and time are set correctly for the local time zone.


5. Click **OK** to add the website to the table. The previous screen appears while the Router attempts to find the site. “Resolving...” appears in the “Status” column while the website is being located.
6. If the site is successfully located, “Resolved” appears in the Status column. If not, “Hostname Resolution Failed” appears. Click **Refresh** to update the status, if necessary. If the Router fails to locate the website, do the following:
 - Use a web browser to verify the website is available. If it is, the website address was entered incorrectly. See “Modifying a Website Address,” below.
 - If the website is not available, return to the Website Blocking screen at a later time and click **Resolve Now** to verify the website can be found and is blocked by the Router.

Modifying a Website Address

To modify a website address currently in the table:

1. Click the appropriate icon in the “Action” column. The “Blocked Website” screen appears.
2. Modify the website address, group, and schedule as necessary. Omit the “http://” at the beginning and the “/” at the end of the address.
3. Click **OK** to save changes.

Static NAT

 **Note:** A block of static IP addresses must be purchased from the ISP to configure this feature.

This option allows multiple static NAT IP addresses to be designated to devices on the network. Static NAT IP addresses allow devices behind a firewall and configured with private IP addresses appear to have public IP addresses on the Internet. This allows an internal host, such as a web server, to have an unregistered (private) IP address and still be reachable over the Internet. To do this:

1. Select **Static NAT** from any Security screen. The “Static NAT” screen appears.

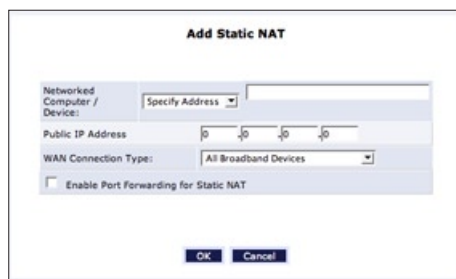


Static NAT

Static IP Mapping Table

ID	Networked Computer / Device	Public IP Address	WAN Connection Type	Status	Port Forwarding	Action
Add						

2. Click **Add**. The “Add Static NAT” screen appears.



Add Static NAT

Networked Computer / Device: Specify Address

Public IP Address:

WAN Connection Type: All Broadband Devices

☐ Enable Port Forwarding for Static NAT

3. Enter the name of the computer to be used as the local host, or, to enter a specific IP address, select **Specify Address** from the “Networked Computer/ Device” drop-down list and enter the IP address in the box on the right.
4. Enter a public IP address from the block of assigned public IP address (received from the ISP) in the “Public IP Address” text box.
5. Select a connection from the “WAN Connection Type” drop-down list.

6. Select the protocol that needs to be accessible from the public IP address by clicking in the check box next to “Enable Port Forwarding for Static NAT,” then selecting a protocol from the drop-down menu. Click **OK**, and **OK** again.

Repeat these steps to add more static IP addresses from the network.

Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. Specific input and output rules can be defined, the order of logically similar sets of rules controlled, and distinctions made between rules that apply to Internet and local network devices.

To access, select **Advanced Filtering** from any Security screen. The “Advanced Filtering” screen appears.

Advanced Filtering

NOTE: Only advanced technical users should use this feature.

Input Rule Sets: Manage all incoming traffic from the Internet

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
Initial Rules Add						
Network (Home/Office) Rules						
<input checked="" type="checkbox"/> 0	Any	192.168.1.1	Telnet -TCP Any -> 23 Telnet Secondary -TCP Any -> 8023 Telnet SSL -TCP Any -> 992	Drop	Active	
Add 						
Broadband Connection(Ethernet) Rules						
<input checked="" type="checkbox"/> 0	Any	224.0.0.0 / 240.0.0.0	Any	Drop	Active	
Add 						
Ethernet Rules Add						
WAN PPPOE Rules Add						
Final Rules Add						

Output Rule Sets: Manage all outbound traffic to the Internet

Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action
Initial Rules Add						
Network (Home/Office) Rules Add						
Broadband Connection(Ethernet) Rules Add						
Ethernet Rules Add						
WAN PPPOE Rules Add						
Final Rules Add						

Two sets of rules can be configured: input rules and output rules. Each set of rules comprises three subsets: initial rules, network devices rules, and final rules. These subsets determine the sequence by which the rules will be applied. Following is a description of the set ordering for inbound and outbound packets.

Inbound Packets - Input Rule Sets

- Initial rules
- All rules defined for the network device on which the packet is
- Local servers rules from the local server tab in the security screen
- Rules to accept all the packets on a device in case the firewall check box “Internet Connection Firewall” in the connection settings screen is unchecked
- Remote administration rules from the remote administration tab
- DMZ host rules from the DMZ tab
- Final rules

Outbound Packets - Output Rules Sets

- Initial rules
- All rules defined for the network device on which the packet is
- Rules to accept all the packets on a device in case the firewall check box “Internet Connection Firewall” in the connection settings screen is unchecked
- IP/hostname filtering rules and access control rules from the tabs in the security screen
- Final rules

There are numerous rules automatically inserted by the firewall in order to provide improved security and block harmful attacks.

To configure advanced filtering rules, click **Add** next to the rule title. The “Add Advanced Filter” screen appears.

The screenshot shows the 'Add Advanced Filter' configuration window. It is divided into several sections: 'Matching', 'Operation', and 'Logging'. In the 'Matching' section, 'Source Address' and 'Destination Address' are both set to 'Any' via dropdown menus, and 'Protocol' is also set to 'Any'. The 'Operation' section has three radio button options: 'Drop' (selected), 'Reject', and 'Accept'. The 'Drop' option is accompanied by a red minus icon. The 'Accept' option is accompanied by a green plus icon. The 'Logging' section has a checkbox for 'Log Packets Matched by This Rule' which is currently unchecked, and a dropdown for 'When should this rule occur?' set to 'Always'. At the bottom, there are 'OK' and 'Cancel' buttons.

To add an advanced filtering rule, define the following rule parameters:

Matching

To apply a firewall rule, a match must be made between IP addresses or ranges and ports. Use the “Source Address” and “Destination Address” drop-down lists to define the coupling of source and destination traffic. Port matching will be defined when selecting protocols. For example, if the FTP protocol is selected, port 21 will be checked for matching traffic flow between the defined source and destination IPs.

Operation

This is where the action the rule will take is defined. Select one of the following radio buttons:

- **Drop** - Deny access to packets that match the source and destination IP addresses and protocol ports defined in “Matching.”
- **Reject** - Deny access to packets that match the source and destination IP addresses and protocol ports defined in upper section of the screen, and send an ICMP error or a TCP reset to the origination peer.
- **Accept** - Allow access to packets that match the source and destination IP addresses and protocol ports defined in upper section of the screen. The data transfer session will be handled using Stateful Packet Inspection (SPI).
- **Accept Packet** - Allow access to packets that match the source and destination IP addresses and protocol ports defined in upper section of the screen. The data transfer session will not be handled using Stateful Packet Inspection (SPI), so other packets that match this rule will not be automatically allowed access. This setting is useful when creating rules that allow broadcasting.

Logging

Click in this check box to add entries relating to this rule to the security log.

Scheduler (When should this rule occur?)

If advanced filtering needs to be active all the time, select “Always” from the “When should this rule occur?” drop-down list. If the rule will only be active at certain times select **Specify Schedule** and click **Add**. Then, add a schedule rule (for more details about schedule rules, see the “Advanced Settings” chapter of this manual)

Security Log

The security log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (MegaControl Panel or Telnet terminal), firewall configuration, and system start-up.

To access the security log, select **Security Log** from any Security screen. The “Security Log” screen appears.

Security Log			
<div> Close Clear Log Settings Save Log Refresh </div>			
Press the Refresh button to update the data.			
Time	Event	Event-Type	Details
Jan 2 21:14:18 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 2 21:14:18 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 2 21:14:03 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 2 21:14:03 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 01:45:20 2003	WBM Login	User authentication success	Username: admin [repeated 17 times, last time on Jan 2 21:08:07 2003]
Jan 1	WBM	User	Invalid password. Username:

Time

The time (based on the Router's date and time settings) the event occurred.

Event

There are five kinds of events listed in the system log:

- **Inbound Traffic** - a result of an incoming packet
- **Outbound Traffic** - a result of an outgoing packet.
- **Firewall Setup** - configuration message
- **WBM Login** - a user logged in to WBM
- **CLI Login** - a user logged in to the command line interface via Telnet

Event-Type

Displays a textual description of the event.

Details

The “Details” column displays more information about the packet or the event, such as protocol, IP addresses, ports, etc. The following are the available event types that can be recorded in the security log:

- **Firewall internal** - from the firewall internal mechanism, in case this event-type is recorded, an accompanying explanation will be added.
- **Firewall status changed** - the firewall changed status from up to down or the vice versa, as specified in the event type description.
- **STP packet** - an STP (Spanning Tree Protocol) packet has been accepted/rejected.
- **Illegal packet options** - the options field in the packet’s header is either illegal or forbidden.
- **Fragmented packet** - a fragment has been rejected.
- **WinNuke protection** - a WinNuke attack has been blocked.
- **ICMP replay** - an ICMP (Internet Control Message Protocol) replay message has been blocked.
- **ICMP redirect protection** - an ICMP redirected message has been blocked.
- **Packet invalid in connection** - an invalid connection packet has been blocked.
- **ICMP protection** - a broadcast ICMP message has been blocked.
- **Broadcast/Multicast protection** - a packet with a broadcast/multicast source IP has been blocked.
- **Spoofing protection** - a packet from the Internet with a source IP belonging the local network has been blocked.
- **DMZ network packet** - a packet from a demilitarized zone network has been blocked.

- **Trusted device** - a packet from a trusted device has been accepted.
- **Default policy** - a packet has been accepted/blocked according to the default policy.
- **Remote administration** - a packet designated for the Router management has been accepted/blocked.
- **Access control** - a packet has been accepted/blocked because of an access control rule.
- **Parental control** - a packet has been blocked because of parental control.
- **NAT out failed** - NAT failed for this packet.
- **DHCP request** - the Router sent a DHCP request (depends on the distribution)
- **DHCP response** - the Router received a DHCP response (depends on the distribution)
- **DHCP relay agent** - a DHCP relay packet has been received (depends on the distribution)
- **IGMP packet** - an IGMP packet has been accepted.
- **Multicast IGMP connection** - a multicast packet has been accepted.
- **PPTP connection** - a packet inquiring whether the Router is ready to receive a PPTP connection has been accepted.
- **AUTH:113 request** - an outbound packet for AUTH protocol has been accepted (for maximum security level).
- **IPV6 over IPV4** - an IPv6 over IPv4 packet has been accepted.
- **ARP** - an ARP packet has been accepted.
- **PPP Discover** - a PPP discover packet has been accepted.
- **PPP Session** - a PPP session packet has been accepted.
- **802.1Q** - a 802.1Q (VLAN) packet has been accepted.
- **Outbound Auth1X** - an outbound Auth1X packet has been accepted.
- **IP Version 6** - an IPv6 packet has been accepted.

- **Router initiated traffic** - all traffic the Router initiates is recorded.
- **Maximum security enabled service** - a packet has been accepted because it belongs to a permitted service in the maximum security level.
- **SynCookies Protection** - a SynCookies packet has been blocked.
- **ICMP Flood Protection** - a packet has been blocked, stopping an ICMP flood.
- **UDP Flood Protection** - a packet has been blocked, stopping a UDP flood.
- **Service** - a packet has been accepted because of a certain service, as specified in the event type.
- **Advanced Filter Rule** - a packet has been accepted/blocked because of an advanced filter rule.
- **Fragmented packet, header too small** - a packet has been blocked because, after defragmentation, the header was too small.
- **Fragmented packet, header too big** - a packet has been blocked because, after defragmentation, the header was too big.
- **Fragmented packet, bad align** - a packet has been blocked because, after defragmentation, the packet was badly aligned.
- **Fragmented packet, packet too big** - a packet has been blocked because, after defragmentation, the packet was too big.
- **Fragmented packet, packet exceeds** - a packet has been blocked because, after defragmentation, the packet exceeded.
- **Fragmented packet, no memory** - a fragmented packet has been blocked because there is no memory for fragments.
- **Fragmented packet, overlapped** - a packet has been blocked because, after defragmentation, there were overlapping fragments.
- **Defragmentation failed** - the fragment has been stored in memory and blocked until all fragments have arrived and defragmentation can be performed.
- **Connection opened** - debug message regarding connection.
- **Wildcard connection opened** - debug message regarding connection.

- **Wildcard connection hooked** - debug message regarding connection.
- **Connection closed** - debug message regarding connection.
- **Echo/Chargen/Quote/Snork protection** - a packet has been blocked due to Echo/Chargen/Quote/Snork protection.
- **First packet in connection is not a SYN packet** - a packet has been blocked due to a TCP connection that started without a SYN packet.
- **Error : No memory** - a new connection has not been established because of lack of memory.
- **NAT Error : connection pool is full. No connection created** - a connection has not been created because the connection pool is full.
- **NAT Error: No free NAT IP** - no free NAT IP, so NAT has failed.
- **NAT Error: Conflict Mapping already exists** - a conflict occurred because the NAT mapping already exists, so NAT failed.
- **Malformed packet: Failed parsing** - a packet has been blocked because it is malformed.
- **Passive attack on ftp-server: Client attempted to open Server ports** - a packet has been blocked.
- **FTP port request to 3rd party is forbidden (Possible bounce attack)** - a packet has been blocked.
- **Firewall Rules were changed** - the firewall rule set has been modified.
- **User authentication** - a message arrived during login time, including both successful and failed authentication.

Security Log Settings

To view or change the security log settings:

1. Click **Settings** in the Security Log screen. The “Security Log Settings” screen appears.

Security Log Settings

Accepted Events

- ☐ Accepted Incoming Connections
- ☐ Accepted Outgoing Connections

Blocked Events

- ☐ All Blocked Connection Attempts
- ☐ WinNuke
- ☐ Defragmentation Error
- ☐ Blocked Fragments
- ☐ Syn Flood
- ☐ Echo Charpen
- ☐ Multicast/Broadcast
- ☐ Spoofed Connection
- ☐ Packet Illegal Options
- ☐ UDP Flood
- ☐ ICMP Replay
- ☐ ICMP Redirect
- ☐ ICMP Multicast
- ☐ ICMP Flood

Other Events

- ☐ Remote Administration Attempts
- ☐ Connection States

Log Buffer

- ☐ Prevent Log Overrun

OK **Apply** **Cancel**

2. Select the type of activities that will generate a log message:
 - **Accepted Incoming Connections** - activating this check box generates a log message for each successful attempt to establish an inbound connection to the local network.
 - **Accepted Outgoing Connections** - activating this check box generates a log message for each successful attempt to establish an outgoing connection to the public network.
3. Select the type of blocked events to be listed in the log:
 - **All Blocked Connection Attempts** - activating this check box generates log messages for all blocked events.
 - **Other Blocked Events** - if “All Blocked Connection Attempts” is unchecked, select specific blocked events from this list to generate log messages.

- 4.** Click in the “Remote Administration Attempts” check box to write a log message for each remote-administration connection attempt, whether successful or not.
- 5.** Click in the “Connection States” check box to track connection handling by the firewall and Application Level Gateways (ALGs).
- 6.** Click **OK** to save changes.

This page left intentionally blank.

Using Parental Controls

6

The abundance of harmful information on the Internet poses a serious challenge for employers and parents alike - “How can I regulate what my employee/child does on the Internet?” The Broadband Router’s Parental Controls allows users to regulate, control, and monitor Internet access. By classifying and categorizing online content, it is possible to create numerous Internet access policies and easily apply them to networked computers.

Activating Parental Controls

The Router’s Parental Control service is provided by Surf Control (<http://www.surfcontrol.com/>), a company specializing in Internet content filtering. A subscription to this service must be activated to use the Router’s Parental Controls. To subscribe through the Router’s MegaControl Panel:

1. Click **Parental Control** from the top of the Home screen.
2. If no subscription has been activated, or the subscription has expired, the “General” screen appears.

General

Subscribe
[Click Here to Initiate and Manage your Subscription](#)

Activate
☐ Enable Web Content Filtering

Subscription Status
Status: Disabled
Partner ID: 6005
License Code: 000fb3e2d7c6

OK Apply Cancel

Powered by
SurfControl

3. If the “Enable Web Content Filtering” check box in the “Activate” section is not checked, click in the check box to activate.
4. Click **Click Here to Initiate and Manage your Subscription** in the “Subscribe” section.

5. The Surf Control subscription site will then be displayed in a new browser window. Follow the instructions on the website and subscribe or enroll for a free trial. A verification E-mail will be sent. Click on the link in the verification E-mail. About 20 seconds after clicking on the verification link, the subscription will be activated.
6. Return to the MegaControl Panel and click **Parental Control**. The “Filtering Policy” screen appears, with a subscription expiration date at the top. If not, select the “Advanced Options” tab, then **Refresh Servers**. Wait a few seconds and repeat this step.

Disabling Web Content Filtering

To disable the Router’s Web content filtering:

1. From the MegaControl Panel, click **Parental Control**.
2. Clear the “Enable Web Content Filtering” check box.
3. Click **OK**.

Creating a Filtering Policy

A filtering policy defines what sites will be blocked, based on their category. The Router provides four built-in policies:

- **Block All** - blocks all access to the Internet
- **Allow All** - allows unlimited Internet access
- **Home** - blocks sites under the “Child Protection” category
- **Employee** - blocks sites from non work-related categories

These policies can be set from the “Default Filtering Policy” drop-down list in the “Filtering Policy” screen. To view or edit the “Home” and “Employee” policies, click their respective links in the Filtering Policy screen.

Custom filtering policies can also be created. To do so:

1. From the MegaControl Panel, click **Parental Control**.

2. Click **Filtering Policy** from the list on the left side of the screen. The “Filtering Policy” screen appears.

Filtering Policy

Default Filtering Policy: Allow All

LAN Computer Policy

LAN Computer	IP Address	Policy	When should this rule occur?	Action
Add a LAN Computer				

Filtering Policy

Policy	Description	Action
Home	At Home	
Employee	Work Environment	
Add a Policy		

OK
Apply
Cancel
Refresh

3. Click **Add a Policy** to generate another “Filtering Policy” screen.

Filtering Policy

Rule Name: Policy

Description:

Blocked Categories

☒
Child Protection

☐
Recreation & Entertainment

☐
Personal Business

☐
Bandwidth Control

☐
Advertisements

☐
Chat

☒
Remote Proxies and Hosting Sites (Possibly untrusted sources)

☐
Other

Websites and URL Keywords Filtering

Block Access to These Websites and URL Keywords ▼

Specify a list of Websites separated by spaces.

Specify a list of URL Keywords separated by spaces.

OK
Cancel

4. Enter a name for the new policy in the “Rule Name” text box.
5. Enter a description of the new policy in the “Description” text box.
6. Select the content filtering check boxes that represent content to be blocked in the “Blocked Categories” section.
7. Click **OK** to save the new policy.

Selecting a category will automatically select all its sub-categories and deselecting a category will automatically deselect its sub-categories. To make a more refined selection of filtering options, click on the “+” next to each category to display a list of its sub-categories. A click on the resulting “-” will revert the category to its previous display. Clicking the “-” of a category will only be possible if all its sub-categories are either checked or unchecked.

Websites and URL Filtering

Additional filtering (by website URL or URL keyword) can be done using the “Websites and URL Filtering” section of the Policy Filtering screen. To do this:

1. Select either **Block Access to These Websites and URL Keywords** or **Allow Access to These Websites and URL Keywords** from the drop-down list.
2. In the “Specify a list of Websites separated by spaces” text box, enter the URLs of the websites to be blocked or accessed. Separate each discrete URL with a space.
3. In the “Specify a list of URL Keywords separated by spaces” text box, enter the URL keywords to be blocked or accessed.
4. Click **OK** to save. If “Block Access to These Websites and URL Keywords” was chosen in step 1, all websites listed and all other websites with the keywords listed in their URLs will be blocked. If “Allow Access to These Websites and URL Keywords” was chosen in step 1, only the websites listed and other websites with the keywords listed in their URLs will be allowed to be accessed.

Applying the Filtering Policy

Once different filtering policies have been created, either define a default policy that will be applied to all networked computers, or apply different policies to individual computers separately.

LAN Filtering Policy

To select a default filtering policy for the local network, select the policy name from the “Default Policy” drop-down list, located in the Filtering Policy screen, and click **Apply**.

PC Filtering Policy

To apply separate policies to individual home computers, do the following:

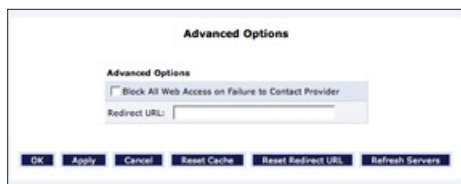
1. In the Filtering Policy screen, click **Add a LAN Computer**. The “LAN Computer Policy” screen appears.



2. Enter the name or IP address of the networked computer to which a policy will be applied.
3. Select the policy to apply from the “Policy” drop-down list.
4. If schedules have been defined, specify when this policy will be active by selecting the schedule to apply from the “Schedule” drop-down list. Otherwise, select **Specify Schedule**, click **Add**, then select the time frame.
5. Click **OK**.
6. In the Filtering Policy screen, use the check-box next to the computer name to enable or disable the policy for a particular computer.
7. Click **OK**.

Advanced Options

The “Advanced Options” screen contains features providing additional Web filtering security.



Provider Consulting Failure

To decide whether to allow or block a specific website, the filter service provider is consulted about the website's category. If an error occurs consulting the provider, the user can decide whether to block or allow access to all sites.

1. Click **Parental Control** in the Home screen.
2. Click **Advanced Options** from the left side of the screen.
3. Click in the “Block All Web Access on Failure to Contact Provider” check box to block access to all sites, in case the provider is not responding.
4. Click **OK**.

Redirect URL

When a site is blocked, the Router's “Blocked Access” page is displayed, specifying the requested URL and the reason it was blocked.

To specify an alternative page to be displayed when a site is blocked, enter the URL of the alternative page in the “Redirect URL” text box .

Statistics

The Router's MegaControl Panel monitors content filtering statistics. Statistics include a record of:

- Access attempts
- Accessed URLs
- Blocked URLs
- URLs that were accessed from cache

To view content filtering statistics:

1. Click **Parental Control** in the Home screen.
2. Click **Statistics** from the left side of the General screen. The “Statistics” screen appears.



Note: When Parental Control is enabled, HTTP services cannot be blocked by the Security Access Control feature.

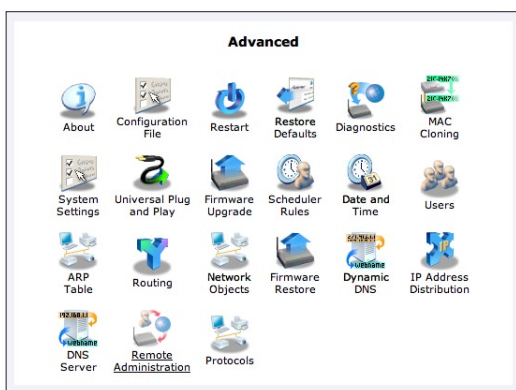
This page left intentionally blank.

Using Advanced Settings

7

The “Advanced” section of the Broadband Router’s MegaControl Panel is intended primarily for more advanced users. Some changes to settings within this section could adversely affect the operation of the Router and the local network, and should be made with caution.

To access the Router’s Advanced Settings, click **Advanced** at the top of the Home screen, which generates the “Advanced” screen.



The following settings are explained in this chapter:

About - view information about the Router

Configuration File - manage configuration files

Restart - restart the Router

Restore Defaults - reset the Router to its default settings

Diagnostics - perform diagnostic tests on the Router

MAC Cloning - clone MAC addresses

System Settings - modify the system’s settings

Universal Plug and Play - configure Universal Plug and Play settings

Firmware Upgrade - download and install new versions of the Router's firmware

Scheduler Rules - schedule firewall activation

Date and Time - set the local date and time

Users - create and manage remote users

ARP Table - display active devices and their IP and MAC addresses, etc.

Routing - manage routing policies

Network Objects - create and manage network objects (discrete LAN subsets)

Firmware Restore - restores firmware to previous version loaded in flash memory

Dynamic DNS - configure Dynamic DNS settings

IP Address Distribution - manage the IP addresses of devices on the network

DNS Server - manage the local (LAN) network for host name and IP address

Remote Administration - configure and manage remote administration policies

Protocols - manage and create open ports for various Internet protocols or customize an application

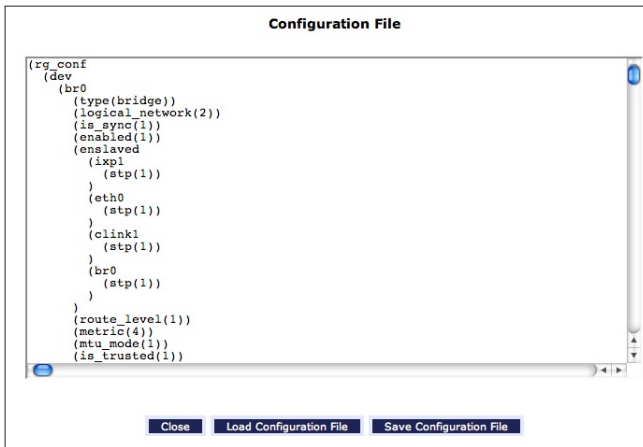
About

To view technical information regarding the Router, click **About** in the Advanced screen. The “About” screen appears, displaying various technical aspects concerning the Router.

Configuration File

Use the Router’s Configuration File feature to view, save, and load configuration files, which are used to backup and restore the Router’s current configuration: To do this:

1. Click **Configuration File** in the Advanced screen. The “Configuration File” screen appears.

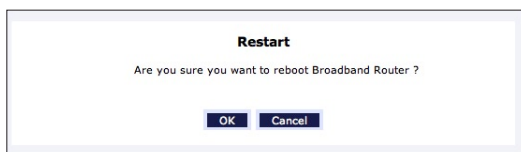


3. Click **Load Configuration File** at the bottom of the screen to load the previous configuration from a file and restart the Router.
4. Click **Save Configuration File** at the bottom of the screen to backup the current configuration to a file.

Restart

To restart the Router:

1. Click **Restart** in the Advanced screen. The “Restart” screen appears.



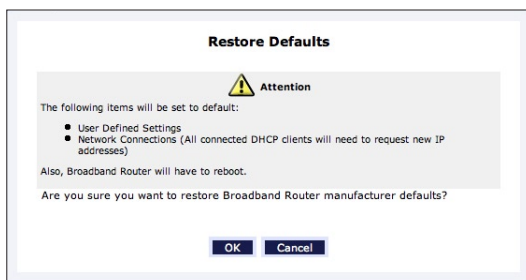
2. Click **OK** to restart the Router. This may take up to one minute.

To reenter the MegaControl Panel after restarting the Router, click the web browser's “Refresh” button.

Restoring Default Settings

If the Router's factory default settings need to be restored (to build a new network from the beginning, for example), use the following procedure:

1. Click **Restore Defaults** in the Advanced screen. The “Restore Defaults” screen appears.



2. Click **OK** to restore the Router's factory default settings.



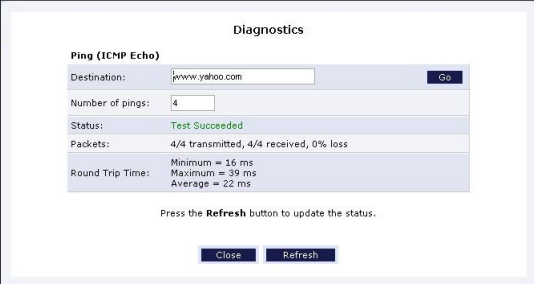
Note: All of the Router's settings and parameters will be restored to their default values after performing the Restore Default procedure. This includes the administrator password; a user-specified password will no longer be valid.

Diagnostics

The Diagnostics screen can assist in testing network connectivity. This feature pings (ICMP echo) an IP address and displays the results, such as the number of packets transmitted and received, round trip time, and success status.

To diagnose network connectivity:

1. Click **Diagnostics** from the Advanced screen. The “Diagnostics” screen appears.



The screenshot shows a window titled "Diagnostics". Inside, there is a section titled "Ping (ICMP Echo)". Below this, there are several fields and buttons:

- Destination:** A text box containing "www.yahoo.com" and a "Go" button to its right.
- Number of pings:** A text box containing the number "4".
- Status:** A label followed by "Test Succeeded" in green text.
- Packets:** A label followed by "4/4 transmitted, 4/4 received, 0% loss".
- Round Trip Time:** A label followed by three lines of text: "Minimum = 16 ms", "Maximum = 39 ms", and "Average = 22 ms".

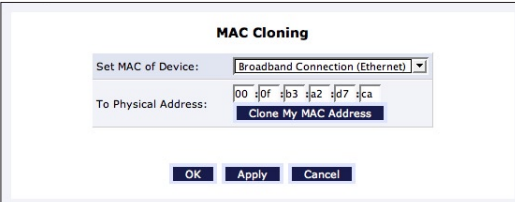
Below these fields, there is a line of text: "Press the **Refresh** button to update the status." At the bottom of the window, there are two buttons: "Close" and "Refresh".

2. Enter the IP address or domain name to be tested in the “Destination” field.
3. Click **Go**.
4. In a few seconds, diagnostics statistics will be displayed. If no new information is displayed, click **Refresh**.

MAC Cloning

A MAC (Media Access Control) address is a unique hexadecimal code that identifies a device on a network. All networkable devices have a MAC address. When replacing another network device with the Router, the installation process can be simplified by copying the MAC address of the existing computer to the Router. To do this:

1. Click **MAC Cloning** in the Advanced screen. The “MAC Cloning” screen appears.



The screenshot shows a window titled "MAC Cloning". Inside the window, there is a section labeled "Set MAC of Device:" with a dropdown menu currently showing "Broadband Connection (Ethernet)". Below this, there is a section labeled "To Physical Address:" with a text box containing the hexadecimal address "00 :0f :d3 :a2 :d7 :ca". A button labeled "Clone My MAC Address" is positioned below the text box. At the bottom of the window, there are three buttons: "OK", "Apply", and "Cancel".

2. Enter the **MAC** address to be cloned in the “To Physical Address” text boxes.
3. Click **Clone My MAC Address**. The Router will now have the new MAC address.

System Settings

Clicking **System Settings** in the Advanced screen generates the “System Settings” screen, where various system and management parameters can be configured.

System Settings

System

Broadband Router's Hostname:

Local Domain:

Actiontec MegaControl Panel

☒ Automatic Refresh of System Monitoring Web Pages

☒ Prompt for password When Accessing via LAN

☒ Warn User Before Network Configuration Changes

Session Lifetime: Seconds

Remote Administration

Management Application Ports

Primary HTTP Management Port:

Secondary HTTP Management Port:

Primary HTTPS Management Port:

Secondary HTTPS Management Port:

Primary Telnet Port:

Secondary Telnet Port:

Secure Telnet over SSL Port:

System Logging

☒ Enable Logging

☒ Low Capacity Notification Enabled

Allowed Capacity Before Email Notification: %

System Log Buffer Size: KB

Remote System Notify Level:

Security Logging

☒ Enable Logging

☒ Low Capacity Notification Enabled

Allowed Capacity Before Email Notification: %

Security Log Buffer Size: KB

Remote Security Notify Level:

Outgoing Mail Server

Server:

From Email Address:

Port:

☐ Server Requires Authentication

Auto WAN Detection

☒ Enabled

PPP Timeout: Seconds

DHCP Timeout: Seconds

Number of Cycles:

☒ Auto Detection Continuous Trying

System

Use the “System” section of this screen to configure the following two option

Broadband Router's Hostname

Specify the Router's host name by entering it into the this text box. The host name is also the Router's URL address, so it can be entered here rather than 192.168.1.1.

Local Domain

Specify the network's local domain by entering it into this text box.

Actiontec MegaControl Panel

Use this section to configure the following:

Automatic Refresh of System Monitoring Web Pages

Click in this check box to activate the automatic refresh of system monitoring web pages.

Prompt for Password When Accessing via LAN

Click in this check box to force users who try to access the MegaControl Panel from the LAN (local area network) to enter the password.

Warn User Before Network Configuration Changes

Click in this check box to activate user warnings before network configuration changes take effect.

Session Lifetime

Enter the time period, in seconds, between MegaControl Panel web page refreshes.

Management Application Ports

This section allows the following management application ports to have their default port numbers to be changed:

- Primary/secondary HTTP ports
- Primary/secondary HTTPS ports
- Primary/secondary Telnet ports
- Secure Telnet over SSL ports

System Logging

Use this section to configure the following system log options.

Enable Logging

Click in this check box to activate system logging.

Low Capacity Notification Enabled

Click in this check box to activate low capacity notification (works in tandem with “Allowed Capacity Before Email Notification” and “System Log Buffer Size” options).

Allowed Capacity Before Email Notification

Enter the percentage of system log buffer capacity reached to trigger an E-mail notification.

System Log Buffer Size

Enter the size of the system log buffer in this text box.

Remote System Notify Level

This feature is used to specify the type of information received for remote system logging. Options include **None**, **Error**, **Warning**, and **Information**.

Security Logging

Use this section to configure the following security log options.

Enable Logging

Click in this check box to activate security logging.

Low Capacity Notification Enabled

Click in this check box to activate low capacity notification (works in tandem with “Allowed Capacity Before Email Notification” and “Security Log Buffer Size” options).

Allowed Capacity Before Email Notification

Enter the percentage of security log buffer capacity reached to trigger an E-mail notification.

Security Log Buffer Size

Enter the size of the security log buffer in this text box.

Remote System Notify Level

This feature is used to specify the type of information received for security logging. Options include **None**, **Error**, **Warning**, and **Information**.

Outgoing Mail Server

Use this section to configure the outgoing mail server options. This server is used format and send system and security log E-mail notifications.

Server

Enter the host name of the outgoing (SMTP) server in this text box.

From Email Address

E-mail notifications require a “from” address. Enter a “from” E-mail address in this text box.

Port

Enter the port number of the E-mail server in this text box.

Server Requires Authentication

If the E-mail server requires authentication, click in this check box, then enter a user name and password in the “User Name” and “Password” text boxes that appear.

Auto WAN Detection

When activated, Auto WAN Detection causes the Router to automatically search for a WAN connection.

Enable Logging

Clicking in this check box activates automatic WAN detection.

PPP Timeout

Enter the amount of time (in seconds) before the Router stops attempting to establish a broadband PPP connection.

DHCP Timeout

Enter the amount of time (in seconds) before the Router stops attempting to establish a broadband DHCP connection.

Number of Cycles

Enter the number of times the Router attempts to detect a broadband PPP and DHCP connection.

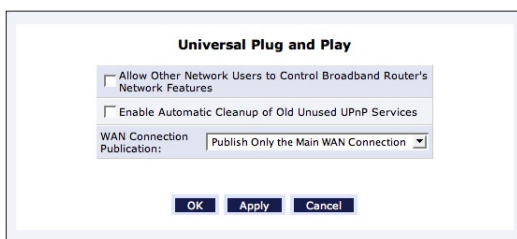
Auto Detection Continuous Trying

Click in this check box to cause the Router to indefinitely search for a broadband connection.

Universal Plug and Play (UPnP)

To access the UPnP settings perform the following:

1. Click **Universal Plug and Play** in the Advanced screen. The “Universal Plug and Play” settings screen appears.



2. Click in the “Allow Other Network Users to Control Broadband Router’s Network Features” check box to enable UPnP and allow UPnP services to be defined on any of the network hosts.
3. Click in the “Enable Automatic Cleanup of Old Unused UPnP Services” check box to enable automatic cleanup of invalid rules. When enabled, this feature checks validity of all the UPnP services and rules every five minutes. Any old and not used UPnP defined service is removed, unless any user defined rule depends on it. Since there is a maximum limitation on the number of UPnP defined services (256), enable the cleanup feature if the limit is in danger of being exceeded.
4. Select whether all WAN connections, or only the main WAN connection, will have UPnP active, from the “WAN Connection Publication” drop-down list.

UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP application (e.g. messenger). Thus, if running a boingo, services may often not be deleted, and will eventually lead to exhaustion of rules and services, and no new services can be defined. In this scenario, the cleanup feature will find the invalid services and remove them, preventing services exhaustion.

Firmware Upgrade

The Router offers a built-in mechanism for upgrading its firmware without losing custom configurations and settings. There are two methods for upgrading the firmware:

- **Upgrading from a local computer** - use a software image file pre-downloaded to the computer's disk drive or located on the accompanying evaluation CD.
- **Upgrading from the Internet** - use this method to upgrade the Router's firmware by remotely downloading an updated software image file.

Upgrading From a Local Computer

To upgrade from a local computer:

1. Click **Firmware Upgrade** from the Advanced screen. The "Firmware Upgrade" screen appears.

Firmware Upgrade

Visit upgrade.actiontec.com for upgrade support, upgrade options and information.

Current Version: 4.0.16.1.41.4

Upgrade From the Internet:

Automatic Check Disabled

Check at URL

Check Now

Status: **Cannot resolve hostname.**

Internet Version: No new version available

Force Upgrade

Upgrade From a Computer in the Network:

Select an updated Broadband Router firmware file from a computer's hard drive or CD on the network

Upgrade Now

Press the **Refresh** button to update the status.

OK **Apply** **Cancel** **Refresh**

2. In the “Upgrade From a Computer in the Network” section, click **Upgrade Now**. The “Upgrade From a Computer in the Network” screen appears.



3. Enter the path of the software image file, or press the “Browse” button to browse for the file, and click **OK**. Make sure to only use files with an “rmt” extension when performing the firmware upgrade procedure.
4. When loading is completed, a confirmation screen appears, asking whether to upgrade to the new version. Click **OK**. The upgrade process begins and should take no longer than one minute to complete.

At the conclusion of the upgrade process the Router automatically reboots. The new firmware will run, maintaining any custom configurations and settings.

Upgrading From the Internet

The Router’s firmware can be automatically updated via the Internet. From the drop-down list next to the globe icon near the top of the Firmware Upgrade screen, a list of options appears, as described below.

Automatically Check and Upgrade

If “Automatically Check for New Version and Upgrade Broadband Router” is selected, enter the period of time the Router checks for a new upgrade, and the URL at which to get the upgrade, in the appropriate text boxes. The Router will then check at each time interval for upgrades and, if one is available, upgrade the Router’s firmware.

Automatically Check and Send E-mail

If “Automatically Check for New Version and Notify via Email” is selected, enter the period of time the Router checks for a new upgrade, and the URL at which to get the upgrade, in the appropriate text boxes. The Router will then check at each time interval for firmware upgrades and, if one is available, send an E-mail to the E-mail address listed in the System Settings.

Automatic Check Disabled

If “Automatically Check Disabled” is selected, the Router will not automatically check for firmware upgrades.

Manual Checking and Upgrading

To manually upgrade the Router’s firmware:

1. Click **Check Now** in the Firmware Upgrade screen.
2. If a new version is available, click **Force Upgrade**. A download process will begin. When downloading is completed, a confirmation screen appears, asking whether to upgrade to the new version.
3. Click **OK**. The upgrade process will begin and should take no longer than one minute to complete.

At the conclusion of the upgrade process the Router automatically reboots. The new firmware runs, maintaining any custom configurations and settings.

Scheduler Rules

Scheduler rules are used for limiting the activation of firewall rules to specific time periods, either for days of the week, or for hours of each day.

To define a rule:

1. Make sure the Router's date and time are set correctly. To do this, see the "Date and Time" section in this chapter.
2. Click **Scheduler Rules** in the Advanced screen. The "Scheduler Rules" screen appears.

Scheduler Rules			
Name	Settings	Status	Action
Add			

Close Refresh

3. Click **Add**. The "Set Rule Schedule" screen appears.

Set Rule Schedule

Rule Name: Scheduler Rule

Rule Settings

☒ Rule will be active at the scheduled time.

☐ Rule will be inactive at the scheduled time.

Rule Schedule	Action
Add Rule Schedule	

OK Cancel

4. Enter a name for the rule in the "Rule Name" text box.
5. Specify if the rule will be active or inactive during the designated time period by clicking the appropriate "Rule Settings" radio button.

6. Click **Add Rule Schedule**. The “Edit Rule Schedule” screen appears.

Edit Rule Schedule

Days of Week

<input type="checkbox"/> Monday
<input type="checkbox"/> Tuesday
<input type="checkbox"/> Wednesday
<input type="checkbox"/> Thursday
<input type="checkbox"/> Friday
<input type="checkbox"/> Saturday
<input type="checkbox"/> Sunday

Hours Range

Start	End	Action
New Hours Range Entry		

OK **Cancel**

7. Select or active or inactive days of the week by clicking in the appropriate text boxes.
8. If applicable, click **New Hours Range Entry** to define an active/inactive hourly range. The “Edit Hour Range” screen appears. Enter a start and end time in the appropriate text boxes.

Edit Hour Range

NOTE: Use military time to edit the hour range. (e.g. 2:30pm = 14:30)

Start time:	00 :00
End time:	00 :00

OK **Cancel**

9. Click **OK**.



Note: Make sure the Router’s date and time settings are properly configured for the time zone.

Date and Time

To configure date, time, and daylight savings time settings perform the following:

1. Click **Date and Time** in the Advanced screen. The “Date and Time” screen appears.

Date and Time

Localization

Local Time: Jan 1, 2003 21:26:10

Time Zone: Eastern_Time (GMT-05:00) ▼

Daylight Saving Time

☒ Enabled

Start: Mar 28 00 : 00

End: Oct 01 00 : 00

Offset: 60 Minutes

Automatic Time Update

☒ Enabled

Protocol: ☐ Time Of Day (TOD) ☒ Network Time Protocol (NTP)

Update Every: 24 Hours Sync Now

Time Server	Action
ntp.actiontec.com	
Add	

Status: Got time update from server, Last Update: Fri Apr 14 13:27:45 2006

Press the **Refresh** button to update the status.

OK Apply Cancel Clock Set Refresh

2. Select the local time zone from the drop-down list. The Router can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for a time zone are not automatically detected, the following fields will be displayed:
 - **Enabled** - Select this check box to enable daylight saving time.
 - **Start** - Date and time when daylight saving starts.
 - **End** - Date and time when daylight saving ends.
 - **Offset** - The time amount daylight saving time changes.

To perform an automatic time update:

1. Click in the “Enabled” check box in the “Automatic Time Update” section.
2. Select the protocol to be used to perform the time update by selecting either the “Time of Day” or “Network Time Protocol” radio button.
3. Specify how often to perform the update in the “Update Every” text box.
4. Define time server addresses by clicking **Add** on the bottom of the “Automatic Time Update” section and entering the IP address or domain name of the time server in the “Time Server Settings” screen.

Users

To manage individual users:

1. Click **Users** in the Advanced screen, which generates the “Users” screen.



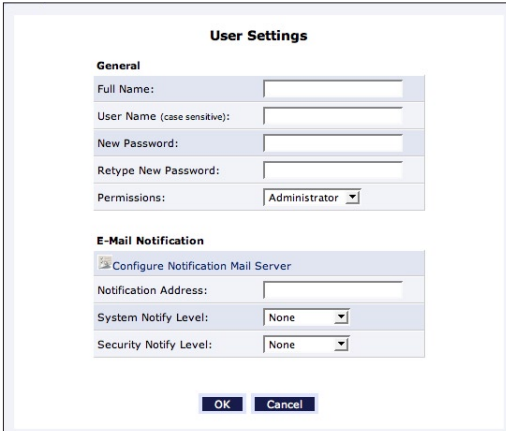
Users

Users

Full Name	User Name	Permissions	Action
Administrator	admin	Administrator	
New User			

Close

2. Click **New User**, which generates the “User Settings” screen.



User Settings

General

Full Name:


User Name (case sensitive):

New Password:

Retype New Password:

Permissions: Administrator ☒

E-Mail Notification

 Configure Notification Mail Server

Notification Address:

System Notify Level: None

Security Notify Level: None

OK **Cancel**

When adding a user, specify the following parameters:

- **Full Name** - The user's full name.
- **User Name** - The name a remote user will use to access the home or office network. This entry is case-sensitive.
- **New Password/Retype New Password** - The password for the user (and enter again to confirm).
- **Permissions** - The level of access the user is allowed. Options include **Administrator** or **Limited**.
- **E-mail Notification** - E-mail notification can be used to receive indications of system events for a predefined severity classification. The available types of events are "System" or "Security" events. The available severity of events are **Error**, **Warning**, and **Information**.

To configure E-mail notification for a specific user:

1. Make sure an outgoing mail server has been configured in "System Settings". If not, click **Configure Notification Mail Server** to configure the outgoing mail server.
2. Enter the user's E-mail address in the "Notification Address" text box.
3. Select the "System" and "Security" notification levels in the "System Notify Level" and "Security Notify Level" drop-down lists.



Note: Changing any of the user parameters will prompt the connection associated with the user to terminate. For changes to take effect, activate the connection manually after modifying user parameters.

ARP (Address Resolution Protocol) Table

Clicking **ARP Table** in the Advanced screen generates the “ARP Table” screen. This screen displays the IP and MAC addresses of each DHCP connection.

ARP Table			
IP Address	MAC Address	Device	DHCP ACL
192.168.1.2	00:90:27:b3:ce:49	Network (Home/Office)	Add

Close Refresh

Routing

Access the routing table rules by clicking **Routing** in the Advanced screen. The “Routing” screen appears.

Routing						
Routing Table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Routing Protocols

☒ Internet Group Management Protocol (IGMP)

☐ Domain Routing (add route entry according to interface from which DNS record is received)

OK Apply Cancel

Routing rules can be added, edited, or deleted from the Routing screen. To add a router, click **New Route**. The “Route Settings” screen appears.

Route Settings	
Rule Name:	Network (Home/Office) ▼
Destination:	0 .0 .0 .0
Netmask:	255 .255 .255 .255
Gateway:	0 .0 .0 .0
Metric:	0

OK Apply Cancel

When adding a routing rule, the following parameters must be specified:

- **Rule Name**- Select the type of network from the drop-down list.
- **Destination** - The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- **Netmask** - The network mask is used in conjunction with the destination to determine when a route is used.
- **Gateway** - Enter the Router's IP address.
- **Metric** - A measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

IGMP Multicasting

The Router provides support for IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When joining a multicast group, all messages addressed to the group will be received by the user, much like when an E-mail message is sent to a mailing list.

IGMP multicasting enables UPnP capabilities over networks and may also be useful when connected to the Internet through the Router. When an application running on a computer in the network sends out a request to join a multicast group, the Router intercepts and processes the request. If the Router is set to "Minimum Security" no further action is required. However, if the Router is set to "Typical Security" or "Maximum Security," the group's IP address must be added to the Router's "Multicast Groups" screen. This will allow incoming messages addressed to the group to pass through the firewall and on to the correct networked computer.

1. Select **Routing** in the Advanced screen.
2. Activate the "Internet Group Management Protocol" check-box.
3. Click **OK**.

Domain Routing

Domain routing is used in multi-router local network configurations. Normally, to access a device connected to one router from another router on the network, its IP address must be used. Activating domain routing (by clicking in the appropriate check box) allows the user to access to the computer by name (as well as IP address).

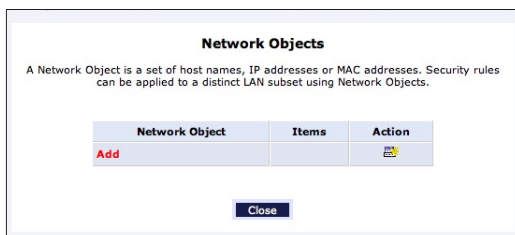
Network Objects

Network objects is used to define a part of the Router's network (a group of computers, for example) by MAC addresses, IP addresses, and/or host names. The defined part becomes a "network object," and settings, such as configuring system rules, can be applied to all the devices defined as part of the network object at once. For example, instead of setting the same website filtering configuration to five computers one at a time, the computers can be defined as a network object, and website filtering configuration can then be applied to all the computers simultaneously.

Network objects can be used to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings.

To define a network object:

1. Click **Network Objects** in the Advanced screen. The "Network Objects" screen appears.



2. Click **Add**. The “Edit Network Object” screen appears.

Edit Network Object

Network Object

Description:

Items

Item	Action
Add	

OK **Cancel**

3. Specify a name for the network object in the “Description” text box.
4. Click **Add**. The “Edit Item” screen appears.

Edit Item

Network Object Type:

IP Address:

OK **Cancel**

5. Select the type of network object type from the “Network Object Type” list box. Options include **IP address**, **IP Subnet**, **IP Range**, **MAC Address**, and **Host Name**.
6. Repeat to create other network objects, if needed. When finished, click **OK** to save all created network objects.

Firmware Restore

Firmware restore resets the Router's firmware to an earlier version, if the current version is unstable or does not meet specified needs. Click **Firmware Restore** from the Advanced screen to generate the "Firmware Restore" screen.

Firmware Restore

Welcome to Firmware Restore.

You can use Firmware Restore to undo changes to your Broadband Router and restore its settings and performance. Firmware Restore returns your Broadband Router to an earlier loaded firmware and its configuration file.

This is useful if the firmware you downloaded does not fit your needs.

Any change Firmware Restore makes to your Broadband Router is completely reversible

Active Firmware	
Rule Name:	Image downloaded from:ftp://192.168.1.20/ri408.img

Backup Firmware	
Rule Name:	rg_conf
Configuration File:	Not Available. Default Settings will be Used in Case of Firmware Downgrade.

Do you want to Restore Firmware?

The screen displays the "Active Firmware" and the "Backup Firmware." To restore the firmware to the backup firmware, click **Restore Backup Firmware**. A confirmation screen appears. Click **OK** to finish restoring the Router's firmware.

Dynamic DNS

Dynamic DNS (Domain Name Server) a dynamic IP address to be aliased to a static hostname, allowing a computer on the network to be more easily accessible from the Internet. Typically, when connecting to the Internet, the service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, while maintaining a constant domain name. This allows to user to access a device (a camera, for example) from a remote location, since the device will always have the same IP address.

When using Dynamic DNS, each time the IP address provided by the ISP changes, the DNS database changes accordingly to reflect the change. In this way, even though the IP address of the computer changes often, its domain name remains constant and accessible.

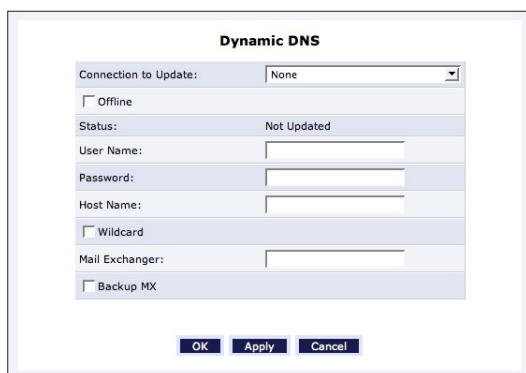
Opening a Dynamic DNS Account

To use Dynamic DNS, a free Dynamic DNS account must be opened at <http://www.dyndns.org/account/create.html>.

When applying for an account, a user name and password must be specified. Have them available when customizing the Router's Dynamic DNS feature. For more information regarding Dynamic DNS, refer to <http://www.dyndns.org>.

Setting up Dynamic DNS

To set up Dynamic DNS on the Router, click **Dynamic DNS** in the Advanced screen. The "Dynamic DNS" screen appears.



Dynamic DNS	
Connection to Update:	None
<input type="checkbox"/> Offline	
Status:	Not Updated
User Name:	<input type="text"/>
Password:	<input type="password"/>
Host Name:	<input type="text"/>
<input type="checkbox"/> Wildcard	
Mail Exchanger:	<input type="text"/>
<input type="checkbox"/> Backup MX	
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Configure the following parameters:

Connection To Update

Select the connection with which to couple the Dynamic DNS service. Options include **None**, **Broadband Connection**, and **WAN PPPoE**.

Offline

Disable the Dynamic DNS feature by clicking this check box. This feature is available only to users who have purchased some type of upgrade credit from Dyndns.org. Note that changing the redirection URL can only be performed via the Dynamic DNS website.

User Name

Enter the Dynamic DNS user name in this text box.

Password

Enter the Dynamic DNS password in this text box.

Host Name

Enter the full Dynamic DNS domain in this text box.

Wildcard

Select the “Wildcard” check box to have any URL that includes the domain name (here.yourhost.dyndns.org, for example) to connect.

Mail Exchanger

Enter the mail exchange server address. This will redirect all E-mails arriving at the Dynamic DNS address to the mail server.

Backup MX

Select this check box to designate the mail exchange server to be a backup server.

IP Address Distribution

The Router’s DHCP server makes it possible to easily add computers configured as DHCP clients to the network. It provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to them.



For example, a client (host) sends out a broadcast message on the network requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as “taken.” At this point, the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease, it will also receive current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration, it can send a release message to the DHCP server, which will then make the IP address available for use by others.

The Router's DHCP server:

- Displays a list of all DHCP hosts devices connected to the Router.
- Defines the range of IP addresses that can be allocated in the network.
- Defines the length of time for which dynamic IP addresses are allocated.
- Provides the above configurations for each network device and can be configured and enabled/disabled separately for each network device.
- Can assign a static lease to a network computer so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers.
- Provides the DNS server with the host name and IP address of each computer connected to the network.

To view a summary of the services currently being provided by the DHCP server, click **IP Address Distribution** in the Advanced screen. The “IP Address Distribution” screen appears.

IP Address Distribution				
Rule Name	Service	Subnet Mask	Dynamic IP Range	Action
Network (Home/Office)	DHCP Server	255.255.255.0	192.168.1.1 - 192.168.1.254	
Broadband Connection (Ethernet)	Disabled			
<div>Close Connection List Access Control</div>				

Editing DHCP Server Settings

To edit the DHCP server settings for a device:

1. Click the appropriate icon in the “Action” column. The “DHCP Settings” screen for the device appears.

DHCP Settings for Network (Home/Office)

Service

IP Address Distribution: DHCP Server

DHCP Server

Start IP Address:	192	.168	.1	.1
End IP Address:	192	.168	.1	.254
Subnet Mask:	255	.255	.255	.0
WINS Server:	0	.0	.0	.0
Lease Time In Minutes:	1440			

☒ Provide Host Name If Not Specified by Client

IP Address Distribution According to DHCP Option 60 (Vendor Class Identifier)

Vendor Class ID	Dynamic IP Range	QoS	Action
IP-STB	192.168.1.100-192.168.1.150	5 - Medium	
New IP Range			

OK
Apply
Cancel





2. Select the “IP Address Distribution” from the drop-down list. Options include DHCP Server, DHCP Relay, or Disable.
3. Complete the following fields:
 - **Start IP Address Range, End IP Address Range** - determines the number of hosts connected to the network in this subnet. “Start” specifies the first IP address assigned in this subnet and “End” specifies the last IP address in the range.
 - **Subnet Mask** - used to determine to which subnet an IP address belongs. An example of a subnet mask value is 255.255.0.0.
 - **WINS Server** - The WINS (Windows Internet Naming Service) server determines the IP address associated with a network device.

- **Lease Time** - each device will be assigned an IP address by the DHCP server for a limited time (“Lease Time”) when it connects to the network. When the lease expires, the server will determine if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses not in use will become available for other computers on the network.
- **Provide host name if not specified by client** - when activated, the Router assigns the client a default name if the DHCP client does not have a host name.
- **IP Address Distribution...Option 60** - DHCP Option 60 is used to preset a general name for a product or product family, as well as set a specific IP range and priority level. In this way, one device and its traffic can be given higher priority over another device.

4. Click OK to save the changes.

DHCP Connections

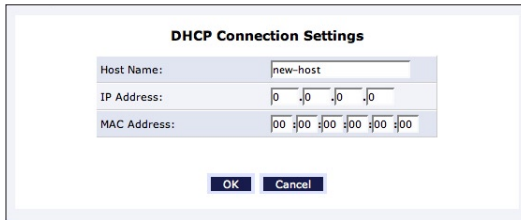
To view a list of computers currently recognized by the DHCP server, click **Connection List** at the bottom of the IP Address Distribution screen. The “DHCP Connections” screen appears.

DHCP Connections							
Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
gateway2	192.168.1.2	00:90:27:b3:ce:49	Dynamic	Network (Home/Office)	Active	9931 minutes	  
New Static Connection							

Press the **Refresh** button to update the data.


To define a new connection with a fixed IP address:

1. Click **New Static Connection** in the DHCP Connections screen. The “DHCP Connection Settings” screen appears.



The screenshot shows a dialog box titled "DHCP Connection Settings". It contains three input fields: "Host Name:" with the text "new-host", "IP Address:" with the value "0 0 0 0", and "MAC Address:" with the value "00 00 00 00 00 00". At the bottom of the dialog are two buttons: "OK" and "Cancel".

2. Enter a host name for this connection.
3. Enter the fixed IP address to assign to the computer.
4. Enter the MAC address of the computer's network card.
5. Click the **OK** to save changes.

 **Note:** A device's fixed IP address is actually assigned to the specific network card's MAC address installed on the network computer. If this network card is replaced, the device's entry in the DHCP Connections list must be updated with the new network card's MAC address.

To remove a host from the table, click the appropriate “Delete” icon in the Action column.

DNS Server

The Domain Name System (DNS) translates domain names into IP addresses and vice versa. The Router's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network, the DNS server learns its name and automatically adds it to the DNS table. Other network users can immediately communicate with this computer using either its name or its IP address.

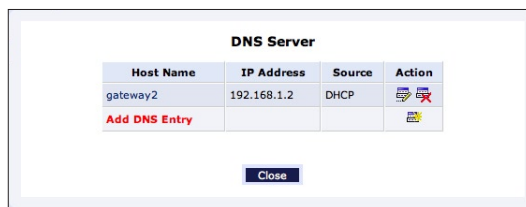
The Router's DNS also provides the following services:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the local network simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using the MegaControl Panel.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

The DNS server does not require configuration. However, the list of computers known by the DNS can be viewed, the host name or IP address of a computer on the list can be changed, or a new computer can be added to the list.

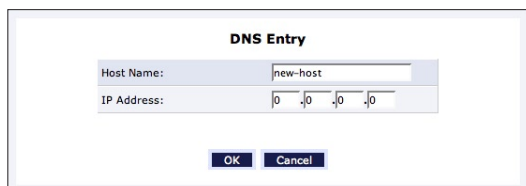
DNS Table

To view the list of computers stored in the DNS table, click **DNS Server** in the Advanced screen. The “DNS Server” screen appears.



To add a new entry to the list:

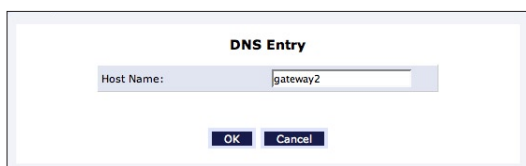
1. Click **New DNS Entry** in the DNS Server screen. The “DNS Entry” screen appears.



2. Enter the computer's host name in the "Host Name" text box.
3. Enter the computer's IP address in the "IP Address" text boxes.
4. Click **OK** to save the changes.

To edit the host name or IP address of an entry:

1. Click the appropriate "Edit" icon in the Action column. The "DNS Entry" screen appears.



2. If the host was manually added to the DNS Table, its host name and/or IP address can be modified. Otherwise, only modify its host name.
3. Click **OK** to save the changes.

To remove a host from the DNS table:

Click the appropriate "Delete" icon in the Action column. The entry will be removed from the table.

Remote Administration

The Router's Remote Administration capabilities are covered in detail in the "Security" chapter of this manual.

Protocols

Protocols features a list of preset and user-defined applications and common port settings. Protocols can be used in various security features, such as Access Control and Port Forwarding. New protocols can be added to support new applications or existing ones can be edited when needed.

To define a protocol:

1. Click **Protocols** in the Advanced screen. The “Protocols” screen appears.

Protocols

Below is a list of currently configured Protocols that are implemented in the Broadband Router.

Protocols	Ports	Action
FTP	TCP Any -> 21	
HTTP	TCP Any -> 80	
HTTPS	TCP Any -> 443	
IMAP	TCP Any -> 143	
L2TP	UDP Any -> 1701	
L2TP (Port Triggering)	UDP Any -> 1701	
Ping	ICMP Echo Request	
POP3	TCP Any -> 110	
SMTP	TCP Any -> 25	
SNMP	UDP Any -> 161	
Telnet	TCP Any -> 23	
TFTP	UDP 1024-65535 -> 69	
TFTP (Port Triggering)	UDP 1024-65535 -> 69	
Traceroute	UDP 32769-65535 -> 33434-33523	
Add		

Close Advanced >>

2. Click **Add** at the bottom of the screen. The “Edit Service” screen appears.

Edit Service

Service Name:

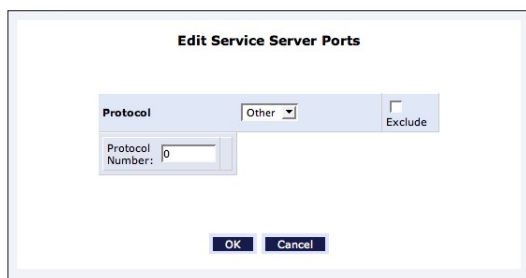
Service Description:

Server Ports

Protocol	Server Ports	Action
Add Server Ports		

OK Cancel

3. Name the service in the “Service Name” text box and, if needed, enter a description of the service in the “Service Description” text box, then click **Add Service Ports**. The “Edit Service Server Ports” screen appears.



The screenshot shows a dialog box titled "Edit Service Server Ports". Inside the dialog, there is a "Protocol" section with a dropdown menu currently set to "Other". To the right of the dropdown is an "Exclude" checkbox, which is unchecked. Below the "Protocol" section is a "Protocol Number:" label followed by a text input field containing the number "0". At the bottom of the dialog are two buttons: "OK" and "Cancel".

4. Select a protocol from the “Protocol” drop-down list. To create a new protocol, select “Other.” After selecting a protocol, the screen will refresh, displaying the relevant text boxes needed to edit the particular protocol.
5. Click **OK** to save the changes.

This page left intentionally blank.

Monitoring the

Router

8

The Broadband Router’s System Monitoring screens display important system information, including:

- Key network device parameters
- Network traffic statistics
- System log
- Amount of time since the Router was last started

Monitoring Connections

1. Click **System Monitoring** at the top of the Home screen to display the “Full System/System-wide Monitoring of Connections” screen, which comprises a table summarizing the monitored connection data.
2. Click **Refresh** to update the table, or click **Automatic Refresh On** to constantly update the displayed parameters.

Full Status/System wide Monitoring of Connections				
NOTE: Only advanced technical users should use this feature				
Rule Name	Network (Home/Office)	Broadband Connection (Ethernet)	Ethernet	WAN PPPOE
Status	Connected	Down	Connected	Disabled
Network	Network (Home/Office)	Broadband Connection	Network (Home/Office)	Broadband Connection
Underlying Device	Ethernet			Broadband Connection (Ethernet)
Connection Type	Bridge	Ethernet	Hardware Ethernet Switch	PPPoE
MAC Address	00:0f:b3:a2:d7:c6	00:0f:b3:a2:d7:ca	00:0f:b3:a2:d7:c7	
IP Address	192.168.1.1			
Subnet Mask	255.255.255.0			
IP Address Distribution	DHCP Server	Disabled	Disabled	
Service Name				
User Name				qa2@local
Received Packets	11835	0	8760	
Sent Packets	845051	0	614542	
Time Span	70:27:09	70:27:09	70:27:09	
Channel				
<div>Close Automatic Refresh Off Refresh</div>				

Traffic Monitoring

The Router constantly monitors traffic within the local network and between the local network and the Internet. You can view up-to-the-second statistical information about data received from and transmitted to the Internet, and about data received from and transmitted to computers in the local network, by clicking **Traffic Monitoring**. This generates the “Traffic Monitoring” screen.

Traffic Monitoring				
Rule Name	Network (Home/Office)	Broadband Connection (Ethernet)	Ethernet	WAN PPPOE
Status	Connected	Down	Connected	Disabled
Network	Network (Home/Office)	Broadband Connection	Network (Home/Office)	Broadband Connection
Underlying Device	Ethernet			Broadband Connection (Ethernet)
Connection Type	Bridge	Ethernet	Hardware Ethernet Switch	PPPoE
IP Address	192.168.1.1			
Received Packets	16485	0	14317	
Sent Packets	589779	0	431658	
Received Bytes	3726194	0	3465635	
Sent Bytes	88379904	0	58305737	
Receive Errors	0	0	0	
Receive Drops	0	0	0	
Time Span	48:21:56	48:21:56	48:21:56	
<div>Close Automatic Refresh Off Refresh</div>				

System Log

The System Log displays a list of the most recent activities of the Router. Click **System Log** to generate the “System Log” screen.

System Log			
<div> Close Clear Log Save Log Refresh </div>			
Press the Refresh button to update the data.			
Time	Event	Event-Type	Details
Jan 2 21:26:34 2003	System Log	Message	kern.debug Clink Link Down (freq timer) [repeated 5 times, last time on Jan 2 21:26:39 2003]
Jan 2 21:26:34 2003	System Log	Message	daemon.warn cLink: clink1: ioctl(DRV_GET_MY_NODE_INFO) failed, res=-1: Bad address.
Jan 2 21:26:20 2003	System Log	Message	kern.debug Clink Link Down (freq timer) [repeated 13 times, last time on Jan 2 21:26:33 2003]
Jan 2 21:26:20 2003	System Log	Message	daemon.warn cLink: clink0: ioctl(DRV_GET_MY_NODE_INFO) failed, res=-1: Bad address.
Jan 2 21:26:04 2003	System Log	Message	kern.debug Clink Link Down (freq timer) [repeated 13 times, last time on Jan 2 21:26:19 2003]
Jan 2 21:26:04 2003	System Log	Message	daemon.warn cLink: clink0: ioctl(DRV_GET_MY_NODE_INFO) failed, res=-1: Bad address.
Jan 2 21:26:00 2003	System Log	Message	kern.debug Clink Link Down (freq timer) [repeated 4 times, last time on Jan 2 21:26:03 2003]
Jan 2			daemon.warn cLink: clink0:

Router Status

To display the amount of time since the Router was last started, click **Router Status**. The “Router Status” screen appears.

Router Status	
Router Has Been Active For: 24 hours	
<div> Close Automatic Refresh Off Refresh </div>	

This page left intentionally blank.

Troubleshooting

9

This chapter contains a list of problems that may be encountered while using the Broadband Router, and techniques to try and overcome the problem. Note that these techniques may not solve the problem (or problems).

Accessing the Router if Locked Out

If the Router's connection is lost while making configuration changes, a setting that locks access to the MegaControl Panel may have inadvertently been activated. There are three common ways to lock access to the Router:

Scheduler If a schedule has been created that applies to the computer over the connection being used, the Router will not be accessible during the times set in the schedule. To regain access, either wait until the connection is scheduled to be active again, or restore the default settings to the Router.

LAN Firewall If the firewall setting for the local network is set to maximum, no computers from the network will be able to connect to the Router. To gain access, restore the default settings to the Router.

Access Control If the access control setting for the computer is set to block the computer, access to the Router will be denied. To gain access, restore the default settings to the Router.

Restoring the Router's Default Settings

There are two ways to restore the Router's default settings. The first is to use the tip of a ballpoint pen and depress the "Reset" button on the back of the Router for at least five seconds. The second is to access the Router's MegaControl Panel and navigate to the "Advanced Settings" screen. Click on "Restore Defaults" and read the instructions on-screen. Note that after performing either of these two procedures, all previously saved settings on the Router will be lost.

LAN Connection Failure

- Ensure the Router is properly installed, the LAN connections are correct, and the power is on.
- Confirm the computer and Router are on the same network segment. If unsure, let the computer get the IP address automatically by initiating the DHCP function, then verify the computer is using an IP address within the default range (192.168.1.2 through 198.168.1.254). If the computer is not using an IP address within the range, it will not connect to the Router.
- Ensure the Subnet Mask address is set to 255.255.255.0.

Time out error occurs when entering a URL or IP Address

- Verify all the computers are working properly.
- Ensure the IP settings are correct.
- Ensure the Router is on and connected properly.
- Verify the Router's settings are the same as the computer.

I've run out of Ethernet ports on my Router. How do I add more computers?

Plugging in an Ethernet hub or switch expands the number of ports on the Router. Run a standard Ethernet cable from the "Uplink" port of the new hub or switch to a yellow Ethernet port on the Router.

How do I change the password on the Router's MegaControl Panel?

From the MegaControl Panel Home screen, click **Advanced**, then **Users**. From the "Users" screen, click **Administrator**, which generates the "User Settings" screen. In the "General" section of the screen, change the password.

Which connection speeds does the Router support?

The Ethernet Internet connection supports 100 Mbps.

Are the Router's Ethernet ports auto-sensing?

Yes. Either a straight-through or crossover Ethernet cable can be used.

How do I find out what IP address my computer is using?

Windows 95, 98, 98SE, and Me - Select **Start, Run**, and type “winipcfg.” Press **Enter**. When the “Winipcfg” window appears, ensure your network device is selected.

Windows NT, 2000, and XP - Select **Start, Run** and type “cmd.” Press **Enter**. When the command screen appears, type “ipconfig” and press **Enter**.

I used DHCP to configure my network. Do I need to restart my computer to refresh my IP address?

No. Follow these steps to refresh the IP address:

Windows 95, 98, 98SE, and Me - Select **Start, Run**, type “winipcfg,” and press **Enter**. Ensure the Ethernet adapter is selected in the device box. Press the **Release_all** button, then press the **Renew_all** button.

Windows NT 4.0 and 2000 - Select **Start, Run**, type “cmd,” and press **Enter**. At the DOS prompt, type “ipconfig /release,” then type “ipconfig /renew.”

Windows XP - Unplug the Ethernet cable and plug it back in.

I cannot access the Router's MegaControl Panel? What should I do?

If you cannot access the Router's MegaControl Panel, make sure the computer connected to the Router is set up to dynamically receive an IP address.

I have an FTP or Web server on my network. How can I make it available to users on the Internet?

For a Web server, enable port forwarding for port 8088 to the IP address of the server and set up the Web server to receive on that port, as well. (Configuring the server to use a static IP address is recommended.)

For an FTP server, enable port forwarding for port 21 to the IP address of the server. (Configuring the server to use a static IP address is recommended.)

How many computers can be connected through the Router?

The Router is capable of 254 connections, but it is recommended to have no more than 45 connections. As you increase the number of connections, you decrease the available speed for each computer.

What is the default user name for the Router?

The default user name for the router is “admin” and the default password is “password” (all lower case, no quotation marks). When logging into the Router the first time (or after restoring the Router’s default settings), the user is asked to create a new user name and password after entering the default user name and password. Enter the new user name and password, write them down on a piece of paper, and keep it in a safe place. The new user name and password will be needed to access the MegaControl Panel in the future.

Quality Of Service

A

Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. For obvious reasons, bandwidth and capacity cannot be expanded infinitely, requiring that bandwidth-demanding services be delivered over existing infrastructure, without incurring additional expensive investments. The next logical means of ensuring optimal use of existing resources are Quality of Service (QoS) mechanisms for congestion management and avoidance.

Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.



STOP! Do not change any Quality of Service settings unless instructed to do so by the ISP.

Traffic Priority

Traffic Priority manages and avoids traffic congestion by defining inbound and outbound priority rules for each device on the Router. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis.

QoS can be configured using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address, or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

The Router supports two priority marking methods for packet prioritization:

- DSCP
- 802.1p Priority

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the Router's firewall mechanism. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, QoS rules can be defined on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown). Applications that support such inheritance have an ALG in the firewall. They are:

- SIP
- MSN Messenger/Windows Messenger
- TFTP
- FTP
- MGCP
- H.323
- Port triggering applications
- PPTP
- IPSec

Setting Priority Rules

To set priority rules:

1. Click **Quality of Service** on the top of the Home screen. The “Traffic Priority” screen appears. This screen is divided into two identical sections, one for “QoS input rules” and the other for “QoS output rules,” which are for prioritizing the inbound and outbound traffic, respectively. Each section lists all the devices on which rules can be set. Rules can be set on all devices at once by clicking **Add** in the “All Devices” row.

Traffic Priority

QoS Input Rules

Rule ID	Device	Source Address	Destination Address	Protocols	Operation	Status	Action
All Devices							Add
Network (Home/Office) Rules							Add
Broadband Connection (Ethernet) Rules							Add
Ethernet Rules							Add
WAN PPPoE Rules							Add

QoS Output Rules

Rule ID	Device	Source Address	Destination Address	Protocols	Operation	Status	Action
All Devices							Add
Network (Home/Office) Rules							Add
Broadband Connection (Ethernet) Rules							Add
Ethernet Rules							Add
WAN PPPoE Rules							Add

2. After choosing the traffic direction and the device on which to set the rule, click **Add** in the appropriate row. The “Add Traffic Priority Rule” screen appears.

Add Traffic Priority Rule

Matching

Source Address:

Destination Address:

Protocol:

DSCP:

DSCP Mask:

Device:

QoS Operation

DSCP:

☐ Set Priority

☒ Set Rx Class Name: No Rx class names available

☒ Set Tx Class Name: No Tx class names available

Logging

☐ Log Packets Matched by This Rule

When should this rule enter?:

Set the following parameters:

Source Address - The source address of the packets sent to or received from the network object. To add an address:

1. Select **Specify Address** from the drop-down list. The screen refreshes and an “Add” link appears.
2. Click **Add**, then add a new network object (see the “Advanced Settings” chapter to learn how to add a network object). Clicking Add is the same as clicking “New Entry” in the “Network Objects” screen.

Destination Address - The destination address of the packets sent to or received from the network object. This address can be configured in the same manner as the source address.

Protocol - Choose a specific traffic protocol from the drop-down list, or add a new one. To add a new traffic protocol:

1. Select **Specify Address** from the drop-down list. The screen refreshes and an “Add” link appears.
2. Click **Add**, and add a new protocol (see the “Advanced Settings” chapter to learn how to add a protocol). Note that clicking Add is equivalent to clicking “New Entry” in the “Protocols” screen.

Set Priority - Activate this check box to add a priority to the rule. The screen will refresh, allowing a selection between one of eight priority levels, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.

Set DSCP - Activate this check box to mark a DSCP value on packets matching a connection that matches this rule. The screen will refresh, allowing the user to enter the Hex value of the DSCP.

Log Packets Matched by This Rule - Check this check box to log the first packet from a connection matched by this rule.

Schedule - By default, the rule will always be active. However, scheduler rules can be configured to define time segments during which the rule may be active.

Traffic Shaping

Traffic Shaping is the solution for managing and avoiding congestion where the network meets limited broadband bandwidth. Typical networks use a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. This is where most bottlenecks occur

A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic. While traffic priority allows basic prioritization of packets, traffic shaping provides more sophisticated definitions, such as:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

Additionally, QoS traffic shaping rules can be defined for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on the default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

Device Traffic Shaping

This section describes the different Traffic Shaping screens and terms, and presents the feature's configuration logic.

1. Click **Quality of Service** at the top of the Home screen, then click **Traffic Shaping**. The following screen appears.



2. Click **Add**. The “Add Device Traffic Shaping” screen appears.
3. Select the device for which the traffic will be shaped. The drop-down list includes all the Router’s devices, as well as the option to select all devices in each category (e.g., “All LAN Devices,” “All WAN Devices”). In this example, select the default WAN device option.

4. Click **OK**. The “Edit Device Traffic Shaping” screen appears

Edit Device Traffic Shaping

Device: Network (Home/Office)

Tx Traffic Shaping

Tx Bandwidth: 282226 Kbits/s

TCP Serialization: Disable

Class ID	Rule Name	Priority	Bandwidth (Kbits/s)		Status	Action
			Reserved	Maximum		
Add						

Rx Traffic Policing

Rx Bandwidth: 282226 Kbits/s

Class ID	Rule Name	Bandwidth (Kbits/s)		Status	Action
		Reserved	Maximum		
Add					

OK Apply Cancel

Configure the following parameters:

Tx Bandwidth - Tx bandwidth limits the Router’s bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link.. This forces the Router to be the network bottleneck, where sophisticated QoS prioritization can be performed.

Rx Bandwidth - In the same manner, this Rx bandwidth limits the Router’s bandwidth reception rate.

TCP Serialization - Enable TCP Serialization from its drop-down list, either for active voice calls only or for all traffic. The screen will refresh, adding a “Maximum Delay” text box. This function allows the maximum allowed transmission time frame (in milliseconds) of a single packet to be defined. Any packet requiring a longer time to be transmitted will be fragmented to smaller sections. This avoids transmission of large, bursty packets that can cause delay or jitter for real-time traffic, such as VoIP.

Shaping Classes

The bandwidth of a device can be divided to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a shaping class. When not used by its predefined traffic type or owner (for example VoIP), the class will be available to all other traffic. However, when needed, the entire class is reserved solely for its owner. Also, the maximum bandwidth that a class uses can be limited, even if the entire bandwidth is available.

When a shaping class is defined for a specific traffic type, two shaping classes are created. The second class is the “Default Class”, which is responsible for all the packets that do not match the defined shaping class, or any other classes that might be defined on the device. This can be viewed in the “Class Statistics” screen.

To define a shaping class:

1. Click **Add** in the “Tx Traffic Shaping” section of the Edit Device Traffic Shaping screen. The “Add Shaping Class” screen appears.



2. Name the new class and click **OK**.

- Click the class name to edit the shaping class. The “Edit Class” screen appears.

Configure the following parameters:

Name Enter the name of the class in this text box.

Class Priority The class can be granted one of eight priority levels, zero being the highest and seven the lowest (opposite the rules priority levels). This level sets the priority of a class in comparison to other classes on the device.

Tx Bandwidth Tx bandwidth is the reserved transmission bandwidth in kilobits per second. The maximum allowed bandwidth can be limited by selecting **Specify** from the drop-down list. The screen will refresh, adding another “Kbits/s” text box. Enter the desired maximum allowed bandwidth.

Rx Bandwidth In the same manner, Rx bandwidth is the reserved reception bandwidth, which can also be limited to a maximum allowed bandwidth.

Policy The class policy determines the policy of routing packets inside the class. Select one of four options:

- **Priority** - Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet’s priority, which can be defined explicitly, by a DSCP value, or by an 802.1p value.
- **FIFO** - The “First In, First Out” priority queue. This queue ignores any previously marked priority the packets may have.
- **Fairness** - The fairness algorithm ensures no starvation by granting all packets a certain level of priority.

- **RED** - The RED (Random Early Detection) algorithm utilizes statistical methods to drop packets in a “probabilistic” way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets lost when a queue overflows and a host is transmitting at a high rate

Schedule By default, the class will always be active. However, scheduler rules can be configured to define time segments during which the class may be active.

Class Rules Class rules define which packets belong to the class. They must be defined in order to associate packets that meet them with the shaping class. Without class rules, the shaping class will have no effect. Each class can have outbound and/or inbound rules for outgoing and incoming traffic, respectively. For example, all outgoing packets from computer A in the network can be defined as belonging to the VoIP class. These packets will be limited to the class settings (bandwidth, schedule, etc.). In addition, the traffic protocol and priority for each rule can be defined (this is not mandatory as it is with Traffic Priority rules).

To add a new outbound/inbound class rule, click **Add** in the Edit Class screen. The “Add Traffic Priority Rule” screen appears.

The screenshot shows a window titled "Add Traffic Priority Rule". It has a light blue background and a white border. The window is divided into several sections. The "Matching" section has fields for "Source Address" (set to "Any"), "Destination Address" (set to "Any"), "Protocol" (set to "Any"), "DSCP" (set to "None"), "DSCP Mask" (set to "0"), and "Device" (set to "Any"). The "QoS Operation" section has a "DSCP" field (set to "None") and a "Set Priority" checkbox. The "Logging" section has a "Log Packets Matched by This Rule" checkbox. The "When should this rule occur?" field is set to "Always". At the bottom are "OK" and "Cancel" buttons.

Source Address - The source address of the packets sent to or received from the network object (computer A in the above example). To add an address:

1. Select **Specify Address** from the drop-down list. The screen will refresh and an “Add” link appears.
2. Click **Add**, and add a new network object. Note that clicking Add is equivalent to clicking “New Entry” in the “Network Objects” screen.

Destination Address - The destination address of the packets sent to or received from the network object. This address can be configured in the same manner as the source address.

Protocol - Select a specific traffic protocol from the drop-down list, or add a new one. To add a new traffic protocol:

1. Select **Specify Protocol** from the drop-down list. The screen will refresh and an “Add” link appears.
2. Click **Add**, and add a new protocol. This is the same as clicking “New Entry” in the “Protocols” screen.

DSCP -Use this drop-down list to mark a DSCP value on packets matching a connection that matches this rule. To do so, select **Specify** from the drop-down list and enter the hexadecimal value of the DSCP.

Set Priority - Activate this check box to add a priority to the rule. The screen will refresh, allowing a selection of one of eight priority levels, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.

Log Packets Matched by This Rule - Check this check box to log the first packet from a connection that was matched by this rule.

When should this rule occur? - By default, the rule will always be active. However, scheduler rules can be configured to define time periods during which the rule is active. To learn how to configure scheduler rules, see the “Advanced Settings” chapter.



Note: The hierarchy of the class rules is determined by the addition order to the class. For example, if the first rule is “match packets with any source address, any destination address, and any protocol to this class,” all packets traveling through Router will be associated with the specific class. Any rules defined later will not have any effect.

Ingress Data

The Router can control outgoing data fairly easily. It can queue packets, delay them, give precedence to other packets, or drop them. This helps in resolving upload (Tx) traffic bottlenecks, and in most cases is sufficient. However, in the case of download (Rx) traffic bottlenecks, the ability to control the flow is much more limited. The Router cannot queue packets, since in most cases the local network (LAN) is much faster than the Internet (WAN), and when the Router receives a packet from the Internet, it passes it immediately to the local network.

QoS for ingress data has the following limitations, which do not exist for outgoing data:

- QoS can only be applied to TCP streams (UDP streams cannot be delayed)
- No borrowing mechanism
- When reserving Rx bandwidth, it is strictly taken from the bandwidth of all other classes

Furthermore, the Router cannot control the behavior of the ISP, which may not have proper QoS handling. Unfortunately, this is a common situation. Let's look at a scenario of downloading a large file and surfing the Internet at the same time. Downloading the file is distinguished by small requests, followed by very large responses. This may result in blocking HTML traffic at the ISP. A solution for such a situation is limiting the bandwidth of low-priority TCP connections (such as the file download).

Differentiated Services Code Point Settings

In order to understand what DSCP is, one must first be familiarized with the Differentiated Services model.

Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements, and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback, or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.


Diffserv defines a field in IP packet headers referred to as the Differentiated Services Codepoint (DSCP). Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior

The Router provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method. Any of the existing DSCP setting can be edited or deleted, and new entries can be added.

1. Click Quality of Service at the top of the Home screen, then click **DSCP Settings**. The “DSCP Settings” screen appears.

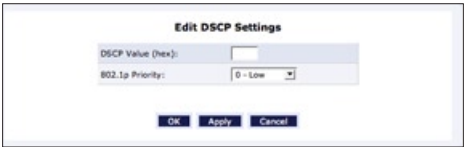


DSCP Settings

DSCP Value (hex)	802.1p Priority	Action
0x0	0 - Low	 
0x2	0 - Low	 
0x4	4 - Medium	 
0x6	4 - Medium	 
0x8	2 - Low	 
0xA	1 - Low	 
0xC	3 - Low	 
0xE	2 - Low	 
0x10	7 - High	 
0x12	6 - High	 
0x14	7 - High	 
0x16	6 - High	 
0x18	5 - Medium	 
0x1A	5 - Medium	 
0x1C	5 - Medium	 
0x1E	5 - Medium	 
0x2E	7 - High	 
Add		

Close

2. To edit an existing entry, click the appropriate icon in the “Action” column. To add a new entry, click **Add**. In either case, the “Edit DSCP Settings” screen appears.



Edit DSCP Settings

DSCP Value (hex):

802.1p Priority:

OK **Apply** **Cancel**

3. Configure the following parameters:

DSCP Value (hex) - Enter the DSCP value as a hexadecimal value.

802.1p Priority - Select an 802.1p priority level from the drop-down list, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). The default DSCP value for packets with an unassigned value is zero.

4. Click **OK** to save the settings.

802.1p Settings

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority. By default, the highest priority is seven, which could be assigned to network-critical traffic. Values five and six can be applied to delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications down to “loss eligible” traffic. Zero is the value for unassigned traffic and used as a best effort default, invoked automatically when no other value has been set.

A packet can match more than one rule. This means that:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

1. Click **Quality of Service** at the top of the Home screen, then click **802.1p Settings**. The “802.1p Settings” screen appears.



The screenshot shows the "802.1p Settings" screen. It contains a table with two columns: "802.1p Value" and "Priority". The table has 8 rows, indexed 0 through 7. The "Priority" column contains drop-down menus with the following values: 0: Low, 1: Low, 2: Low, 3: Low, 4: Medium, 5: Medium, 6: High, 7: High. At the bottom of the screen are three buttons: "OK", "Apply", and "Cancel".

802.1p Value	Priority
0	Low
1	Low
2	Low
3	Low
4	Medium
5	Medium
6	High
7	High

2. The eight 802.1p values are pre-populated with the three priority levels: Low, Medium, and High. These levels can be changed for each of the eight values in their respective drop-down lists.
3. Click **OK** to save the settings.

Class Statistics

The Router provides accurate, real-time information on the traffic moving through the defined device classes. For example, the amount of packets sent, dropped, or delayed are just a few of the parameters monitored per each shaping class.

To view class statistics, click **Quality of Service** at the top of the Home screen, then click **Class Statistics**. The following screen appears. Note that class statistics will only be available after defining at least one class (otherwise the screen will not present any information).

Class	Packets Sent	Bytes Sent	Packets Dropped	Packets Delayed	Rate (bytes/s)	Packet Rate
Close	Automatic Refresh On	Refresh				

Specifications



General

Model Number

MI408 (8-Port Broadband Router)

Standards

IEEE 802.3x

IEEE 802.3u

IP

IP version 4

Firewall

ICSA certified

Speed

LAN Ethernet: 10/100 Mbps auto-sensing

Cabling Type

Ethernet 10BaseT: UTP/STP Category 3 or 5

Ethernet100BaseTX: UTP/STP Category 5

LED Indicators

Power, LAN (8), WAN, Internet

Environmental

Power

External, 5V DC, 3A

Certifications

FCC Part 15, UL-60959-1

Operating Temperature

0° C to 40° C (32° F to 104° F)

Storage Temperature

-20° C to 70° C (-4° F to 158° F)

Operating Humidity

8% to 93% (non-condensing)

Storage Humidity

5% to 100% (non-condensing)



Note: Specifications are subject to change without notice.

Notices

Regulatory Compliance Notices

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by implementing one or more of the following measures:

- Reorient or relocate the receiving antenna;
- Increase the separation between the equipment and receiver;
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected;
- Consult the dealer or an experienced radio or television technician for help.

Modifications


The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by *Actiontec Electronics, Inc.*, may void the user's authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo – United States only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference;

2. This device must accept any interference received, including interference that may cause unwanted operation.

 **Note:** To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

For questions regarding your product or the FCC declaration, contact:

Actiontec Electronics, Inc.
760 North Mary Ave.
Sunnyvale, CA 94086
United States
Tel: (408) 752-7700
Fax: (408) 541-9005