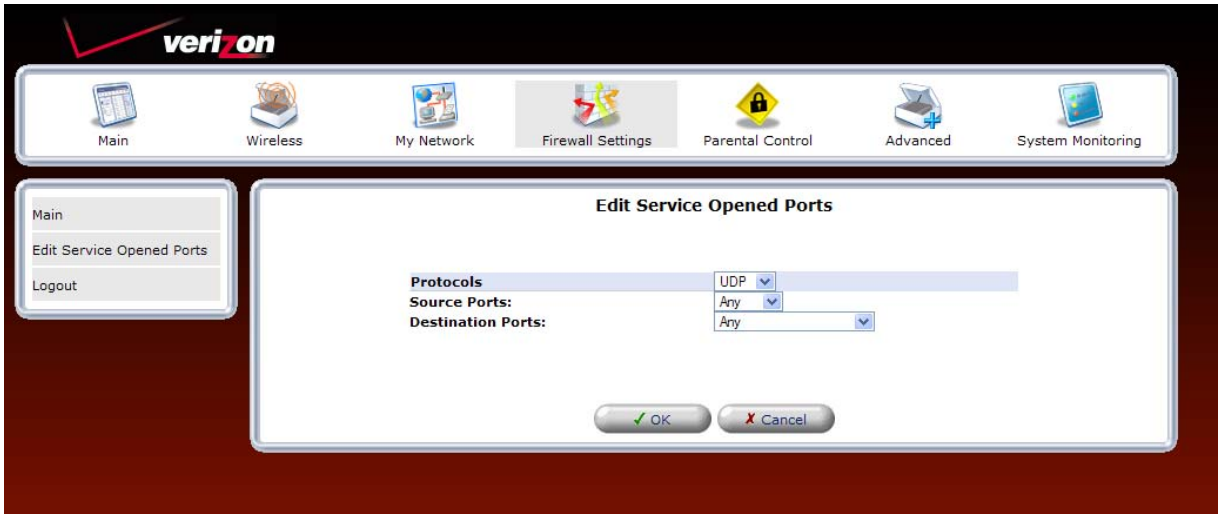
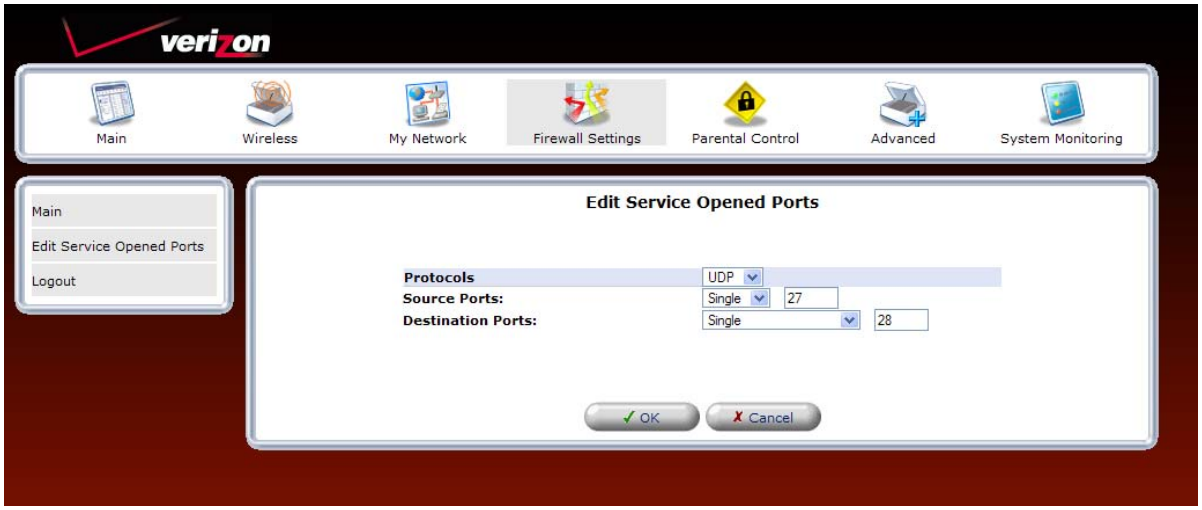
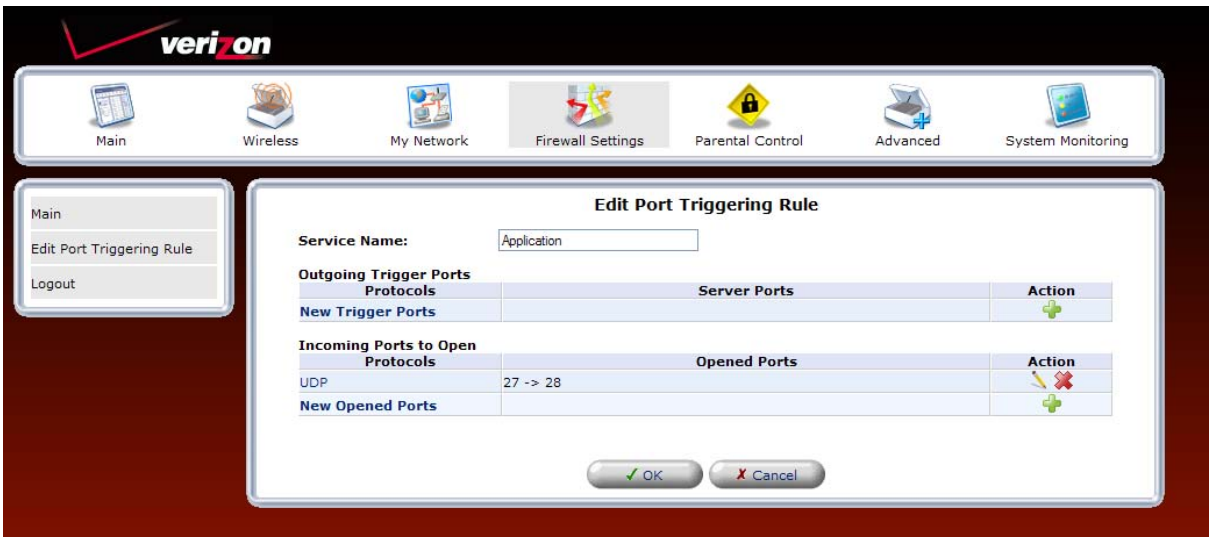
For example, if you select **UDP**, the following screen appears. Select the desired source port and destination port settings from the drop-down lists.



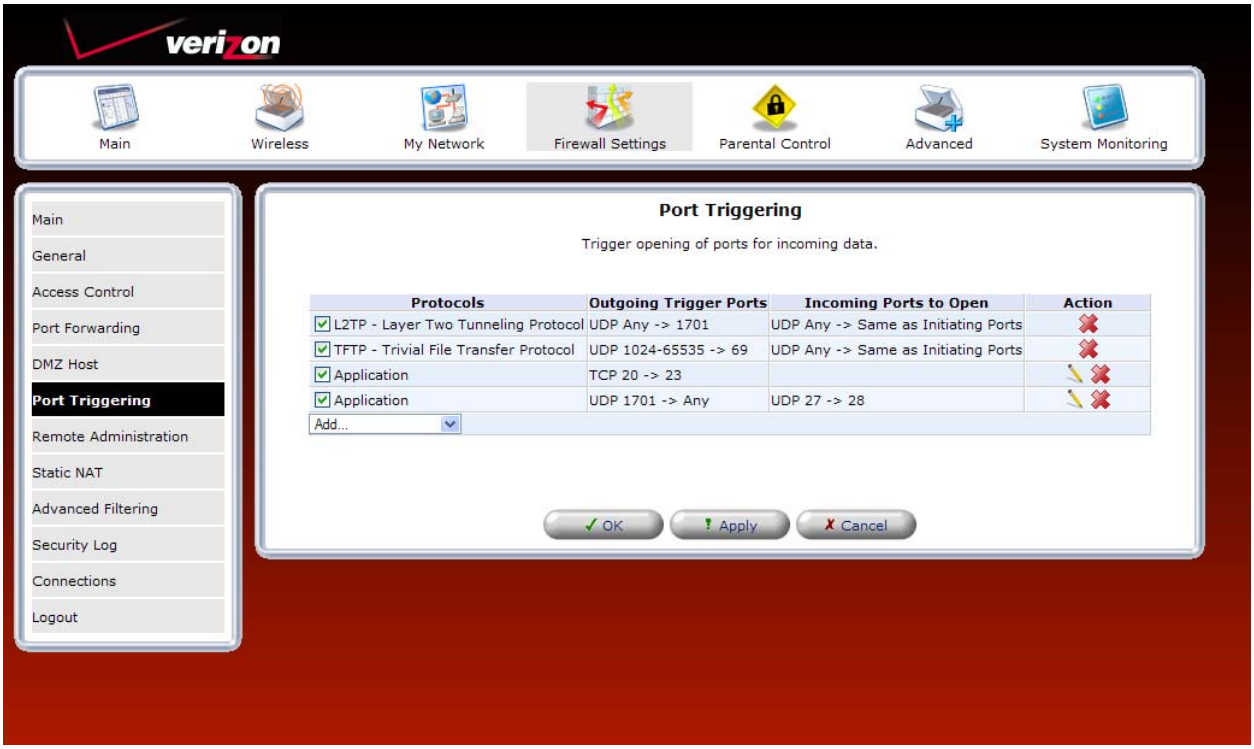
Next, enter the desired source and destination port values in the fields provided, and click **OK** to continue.



If you clicked **OK**, the following screen appears. Click **OK** to continue.

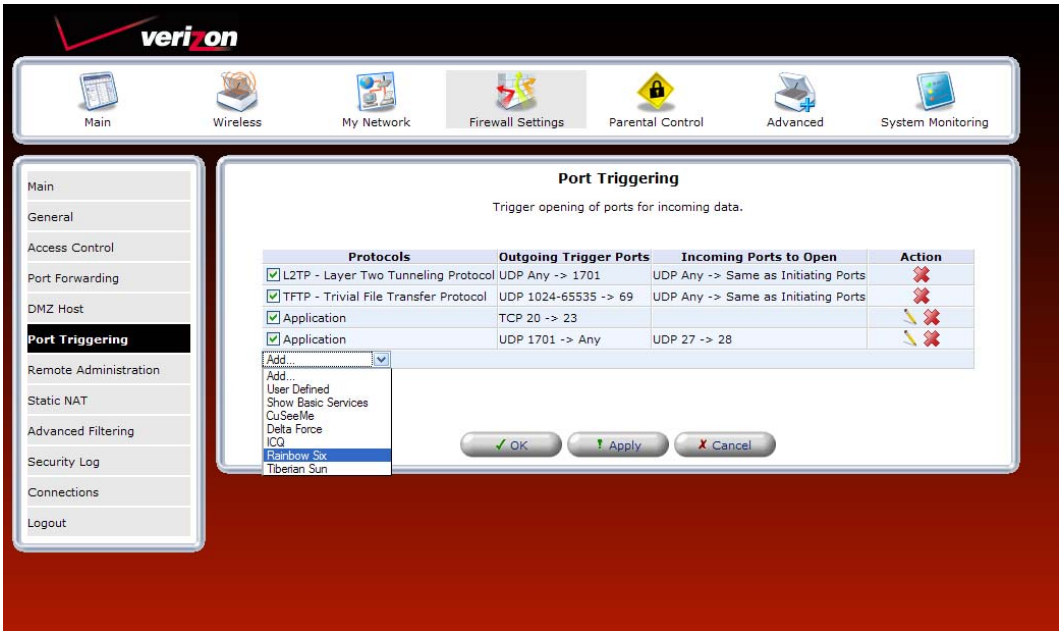


If you clicked **OK**, the following screen appears. This screen shows that the triggering rule has been added to the list of triggering services. Click **Apply** to save the settings. If you want to edit a rule, click the pencil icon next to the rule that you want to edit. To delete a rule, click the "X" icon next to the rule that you want to delete.

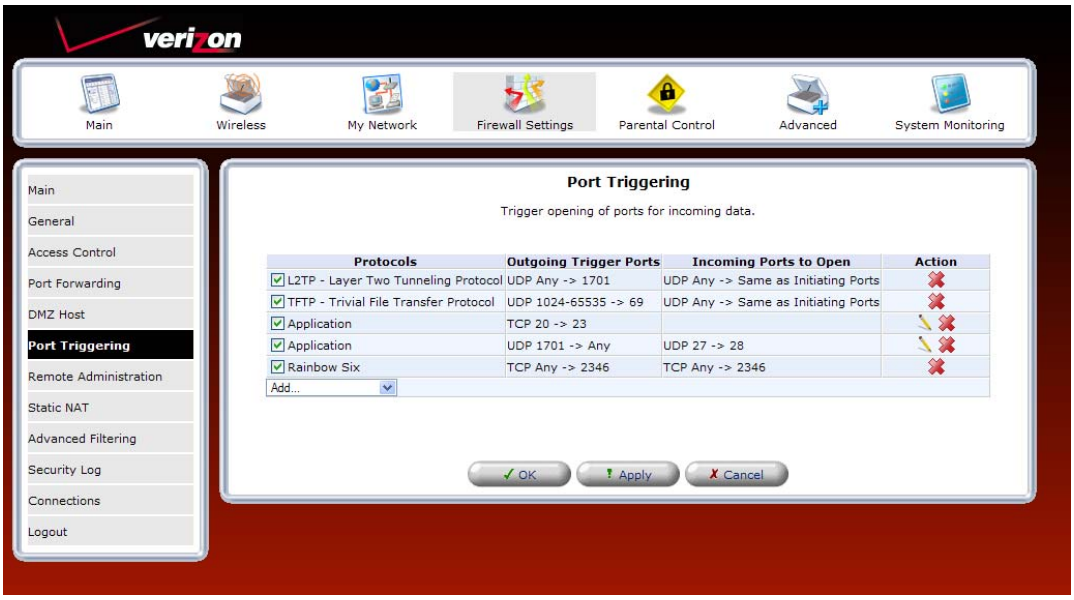


13.5.2 Setting Up a Predefined Port Triggering Rule

To set up a predefined port triggering rule, in the **Add** drop-down list, select a predefined service.



After you have selected a service, the following screen appears. The service that you selected will be displayed. Click **Apply** to save the settings.



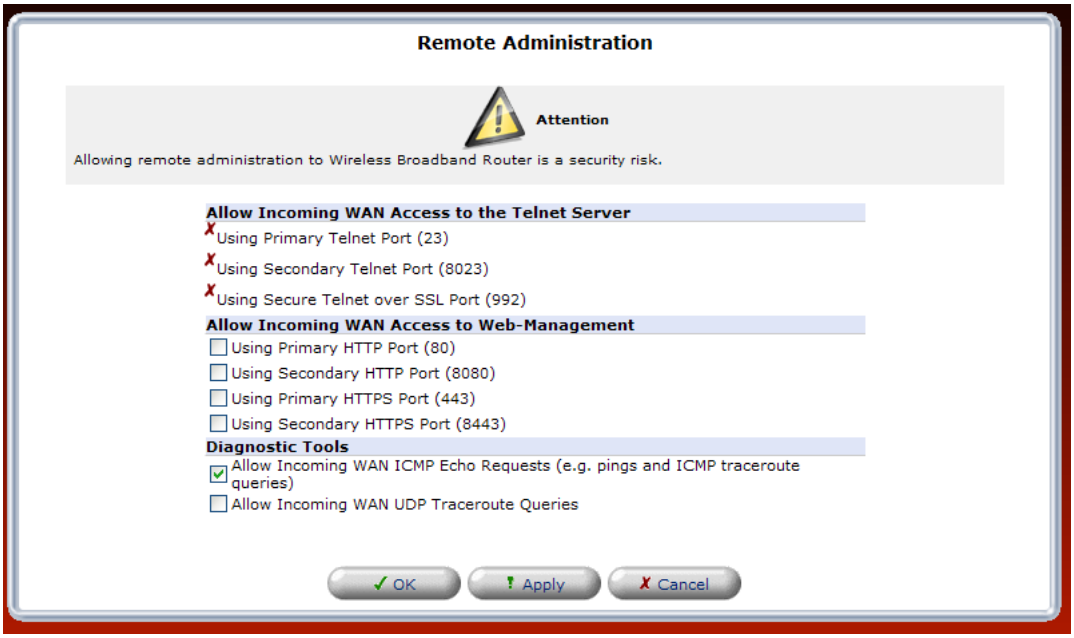
13.6 Remote Admin

If you select **Firewall Settings** in the top navigation menu, and then select **Remote Administration** in the left submenu, the following screen appears.

It is possible to access and control your Router not only from within the home network, but also from the Internet. This allows you to view or change settings while traveling. It also enables you to allow your service provider to change settings or help you troubleshoot functionality or communication issues from a remote location. Remote access to your Router is blocked by default to ensure the security of your network. However, your Router supports the following services, and you can use the Remote Administration screen to selectively enable these services if they are needed.

WARNING: With Remote Administration enabled, your network will be at risk from outside attacks. Note that remote command line access (Telnet) is not enabled on this Router.

To configure Remote Administration, enter the appropriate settings, and then click **Apply** to save the settings.



13.7 Static NAT

If you select **Firewall Settings** in the top navigation menu and then select **Static NAT** in the left submenu, the following screen appears.

NOTE: A block of static IP addresses must be purchased from Verizon to configure this feature. This Router supports 253 static IP addresses.

Static NAT allows LAN devices to use public IP addresses (different from the Router's public IP address). The LAN devices are still configured with private IP addresses (either statically or dynamically through DHCP). Traffic between the LAN devices and the Internet is still "NAT'ed," but the Static NAT mappings allow packets from specific devices to use a distinct public IP address; and packets sent to different public IP addresses to be forwarded to specific devices.

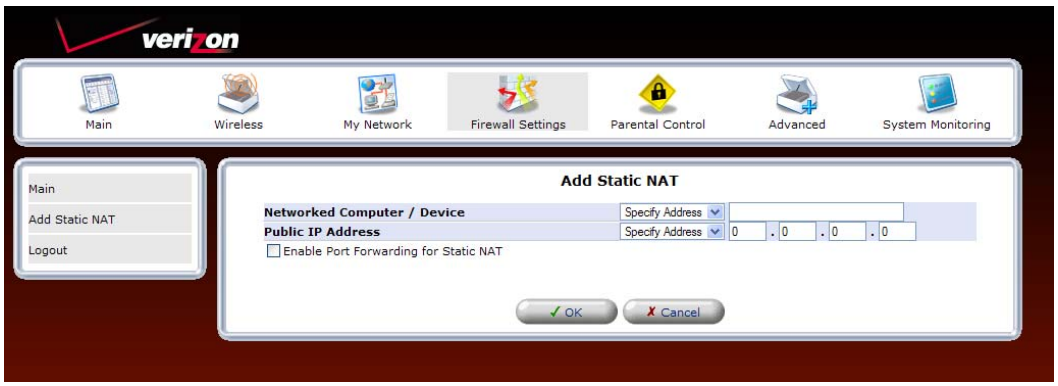
With Static NAT, devices that are behind the firewall and that are configured with private IP addresses appear to have public IP addresses on the Internet. This allows an internal host, such as a Web server, to have an unregistered (private) IP address and still be reachable over the Internet. This section also allows you to perform port translations (NAPT).

There are three steps to setting up a Static NAT entry:

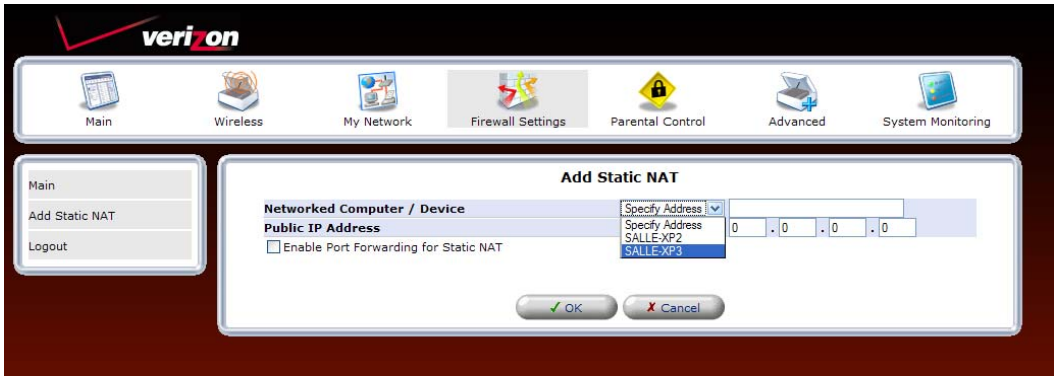
1. **Create an address pool** – These are addresses on your WAN network side.
2. **Create a NAT rule** – This defines the local computer to be NAT'd, the external IP address from the pool and the services that are allowed.
3. **Create a Port Forwarding Rule** – This matches the NAT rule you created above and forwards the packets received on the WAN side to reach your internal computer.

To configure Static NAT, click the **New Entry** link.

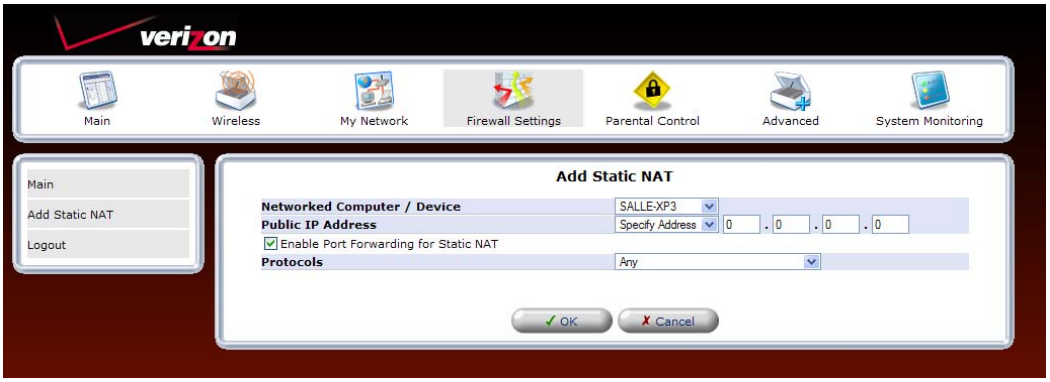
The following screen appears.



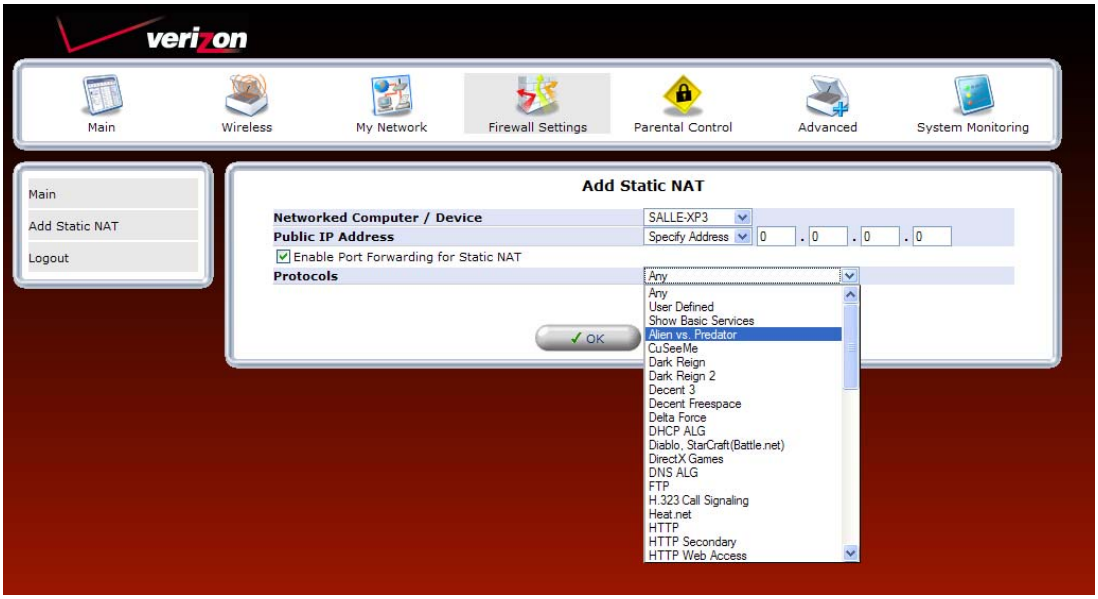
From the **Networked Computer/Device** drop-down list, select the device to which you will apply Static NAT. Or you can enter the device name in the field provided.



Next, you must first define what external (public) address will be assigned to this device. To use public IP addresses, you must first obtain them from Verizon. Enter your IP address in the Public IP Address fields. If you want to Enable Port Forwarding service, click the box next to Enable Port Forwarding for Static NAT. The **Protocol** drop-down list appears.

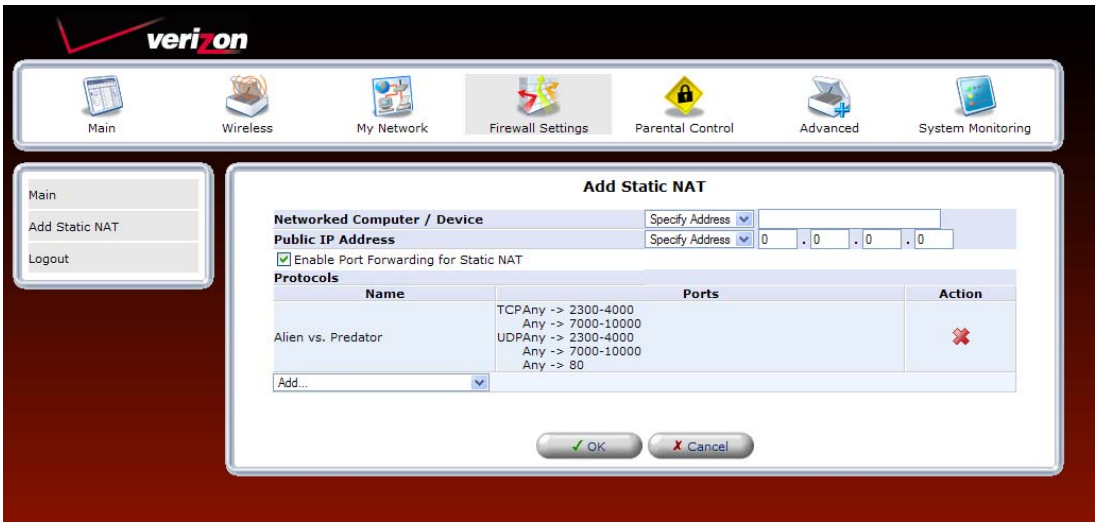


Select the desired protocol from the **Protocol** drop-down list.



For example, if you select **IP Address** as the network object type, you must specify a single WAN IP address to add to the pool. Enter a valid WAN IP address then click **OK** to continue.

Note: NAT/NAPT configuration—User defined work object must be contained in the device's IP address pool. Refer to section 15.11, "Network Objects," for details.



13.8 Advanced Filtering

If you select **Firewall Settings** in the top navigation menu and then select **Advanced Filtering** in the left submenu, the following screen appears.

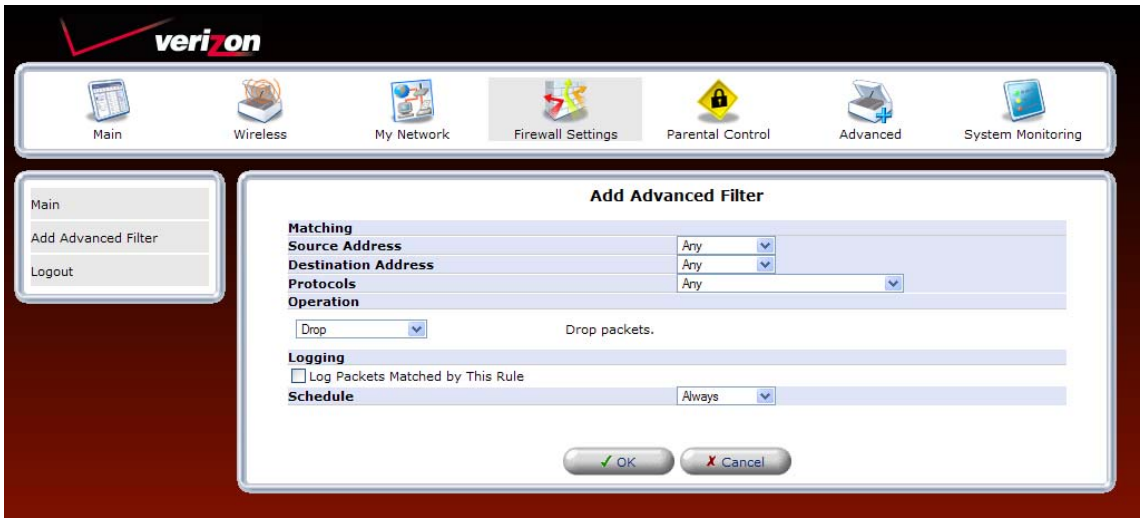
Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

This screen is divided into two sections: one for Input Rule Sets and the other for Output Rule Sets, which are for configuring inbound and outbound traffic, respectively. Each section comprises subsets, which can be grouped into three main subjects:

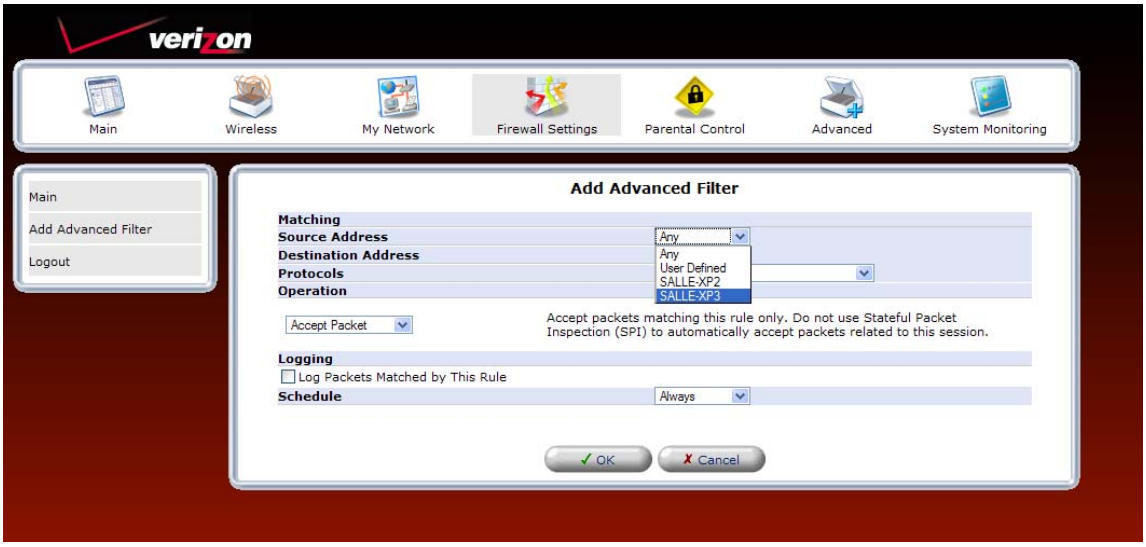
- Initial rules—rules defined here will be applied first, on all gateway devices.
- Network device rules—rules can be defined per each gateway device.
- Final rules—rules defined here will be applied last, on all gateway devices.

To add rules to Input or Output rules sets, click the adjacent **New Entry** link.

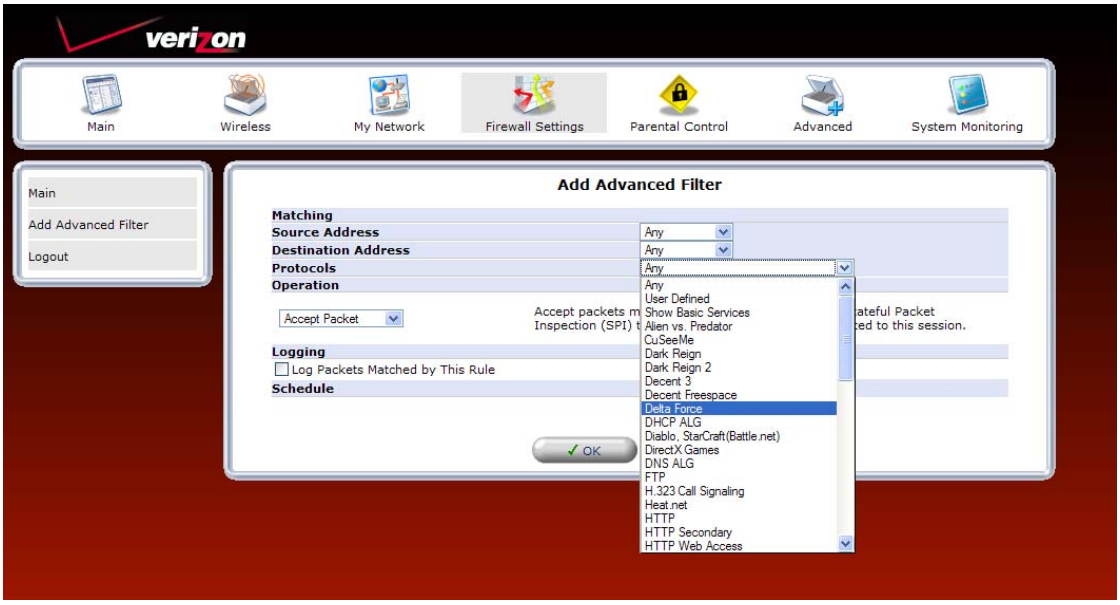
For example, in the preceding screen, under **Input Rule Sets,** if you click the **New Entry** link next to **Network (Home/Office) Rules,** the following screen appears.



Select the desired address from the **Source Address/Destination Address** drop-down list.

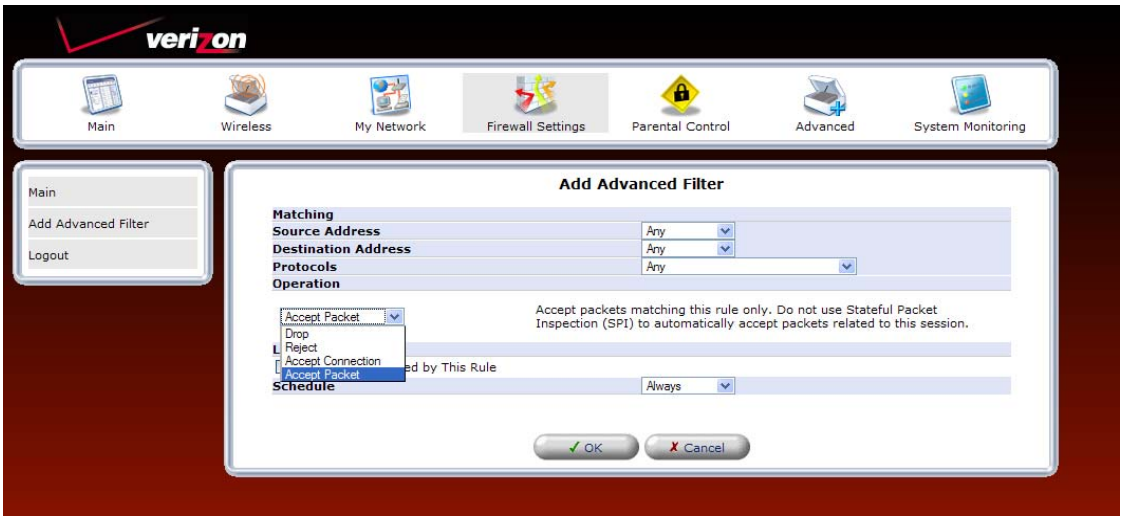


Next, select the desired protocol from the **Protocols** drop-down list.



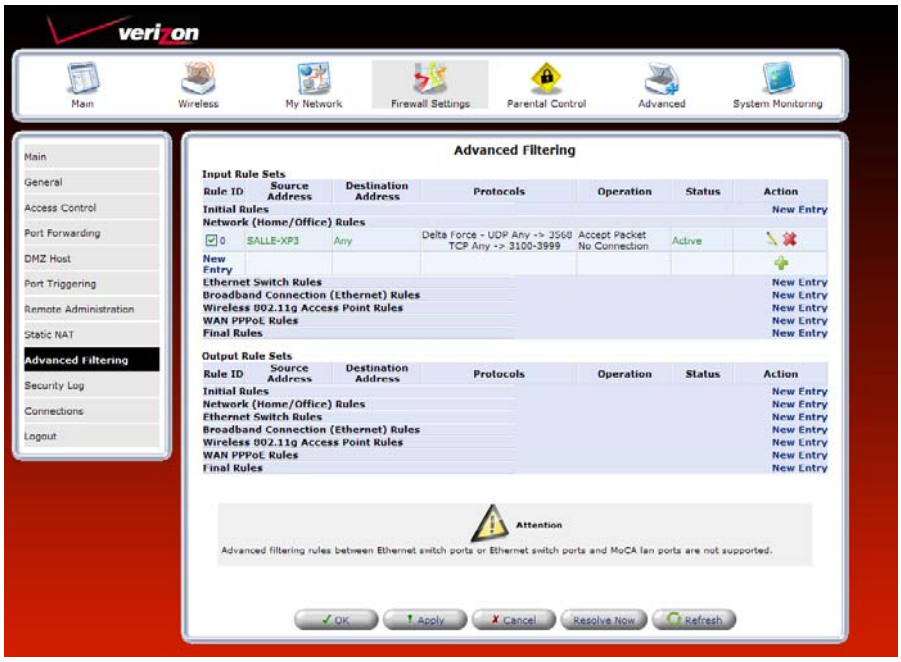
Select one of the following settings from the **Operation** drop-down list:

- Select **Drop** to drop packets.
- Select **Reject** to drop packets, and to send TCP Reset or ICMP Host Unreachable packets to the sender.
- Select **Accept Connection** to accept all packets related to this session.
- Select **Accept Packet** to accept packets matching this rule only. Do not use Stateful Packet Inspection (SPI) to automatically accept packets related to this session.



After you have selected the desired values, the following screen appears. If you want to log packets matched by this rule, click the check box located under **Logging**. If you want to set up a schedule for this rule, refer to section 15.21 for instructions on creating a schedule rule. After you have finished entering the desired settings in this screen, click **OK** to continue.

If you clicked **OK**, the following screen appears. The rule is now active. To add additional rules, click the **New Entry** link next to the rule that you want to set up.



The order of the rules appearance represents both the order in which they were defined and the sequence by which they will be applied. By clicking the Move Up and Move Down action icons, you can change this order after your rules are already defined (without having to delete and then re-add them). After you click the desired icon, the screen will refresh and display the change.

0	10.10.1.5	192.168.1.50	Dark Reign 2 - TCP Any -> 26214 UDP Any -> 26214	Drop	Active	
1	234.10.65.25	192.168.1.51	FTP - TCP Any -> 21	Accept Connection	Active	

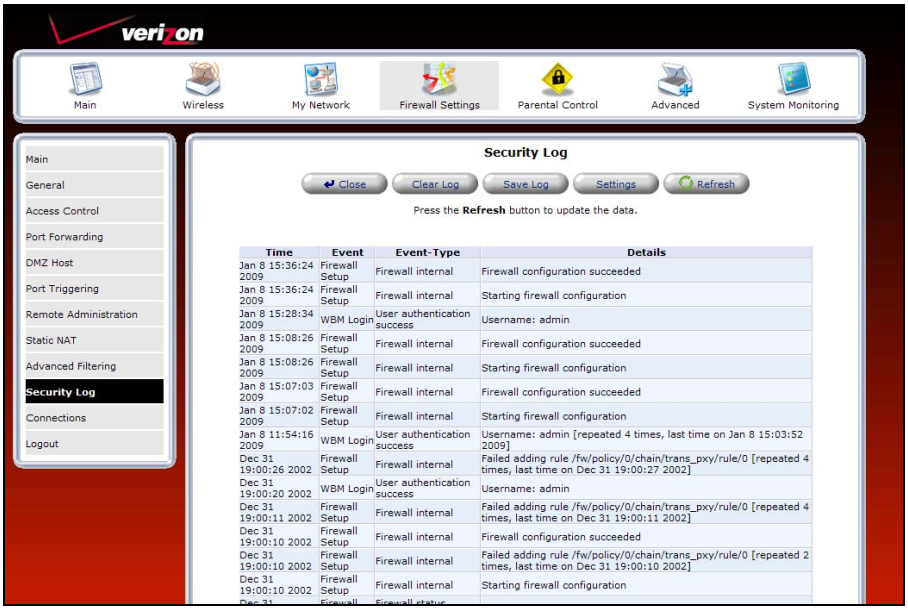
13.9 Security Log

If you select **Firewall Settings** in the top navigation menu and then select **Security Log** in the left submenu, the following screen appears.

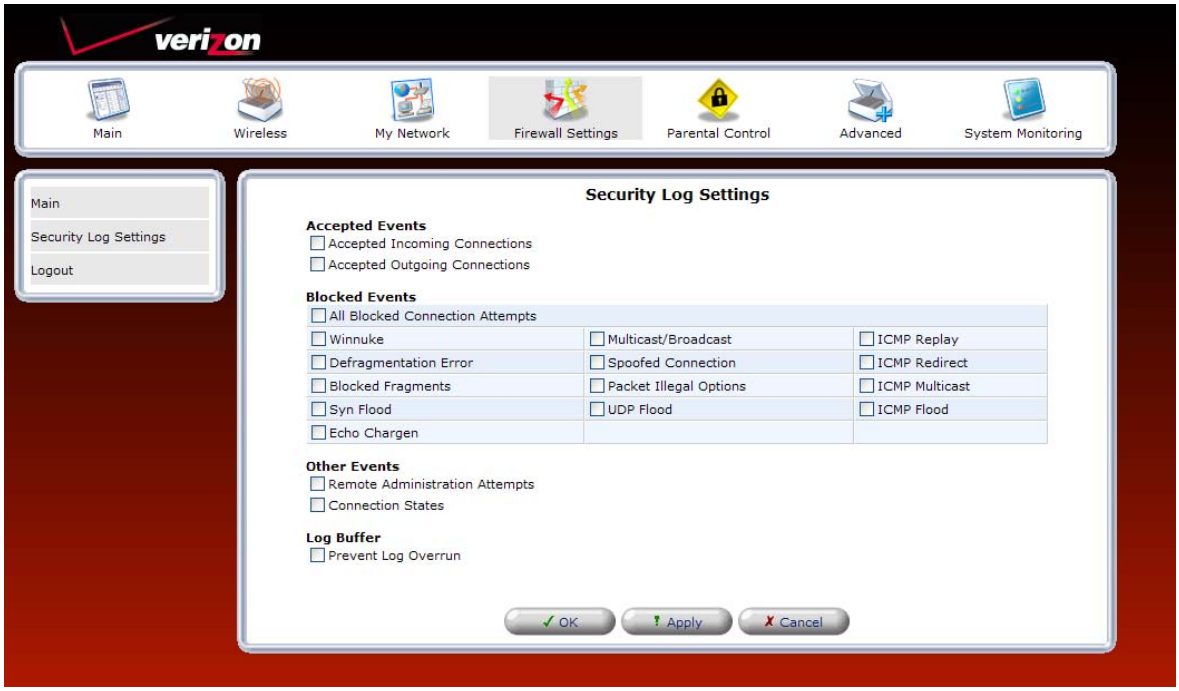
This screen alerts you of noteworthy information sent to the Router from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur. In this screen, do any of the following:

- Click **Close** to close the security log screen.
- Click **Clear** Log to remove all entries from the log.
- Click **Save** to save the settings to a syslog server.
- Click Settings to configure the security settings. Clicking this button opens a new window that contains configuration options for selecting the information that you want logged.
- Click **Refresh** to refresh the security log screen.

To configure the security log settings, click the **Settings** button.



If you clicked **Settings**, the following screen appears. Select the desired settings by clicking the check boxes (a checkmark will appear in the box when a setting is enabled). Then, click **Apply** to save the settings.



Select the types of activities for which you would like to have a log message generated:

- Accepted Events
  Accepted Incoming Connections: Write a log message for each successful attempt to establish an inbound connection to the home network.
  Accepted Outgoing Connections: Write a log message for each successful attempt to establish an outgoing connection to the public network.
- Blocked Events
  All Blocked Connection Attempts: Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.
  Specific Events: Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check-box is checked, or the "All Blocked Connection Attempts" check-box is checked.
- Other Events
  Remote Administration Attempts: Write a log message for each remote-administration connection attempt, whether successful or not.

  Connection States: Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and the Application Level Gateways (ALGs).
- Log Buffer
  Prevent Log Overrun: Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.

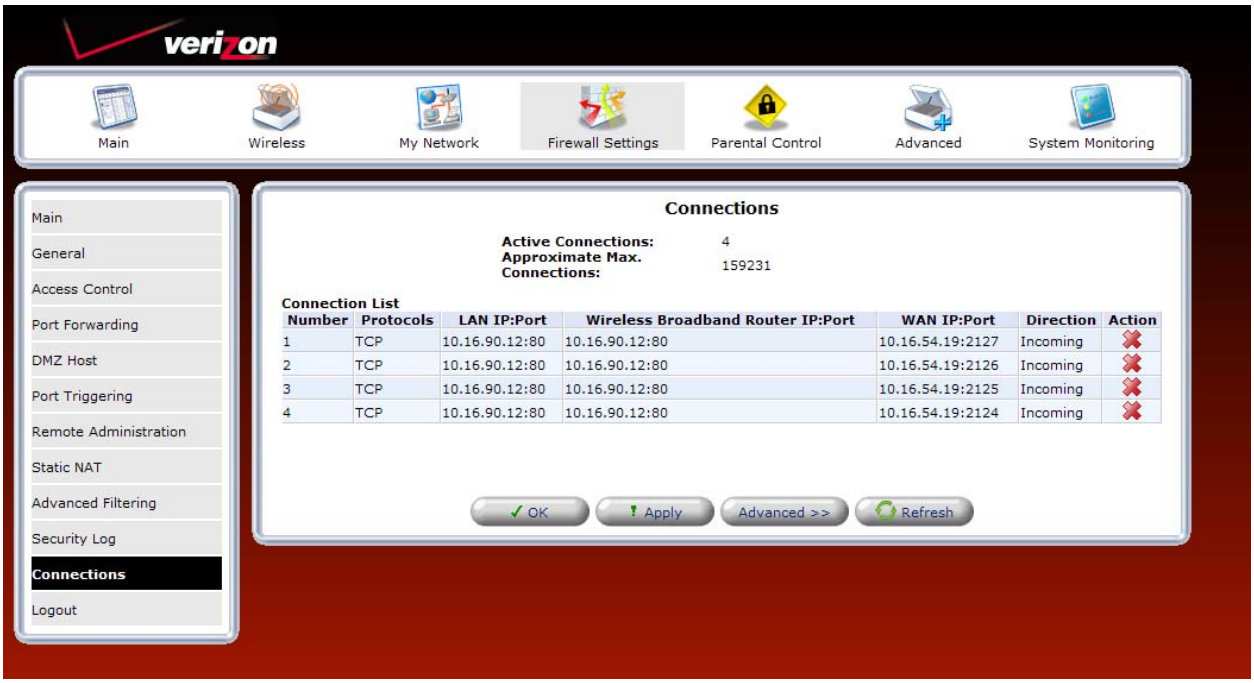
13.10 Connections

If you select **Firewall Settings** in the top navigation menu and then select **Connections** in the left submenu, the following screen appears.

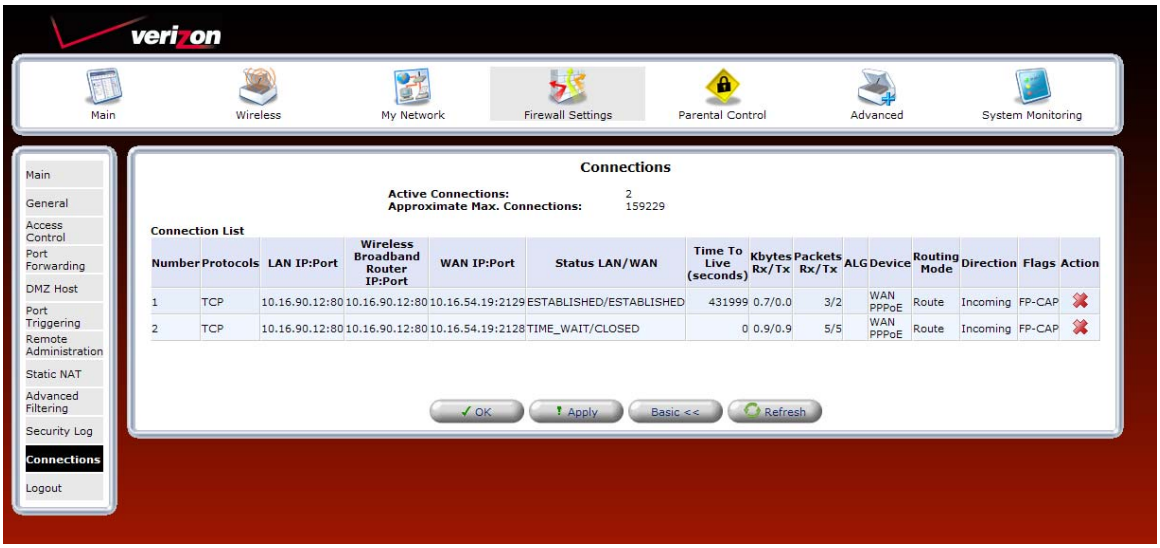
The connections list displays all the connections that are currently open on the firewall, as well as various details and statistics. You can use this list to close undesired connections by clicking the "X" icons. The basic display includes the protocol type, the different ports it uses, and the direction of the secured traffic.

- Active Connections—this value represents the number of active concurrent connections.
- Approximate Max. Connections—this value represents the amount of additional concurrent connections possible.
- Connections Per Page—use this drop-down list to select the number of connections to display at once.

Click the **Advanced** button to display a more detailed connection list.



If you clicked **Advanced**, the following screen appears. Additional details in this page include connection status (LAN/WAN), time-to-live, number of kilo-bytes and packets received and transmitted, ALG device, routing mode, and flags. To close a undesired connection, click the adjacent "X" icon.

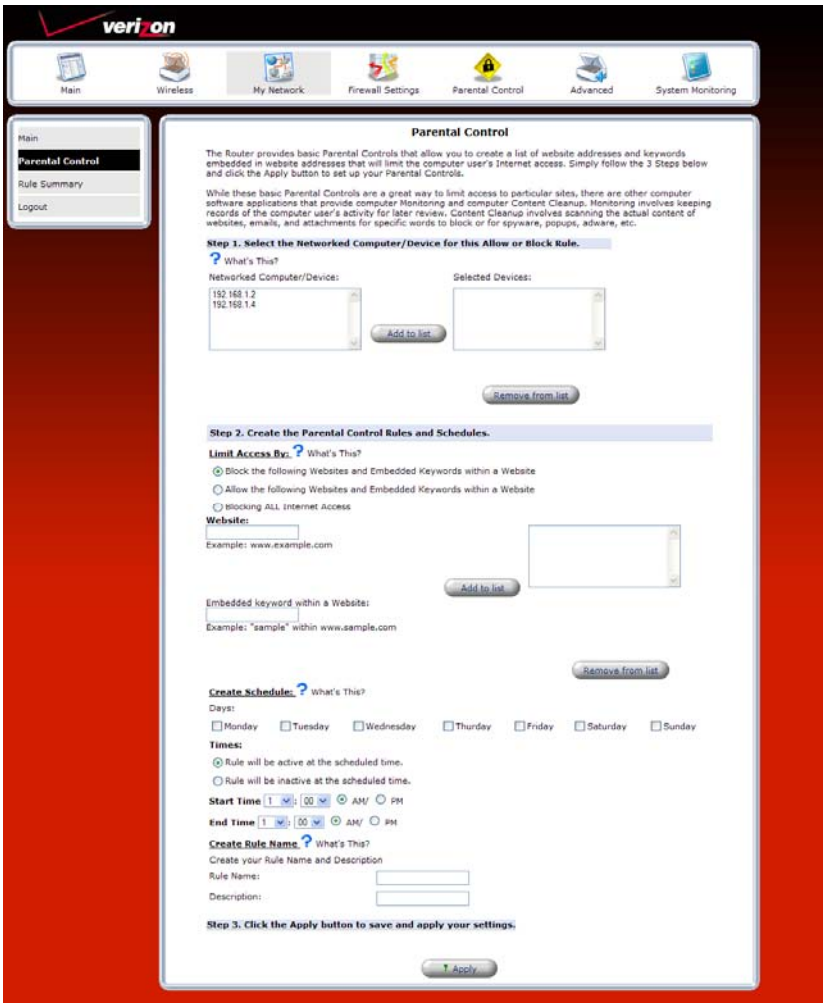


14. PARENTAL CONTROLS

If you select **Parental Controls** in the top navigation menu, the following screen appears. The Router provides basic Parental Controls that allow you to create a list of Web site addresses and keywords embedded in website addresses that will limit the computer user's Internet access. Simply follow the 3 steps below, and click the **Apply** button to set up your Parental Controls.

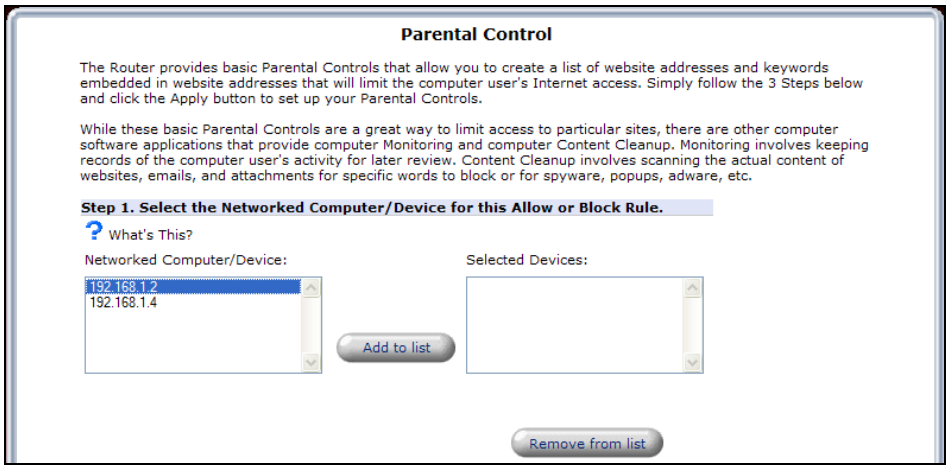
While these basic Parental Controls are a great way to limit access to particular sites, there are other computer software applications that provide computer Monitoring and computer Content Cleanup. Monitoring involves keeping records of the computer user's activity for later review. Content Cleanup involves scanning the actual content of websites, emails, and attachments for specific words to block or for spyware, popups, adware, etc.

The following steps guide you through configuring Parental Controls. If you have questions about a feature, click the ? What's This? icon to learn more about that feature.

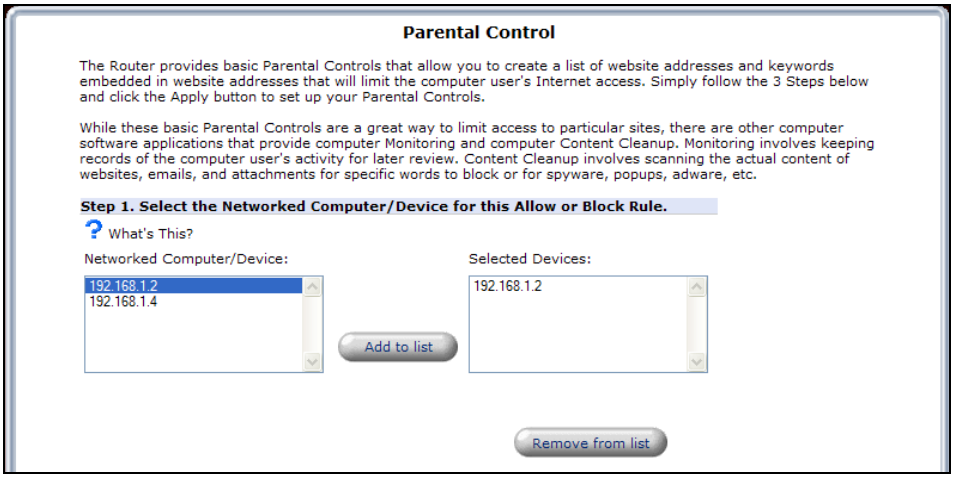


1. In the **Networked Computer/Device** box, select the device that will receive this rule. Then click the **Add to list** button.

Note: You can select only specified devices, not specific accounts on these devices.



The selected device will appear in the **Selected Devices** box. If you want to remove a device from the **Selected Devices** panel, click the **Remove from list** button.

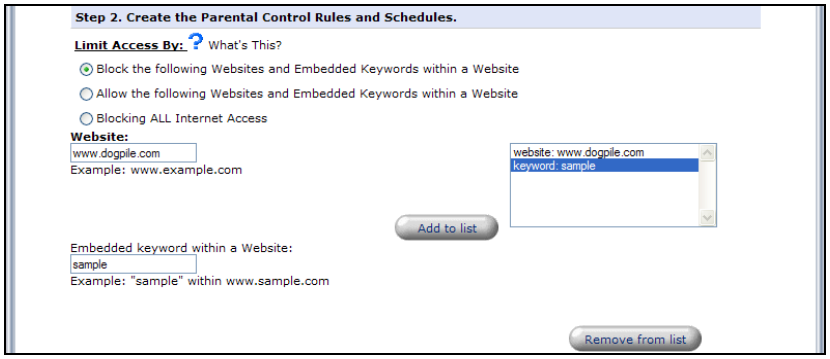


2. Below **Limit Access By,** click the option button next to the rule that you want to apply. Then in the box labeled **Website,** enter a website domain name (for example, www.example.com) and click the **Add to list** button.

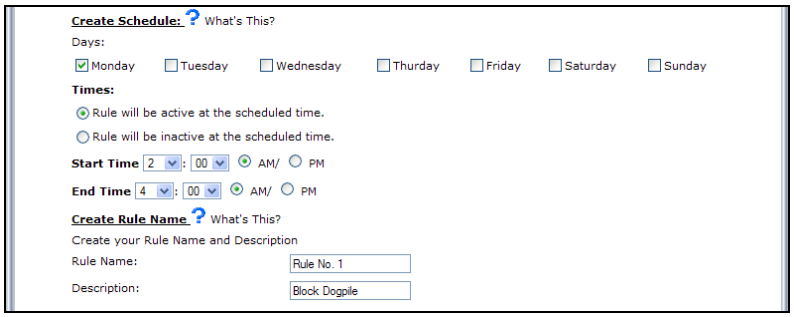
IMPORTANT: The Router does not block or allow based on content of websites, emails, or attachments, only based on website addresses or keywords embedded in those website addresses.

The domain name will appear in the Add to list box.

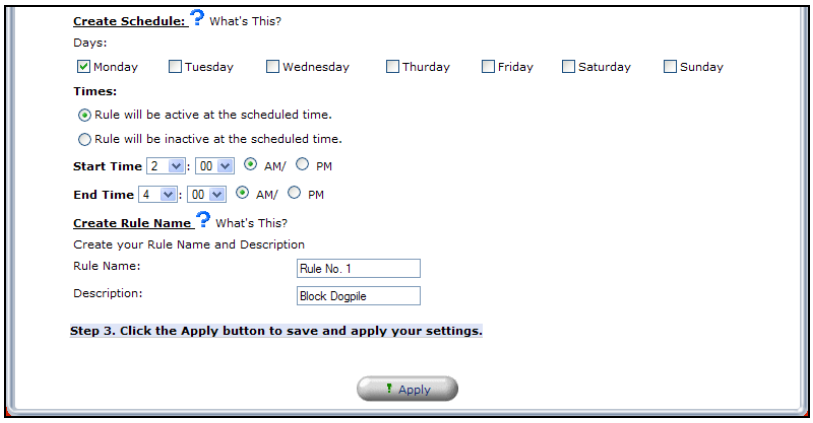
If you want to embed a keyword, type the word in the box provided, and then click the **Add to list** button. If you want to remove a website domain name from the box, click the **Remove from list** button.



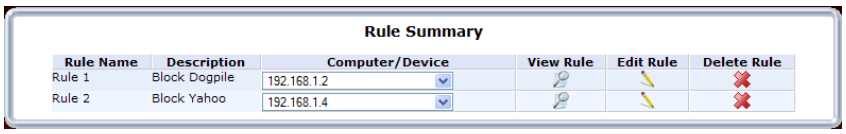
To set up a schedule rule for the website restriction in the section labeled **Create a Schedule**, enter the desire settings in the fields provided. Then in the section labeled **Create Rule Name,** enter the desired rule name and description.



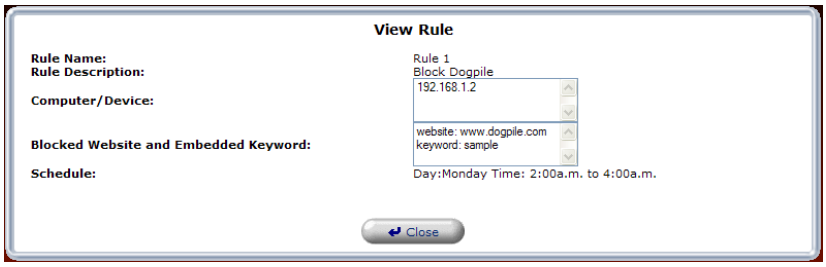
3. After you have entered the desired settings, click the **Apply** button to save the settings to the Router.



After you click **Apply**, the following screen appears. Click any of the icons (view, edit, or delete) next to the website rule that you want to view or modify.



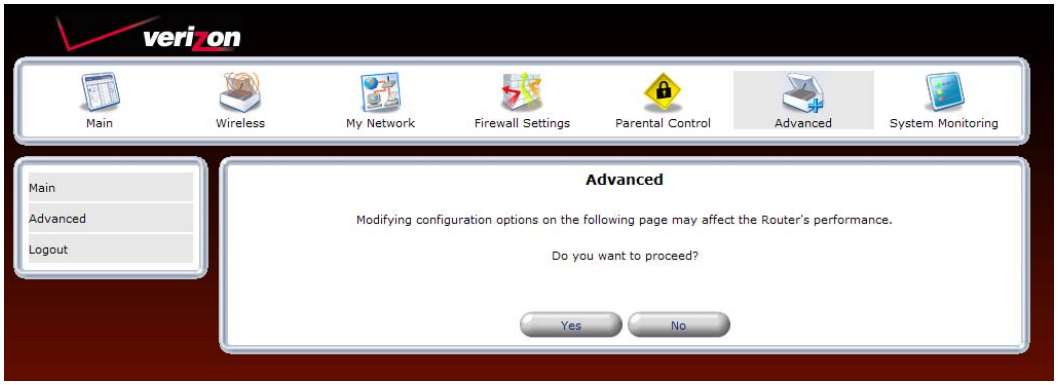
If you click the **View Rule** icon, the following screen appears. After viewing this screen, click **Close** to return to the **Rule Summary** page.



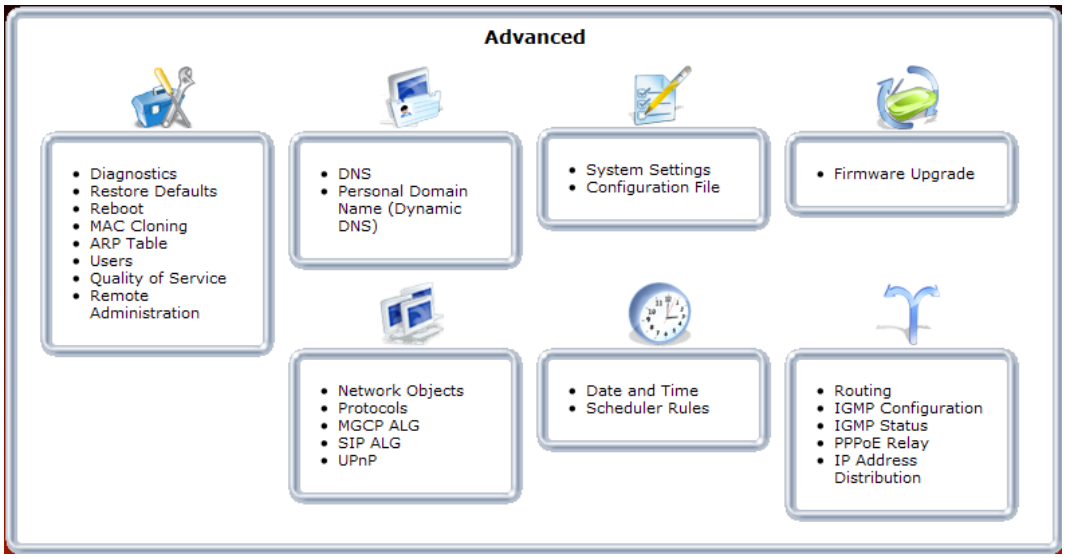
15. ADVANCED

If you select **Advanced** in the top navigation menu, the following screen appears. The Advanced section of this User Guide is intended to provide assistance with configuring the Advanced features of your Verizon FiOS Router and assumes that the user has an in-depth understanding of computers, routing, and Internet networking.

Click **Yes** to proceed to the Router's **Advanced** screen.



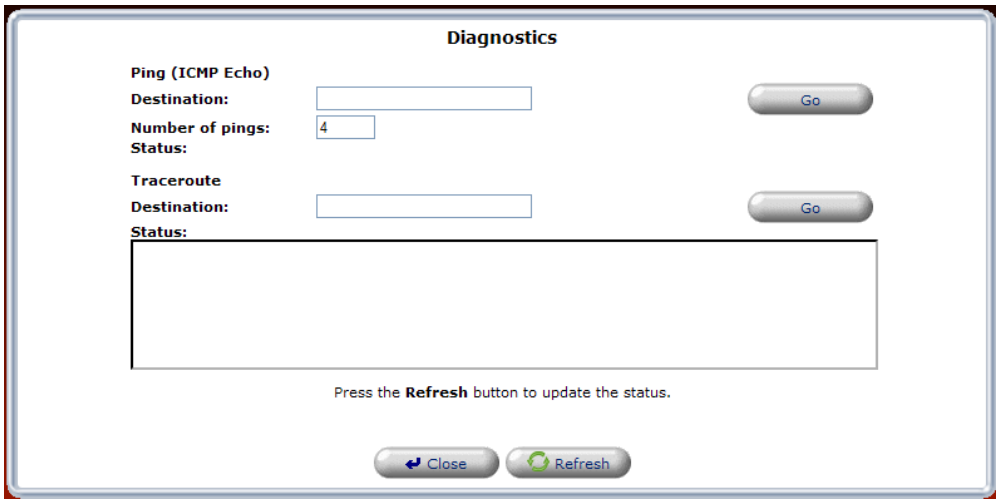
Clicking the links in the **Advanced** screen allows you to access various configurable settings in your Router.



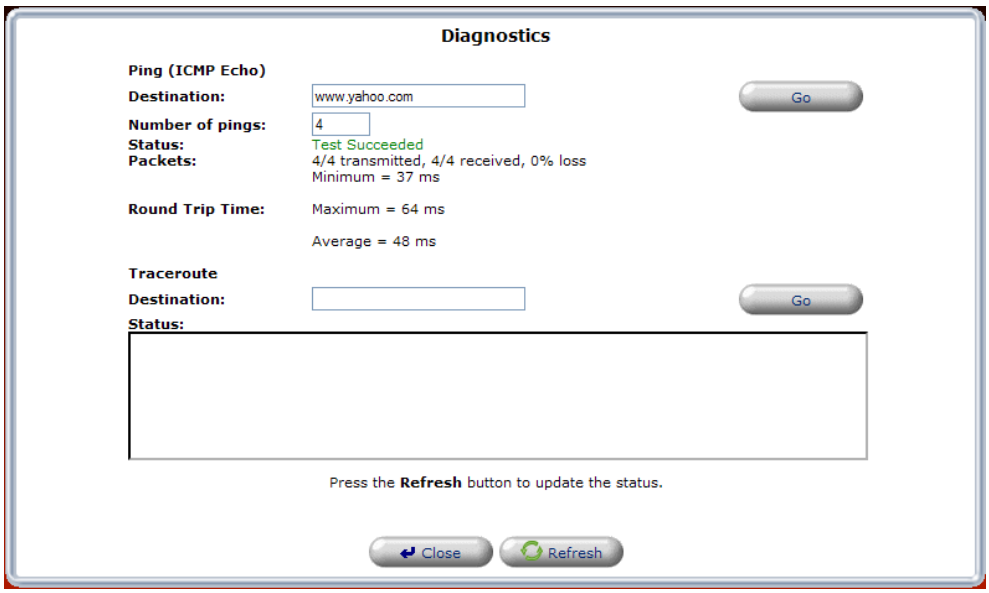
15.1 Diagnostics

If you click the **Diagnostics** link in the **Advanced** screen, the following screen appears. Using this screen, you can run the following diagnostics tests:

- To run a PING test, type the appropriate IP address or host name in the field provided, and then click **Go.**
- To run a Traceroute test, type the appropriate IP address or host name in the field provided, and then click **Go.**



For example, if you enter a host name in the **Destination** field and then click **Go**, the following screen appears. This screen shows that the Ping test succeeded. Click **Close** to return to the **Advanced** screen.



15.2 Restore Defaults

If you click the **Restore Defaults** link in the **Advanced** screen, the following screen appears. Click **OK** to allow the Router to be reset to factory default settings. After the Router has rebooted, you will need to log in to the Router.

IMPORTANT: If you click **OK**, any settings that you have configured in the Router will be erased, and any data that the Router has reported will be lost.

15.3 Reboot

If you click the **Reboot** link in the **Advanced** screen, the following screen appears. Rebooting the Router allows the Router to be restarted. Click **OK** to allow the Router to reboot. Please wait a brief moment while the Router is rebooting. Afterwards, you will need to log in to the Router.

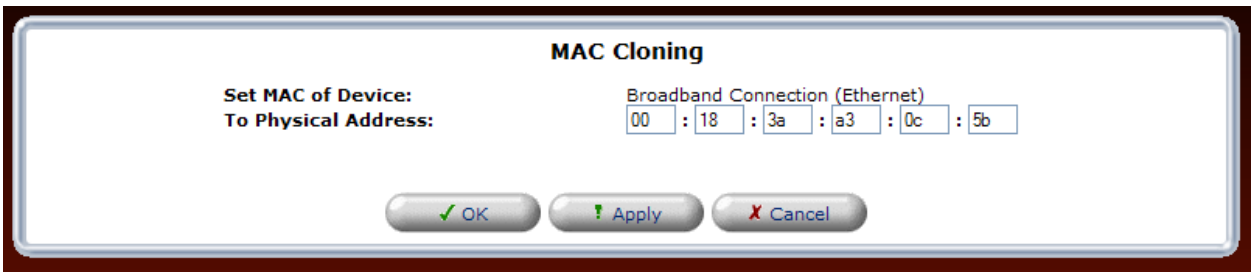
IMPORTANT: The **Reboot** feature does not reset the Router to factory default settings. If you want to reset the Router to factory default settings, follow the instructions in section 15.2, "Restore Defaults."

15.4 MAC Cloning

If you click the **MAC Cloning** link in the **Advanced** screen, the following screen appears. A Media Access Control (MAC) address is a hexadecimal code that identifies a device on a network, such as a router. All networking devices have a MAC address, and in some cases, your service provider may need you to provide the MAC address of your network device. If you use MAC Cloning, you can simply enter the MAC address of the "old" Router into your Verizon Router, bypassing the need to contact the service provider with "new" MAC Address values (from the Verizon Router).

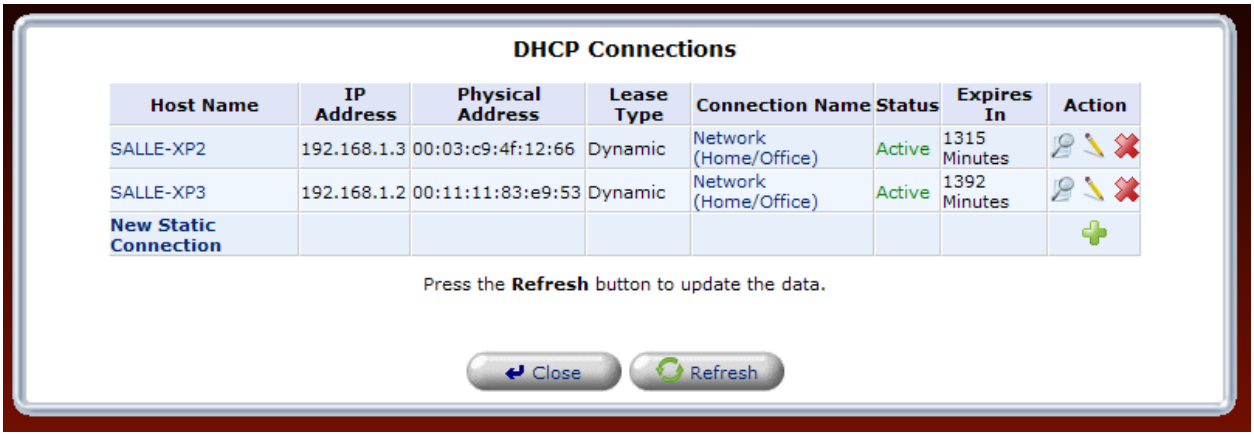
To configure MAC Cloning, enter the MAC Address of the Router you are replacing. Then, click **Apply** to save the settings.

NOTE: By default, this screen displays the MAC address of the Verizon Router. Replace these values with the MAC address of your "old" Router and click **Apply.**



15.5 ARP Table

If you click the **ARP Table** link in the **Advanced** screen, the following screen appears. This screen allows you to set up static DHCP connections using Host Names, IP Addresses, or MAC addresses. To configure a static DHCP connection, click the **New Static Connection** link.

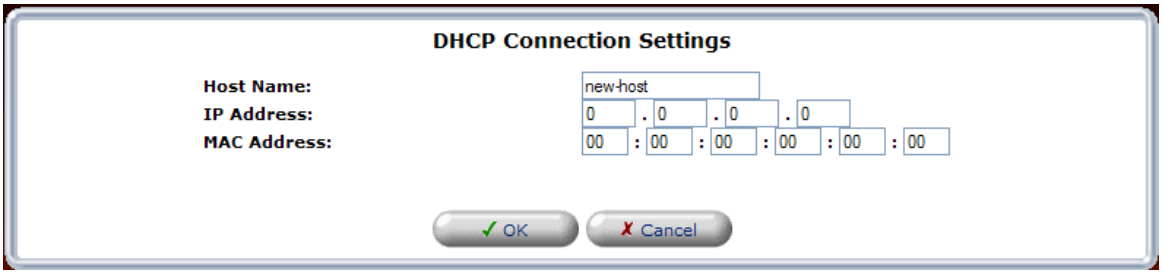


If you clicked **New Static Connection,** the following screen appears. Enter the appropriate values in the fields provided, and then click **OK** to continue.

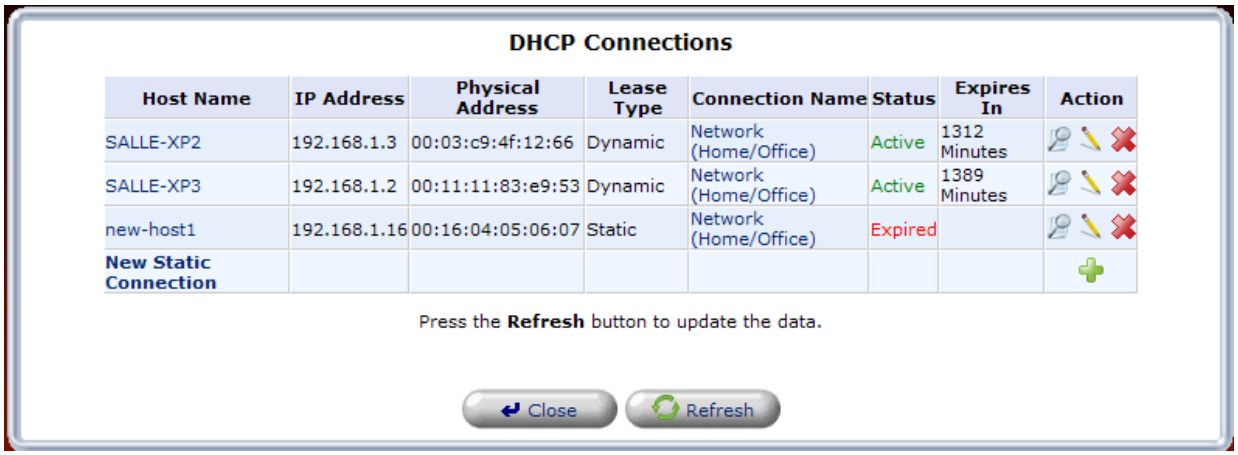
NOTE: You can have a total of 253 static LAN devices connected to your Verizon Router.

- Enter a host name for this connection.
- Enter the fixed IP address to assign to the computer.
- Enter the MAC address of the computer's network card.

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.



For example, if you enter an IP Address and a MAC address and then click **OK**, the following screen appears. The screen shows that the entry has been added to the list of static DHCP connections. To run a diagnostics test on a DHCP connection, click the diagnostics icon adjacent to the connection you want to test. To remove a host from the table, click the appropriate "X" icon in the Action column.



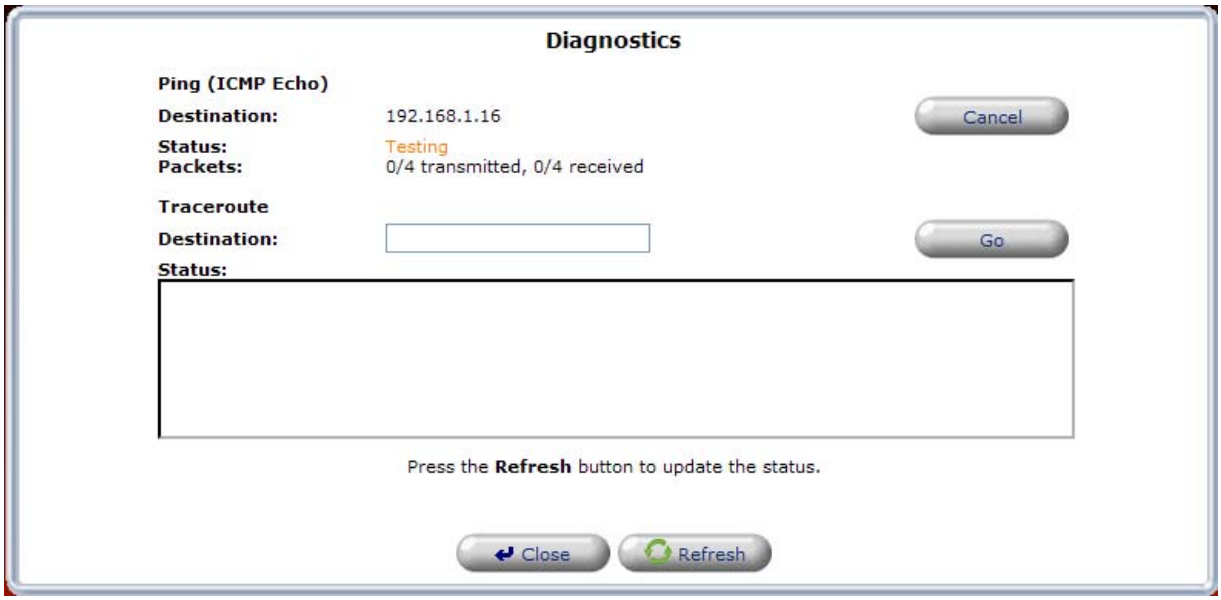
DHCP Connections

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
SALLE-XP2	192.168.1.3	00:03:c9:4f:12:66	Dynamic	Network (Home/Office)	Active	1312 Minutes	
SALLE-XP3	192.168.1.2	00:11:11:83:e9:53	Dynamic	Network (Home/Office)	Active	1389 Minutes	
new-host1	192.168.1.16	00:16:04:05:06:07	Static	Network (Home/Office)	Expired		
New Static Connection							

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

Close Refresh

If you clicked the diagnostics icon, the following screen appears. Review the status of the diagnostics test, and then click **Close** to return to the **DHCP Connections** screen.



Diagnostics

Ping (ICMP Echo)

Destination: 192.168.1.16 Cancel

Status: Testing

Packets: 0/4 transmitted, 0/4 received

Traceroute

Destination: Go

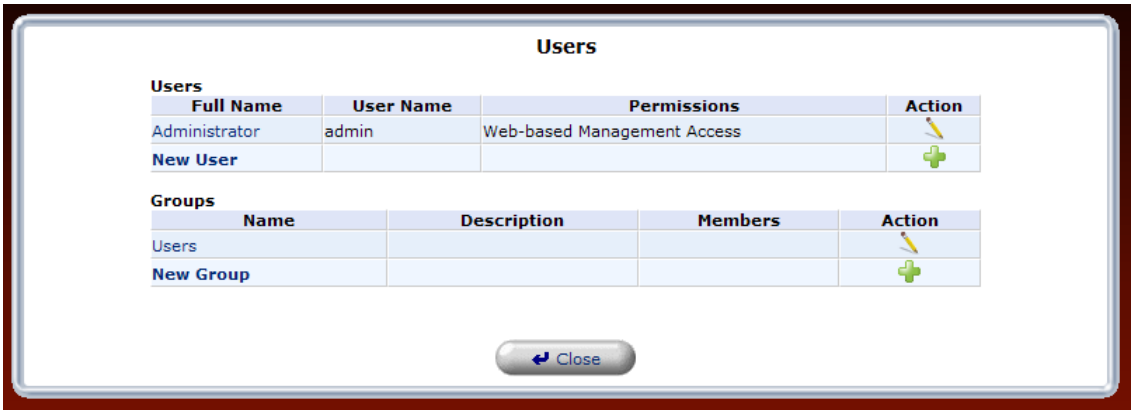
Status:

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

Close Refresh

15.6 Users

If you click the **Users** link in the **Advanced** screen, the following screen appears. This feature allows you to configure user settings in the Router.

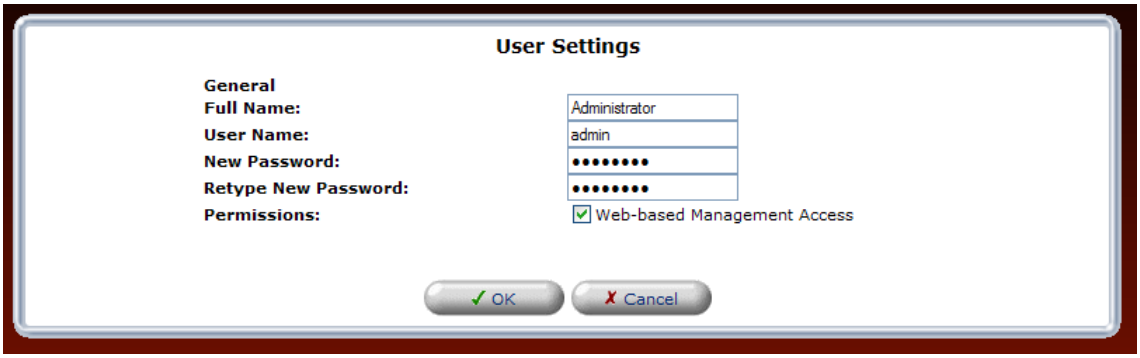


15.6.1 Users—Adding a New Administrator

If you click the **Administrator** link in the **Users** screen, the following screen appears. This screen allows you to set up the desired Administrator values. Enter the appropriate values, and then click **OK** to save the changes.

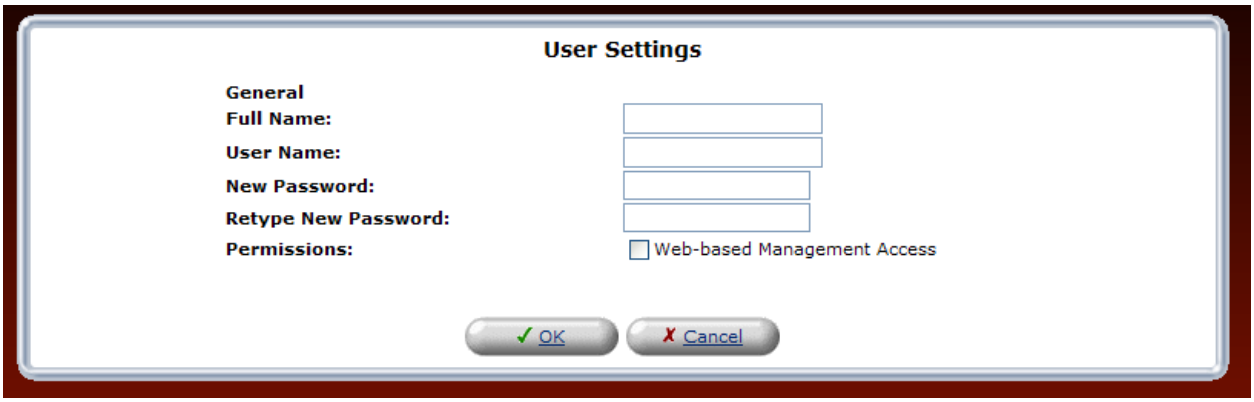
NOTE: If the Router is password protected and you are not an authorized user, you will not be allowed to change and save the values in this screen. (The Router cannot be configured unless the user is logged in.) Contact your network administrator for further instructions.

- Full Name—Enter the user's full name.
- User Name—Enter the name a remote user will use to access the home or office network. This field is case-sensitive.
- New Password/Retype New Password—Enter the password for the user (and enter it again to confirm).
- Permissions—Click the check box to enable web-based management access.



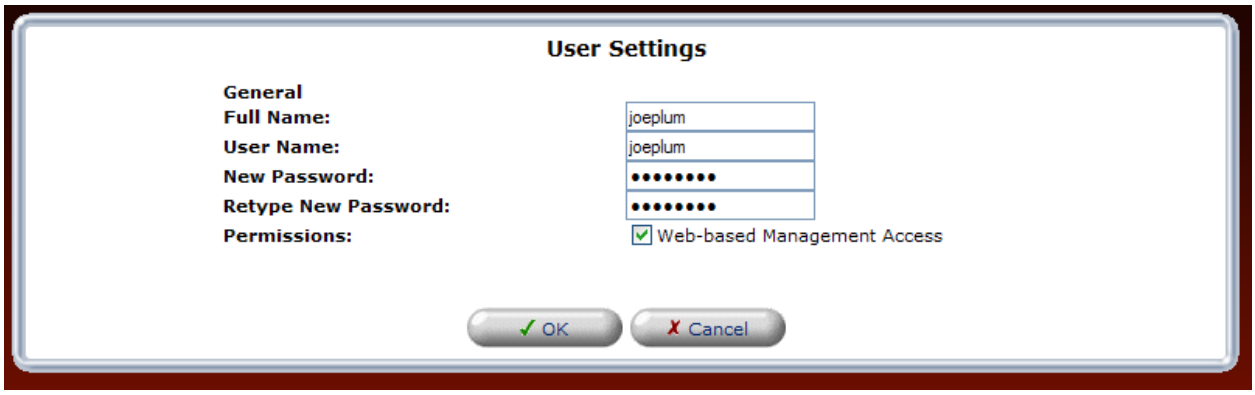
15.6.2 Users—Adding a New User

If you click the **New User** link, the following screen appears. This screen allows specific users to have administrative permissions in the Router.

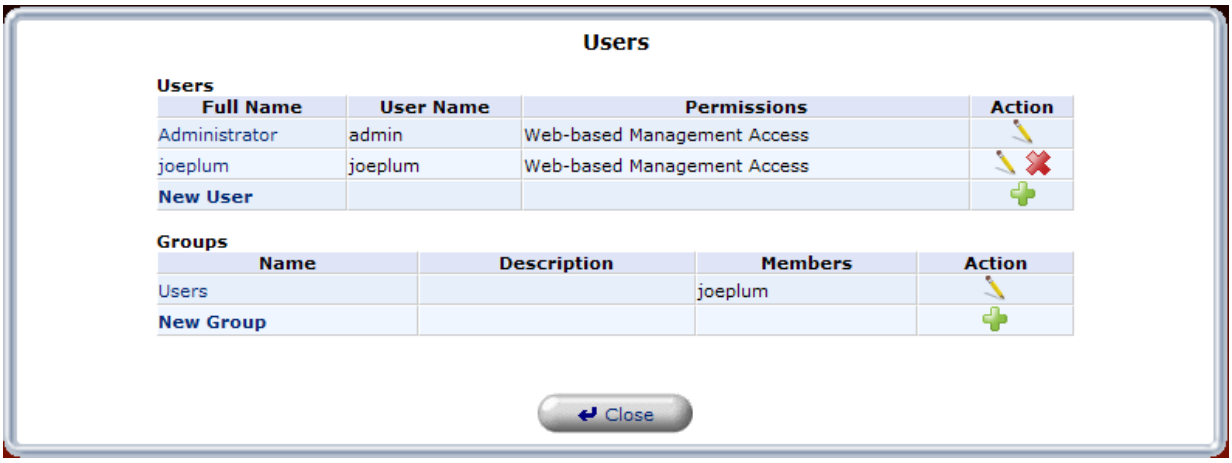


To configure User Settings, enter the appropriate values, and then click **OK** to save the changes.

NOTE: The User Name and Password values must be at least 6 characters, and should consist of standard characters only (ASCII 32-126), excluding the special character space and any of these characters :**@"**|\/=+<>**[]*?,;**. Also, user names containing capital letters are not recommended. It might cause connectivity problems on Windows 98 hosts.

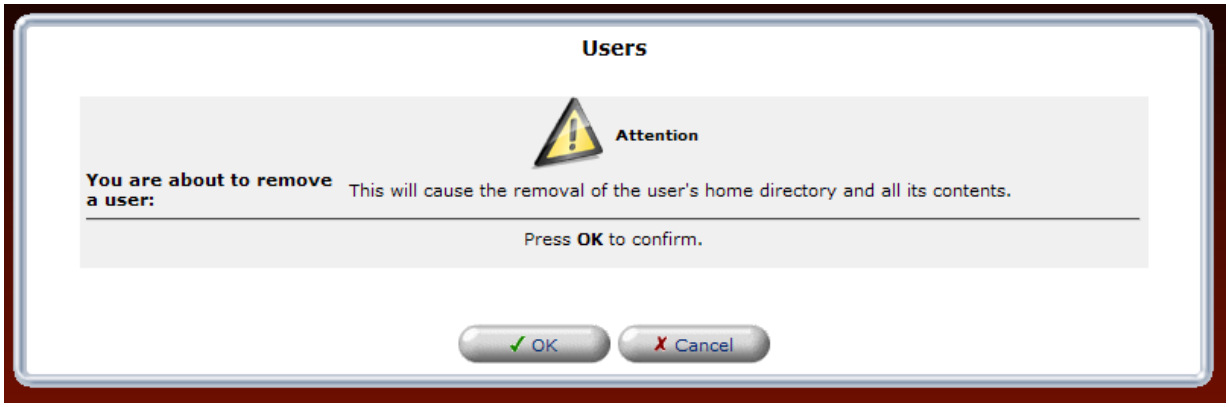


After you have entered the appropriate values and click **OK**, the following screen appears. The user information has been added to the Router. If desired, repeat the preceding instructions to add additional users to the administrator permissions list.



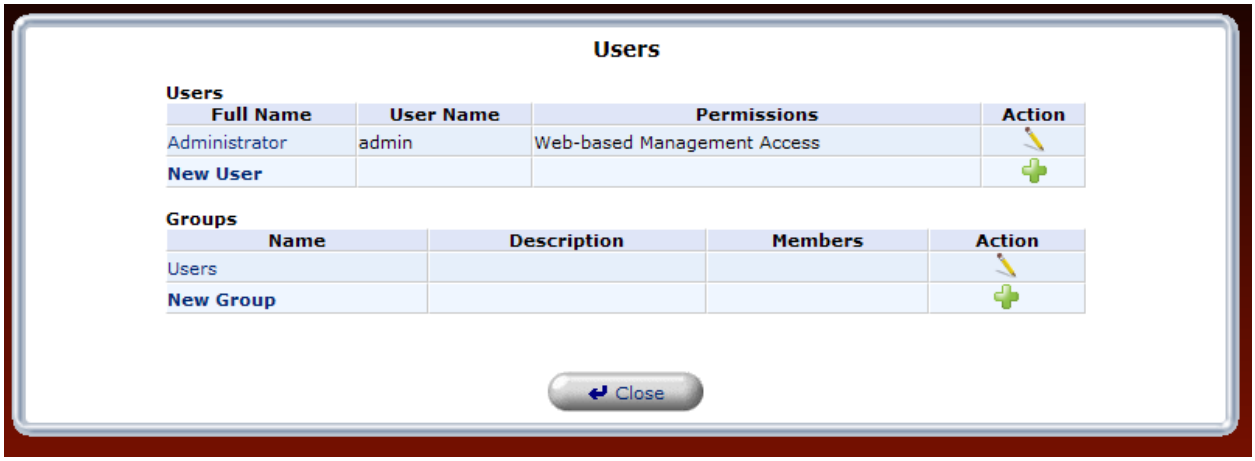
15.6.3 Users—Removing a User

To remove a user from the list, click the "X" icon. The following screen appears. Click **OK** to continue.



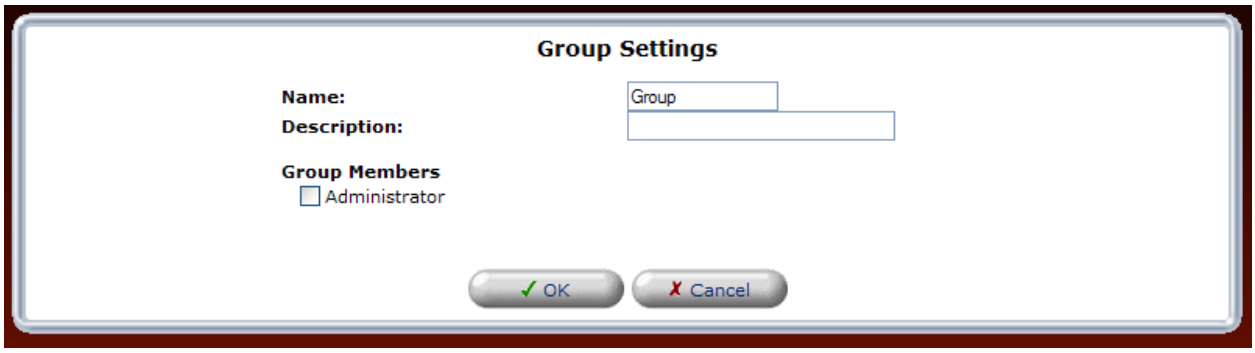
15.6.4 Groups—Adding a New Group

To add a new group, click the **New Group** link.

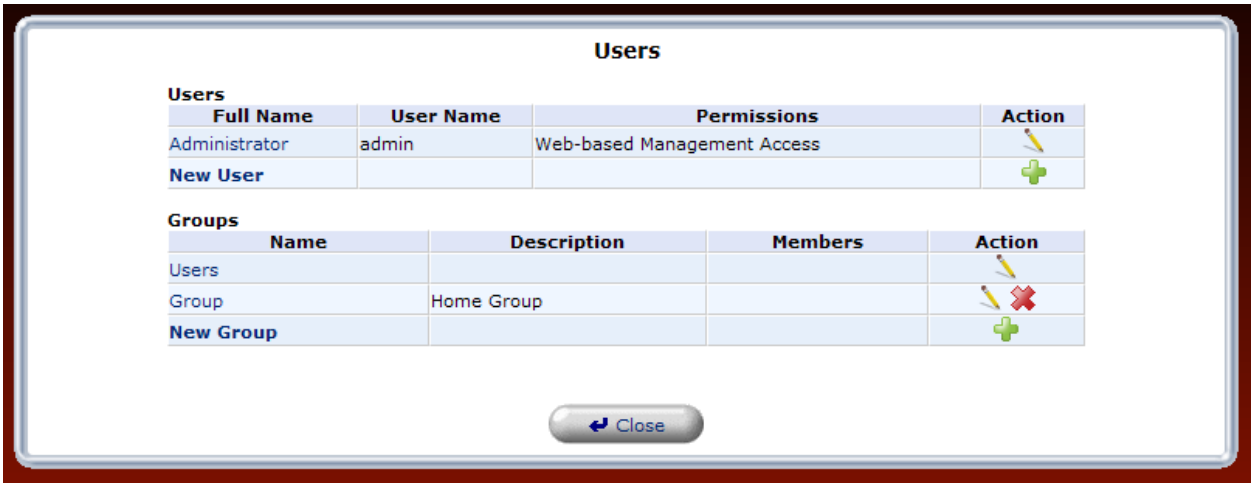


If you clicked the **New Group** link, the following screen appears. Using this screen, you can configure additional groups in the Router. At this screen, do the following:

1. Enter a Group Name of your choice.
2. Enter a description of your choice.
3. If you want to assign administrative permissions to the group, click the **Group Members Administrator** check box; otherwise, leave this box empty.
4. Click **OK** to save the settings.



After you have entered the desired values and clicked **OK**, the following screen will display the group attributes. Click **Close** to return to the **Advanced** screen.

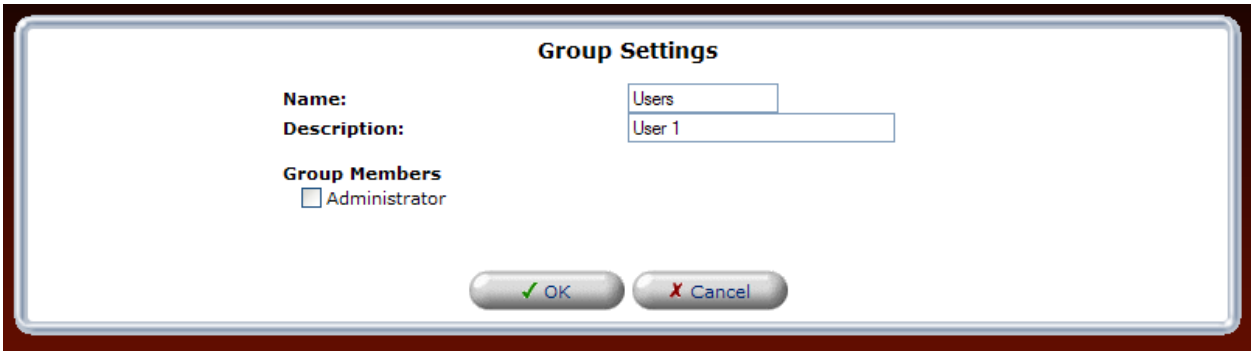


15.6.5 Groups—Add a User to a Group

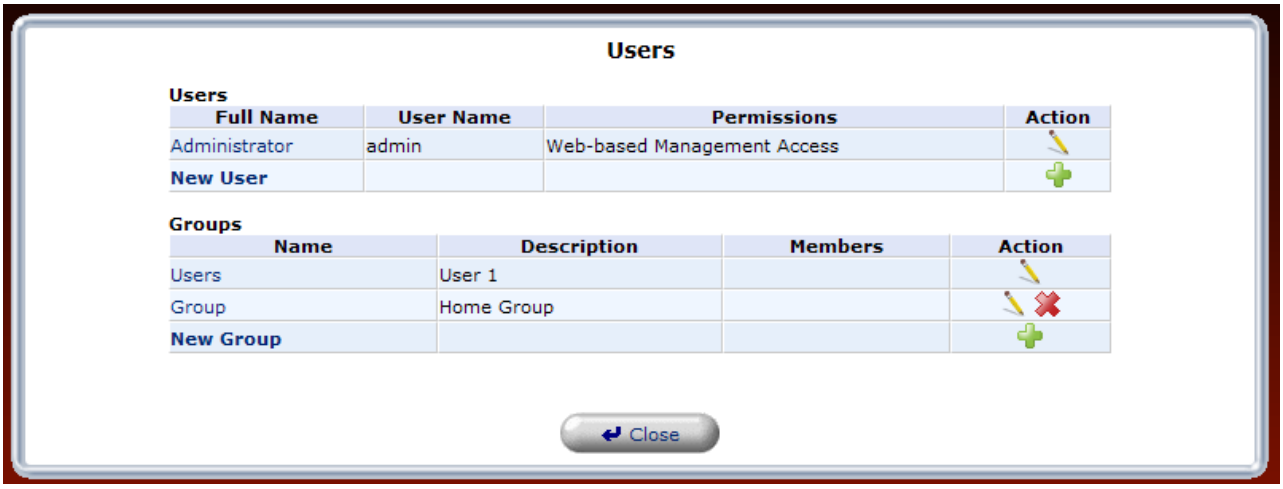
To set up new users for a group, click the **User** link in the **Groups** section of the screen. The following screen appears. Using this screen, you can assign users to a designated group.

At this screen, do the following:

1. Enter a User name of your choice.
2. Enter a description of your choice.
3. If you want to assign administrative permissions to the user, click the **Group Members Administrator** check box; otherwise, leave this box empty.
4. Click **OK** to save the settings.



After you have entered the desired values and clicked **OK**, the following screen will display the group attributes. Click **Close** to return to the **Advanced** screen.



15.7 Quality of Service

The QoS feature allows you to configure Quality of Service parameters in your Router. Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. 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.

15.7.1 General

If you click the **Quality of Service** link in the **Advanced** screen, the following screen appears. This screen allows you to configure general QoS settings. Enter the appropriate settings, and then click **Apply**.

NOTE: Choosing a new QoS profile will cause all previous QoS settings to be lost.

Before selecting the QoS profile that mostly suits your needs, select your bandwidth from this combo-box. If you do not see an appropriate entry, select 'User Defined', and enter your Tx and Rx bandwidths manually.

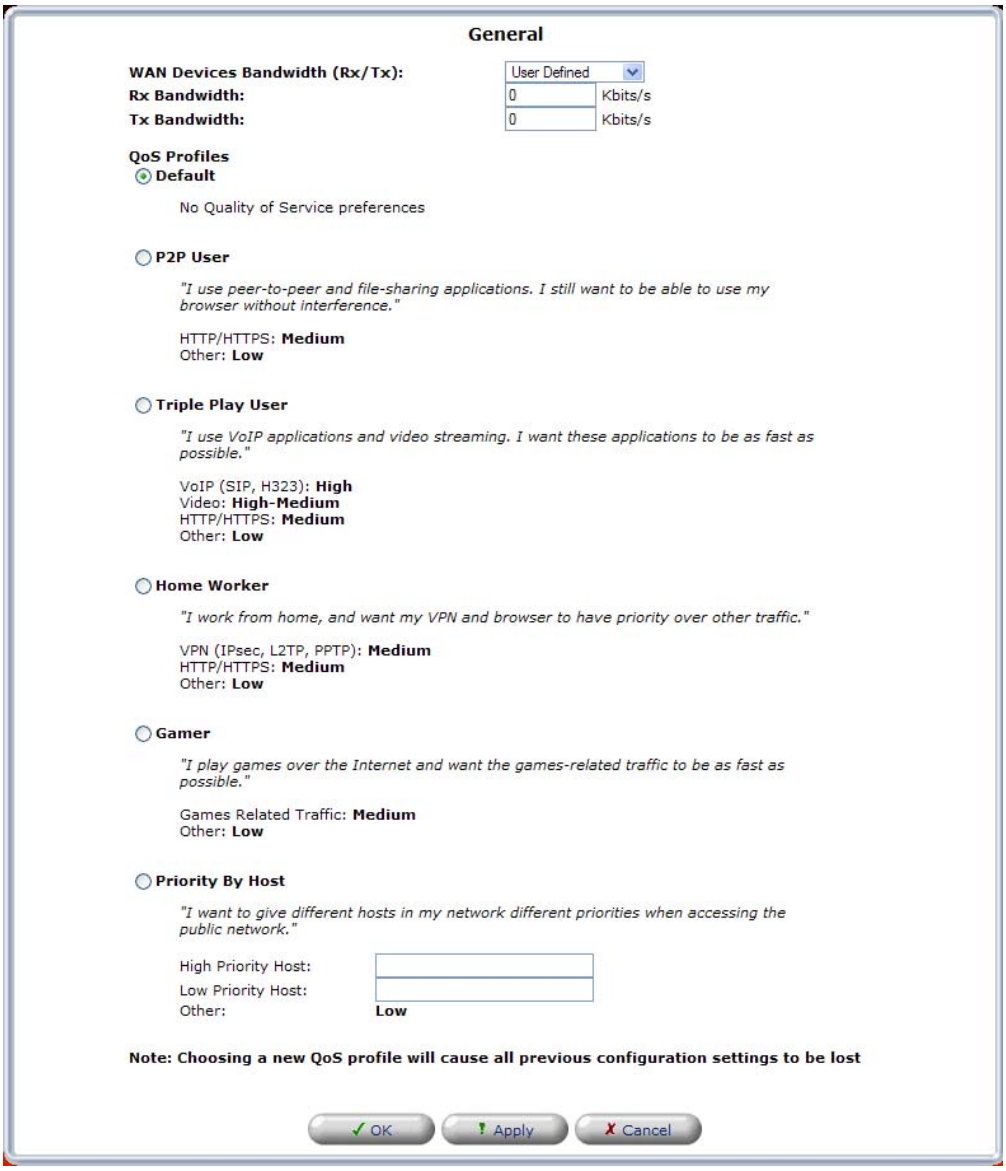
- Enter your Tx bandwidth in Kbits per second.
- Enter your Rx bandwidth in Kbits per second.

Select the profile that mostly suits your bandwidth usage. Each profile entry displays a quote describing what the profile is best used for, and the QoS priority levels granted to each bandwidth consumer in this profile.

- Default - No QoS preferences
- P2P User - Peer-to-peer and file sharing applications will receive priority
- Triple Play User - VoIP and video streaming will receive priority
- Home Worker - VPN and browsing will receive priority
- Gamer - Game-related traffic will receive priority
- Priority By Host - This entry provides the option to configure which computer in your LAN will receive the highest priority and which the lowest. If you have additional computers, they will receive medium priority.

  High Priority Host: Enter the host name or IP address of the computer to which you would like to grant the highest bandwidth priority.

  Low Priority Host: Enter the host name or IP address of the computer to which you would like to grant the lowest bandwidth priority.


General
WAN Devices Bandwidth (Rx/Tx):
User Defined
Rx Bandwidth:
0
Kbits/s
Tx Bandwidth:
0
Kbits/s
QoS Profiles
Default
No Quality of Service preferences
P2P User
"I use peer-to-peer and file-sharing applications. I still want to be able to use my browser without interference."
HTTP/HTTPS: Medium
Other: Low
Triple Play User
"I use VoIP applications and video streaming. I want these applications to be as fast as possible."
VoIP (SIP, H323): High
Video: High-Medium
HTTP/HTTPS: Medium
Other: Low
Home Worker
"I work from home, and want my VPN and browser to have priority over other traffic."
VPN (IPsec, L2TP, PPTP): Medium
HTTP/HTTPS: Medium
Other: Low
Gamer
"I play games over the Internet and want the games-related traffic to be as fast as possible."
Games Related Traffic: Medium
Other: Low
Priority By Host
"I want to give different hosts in my network different priorities when accessing the public network."
High Priority Host:
Low Priority Host:
Other:
Low
Note: Choosing a new QoS profile will cause all previous configuration settings to be lost
OK
Apply
Cancel

15.7.2 Traffic Priority

If you click the **Quality of Service** link in the **Advanced** screen and then click **Traffic Priority** in the left submenu, the following screen appears. This screen allows you to configure QoS to prioritize input and output traffic.

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:

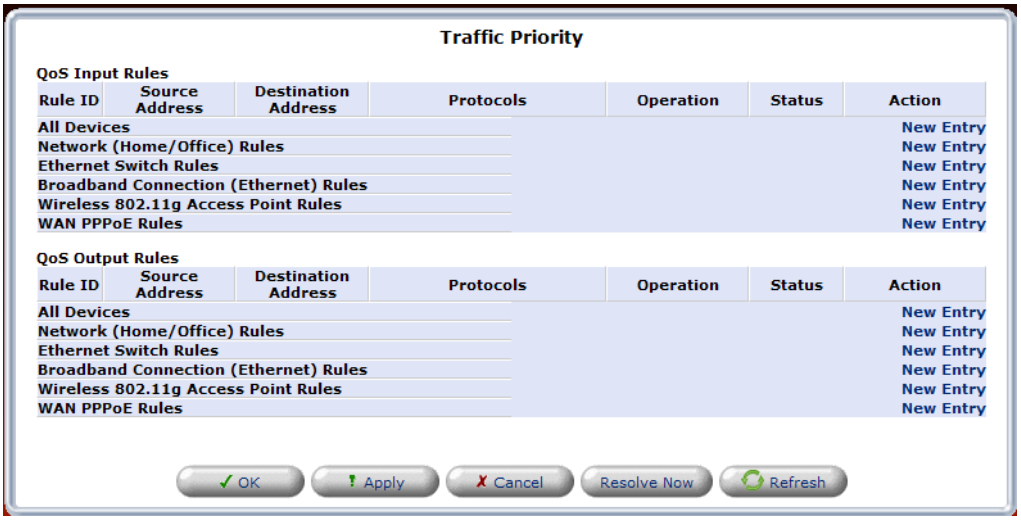
- DSCP
- 802.1p Priority

The matching of packets by rules, also known as Stateful Packet Inspection is connection-based and uses 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.

A packet can match more than one rule. Therefore:

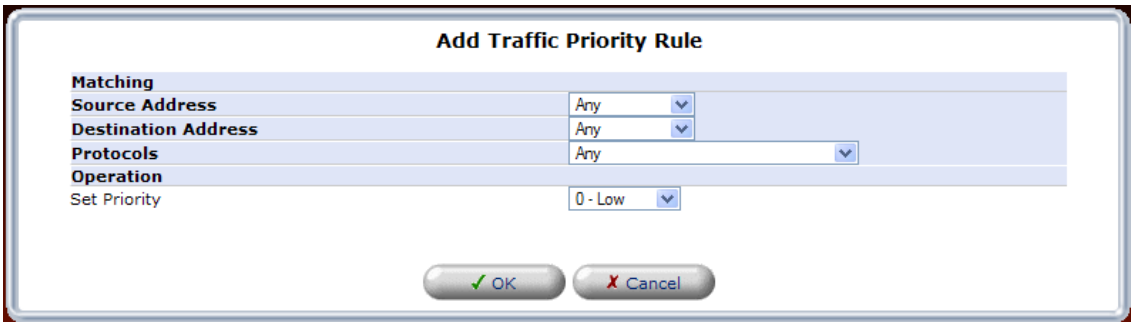
- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule.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

To set up a traffic priority rule, click the adjacent **New Entry** link for the input/output device you want to configure.



If you clicked **New Entry,** the following screen appears. At this screen, do the following:

1. Select the desired **Source Address, Destination Address, and Protocol** options from the drop-down lists.
2. Click the **Device** check box if you will apply the settings to a device. By default this box is cleared.
3. Select the desired option from the **Set Priority** drop-down list. (Zero is the lowest priority level.)
4. Click **OK** to save the settings.



Source Address—The source address of packets sent or received from the LAN computer. The drop-down list displays all the host names or IP addresses of currently connected LAN computers, as well as the options 'Any' and 'User Defined'. Select an address from the list, or select **Any** to apply the rule on all computers. If you would like add a new address, select the **User Defined** option in the drop-down list. This will commence a sequence that will add a new network object, representing the LAN computer. The network object may be an IP address, subnet or range, a MAC address or a host name.

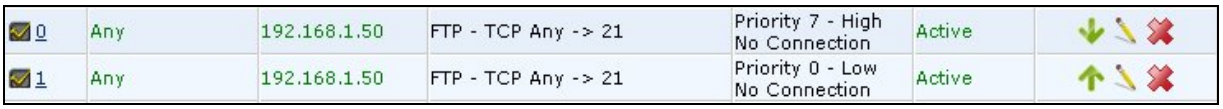
Destination Address—The destination address of packets sent or received from the network object. This address can be configured in the same manner as the source address. This entry enables further filtration of the packets.

Protocols—You may also specify a traffic protocol. Selecting the **Show All Services** option in the drop-down list will expand the list of available protocols. Select a protocol or add a new one using the **User Defined** option. This will commence a sequence that will add a new service, representing the protocol.

Operation—Set rule priority with Quality of Service:

Set Priority—Check this check-box to add a priority to the rule then select 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.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the Move Up and Move Down action icons as shown in the following image.



0	Any	192.168.1.50	FTP - TCP Any -> 21	Priority 7 - High No Connection	Active	
1	Any	192.168.1.50	FTP - TCP Any -> 21	Priority 0 - Low No Connection	Active	

15.7.3 Traffic Shaping

If you click the **Quality of Service** link in the **Advanced** screen and then click **Traffic Shaping** in the left submenu, the following screen appears.

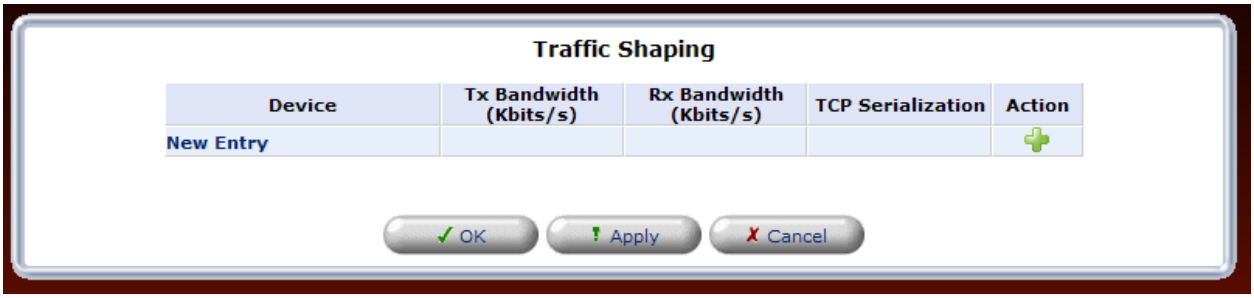
Traffic Shaping is the solution for managing and avoiding congestion where the network meets limited broadband bandwidth. Typical networks use a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. This is where most bottlenecks occur. A traffic shaper is essentially a regulated queue that accepts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

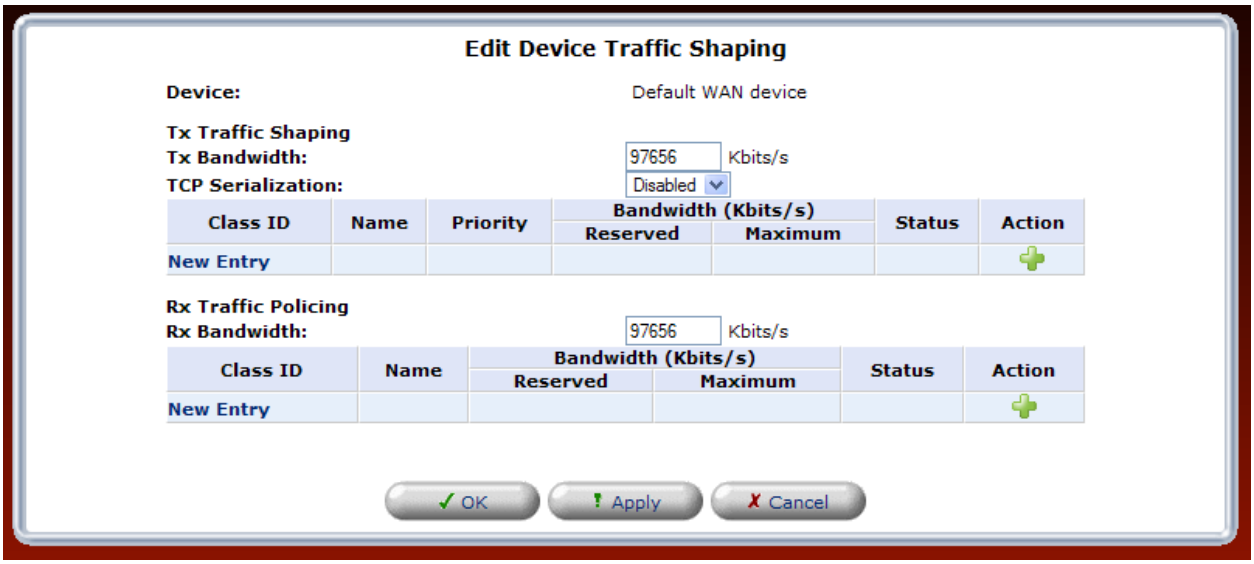
The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the Router's firewall mechanism. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. Connection-based QoS also allows 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 application-level gateway (ALG) in the firewall.

To add a traffic shaping rule, click the **New Entry** link.



If you clicked **New Entry**, the following screen appears. Select a device from the **Device** drop-down list. Then, click **OK** to continue.

After you have selected a device and clicked **OK** in the preceding screen, the following screen appears. Enter the bandwidth values for transmit (Tx) and receive (Rx), and then select the desired option from the TCP Serialization drop-down list. Next, click the desired **New Entry** link to add a class.



Tx Traffic Shaping

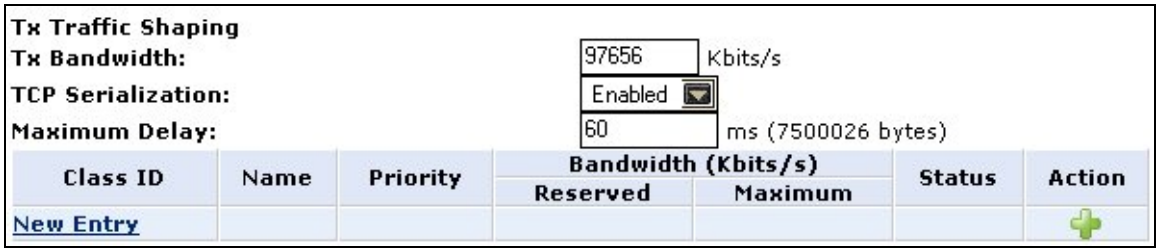
The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Shaping Class. When not used by its predefined traffic type, or owner (for example VoIP), the class will be available to all other traffic. However when needed, the entire class is reserved solely for its owner. Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. Configure the following fields:

Tx Bandwidth

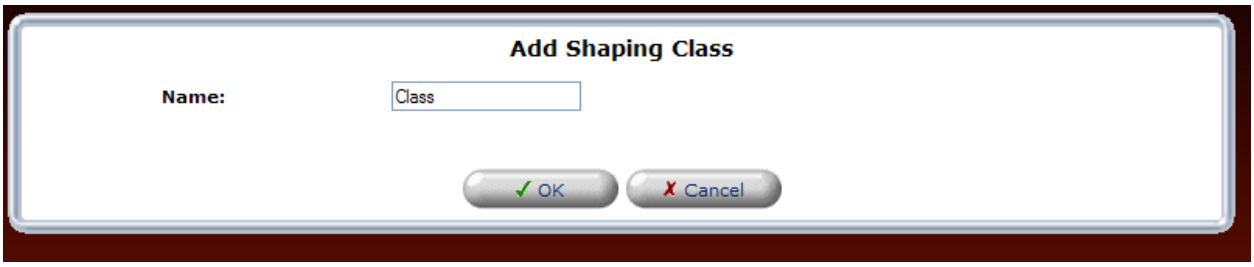
This parameter limits the gateway's bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces the router to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device's bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering this router’s QoS useless.

TCP Serialization

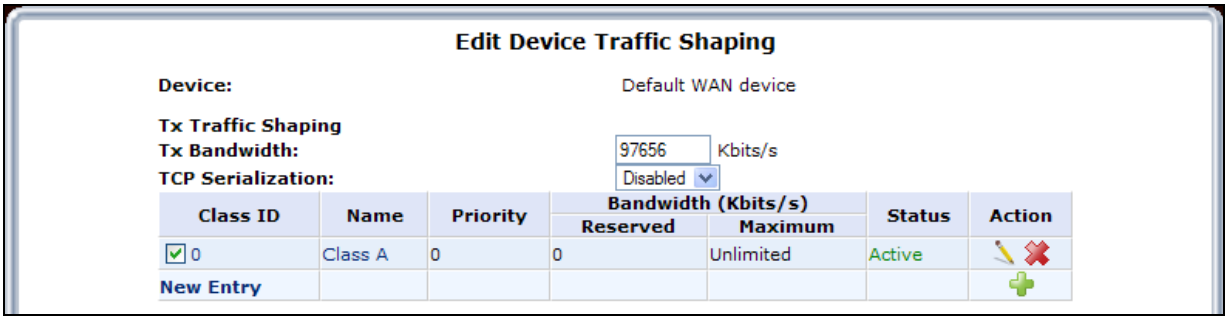
You can enable TCP Serialization in its combo box, either for active voice calls only or for all traffic. The screen will refresh, adding a 'Maximum Delay' field. This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted, will be fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes will be automatically updated on refresh.



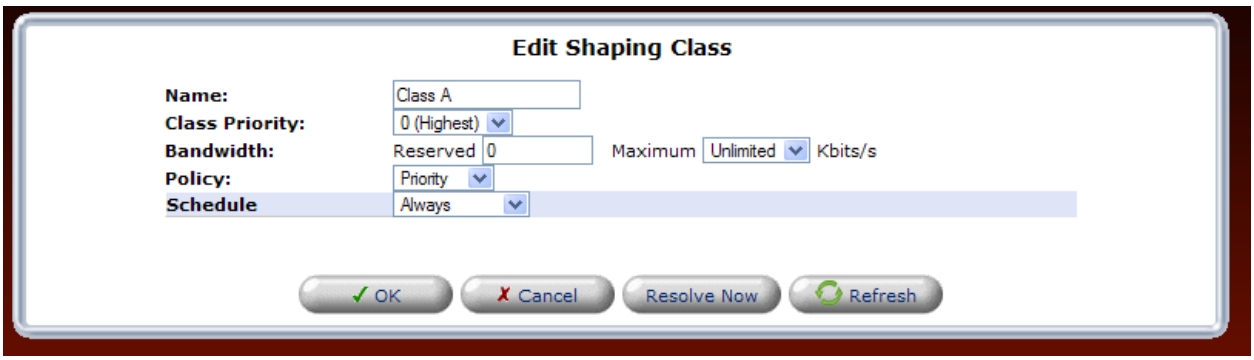
For example, if you click the New Entry link in the **Tx Traffic Shaping** section of the **Edit Device Traffic Shaping** screen the **Add Shaping Class** screen will appear.



Name the new class and click **OK** to save the settings, e.g., Class A. Now click the class name to edit the shaping class or alternatively, click its pencil (edit) icon in the Action column.



If you clicked the edit icon in the preceding screen, the **Edit Shaping Class** screen will appear.



Configure the following fields by entering or selecting the desired values:

Name—The name of the class.

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

Bandwidth—The reserved transmission bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting **Specify** in the drop-down list. The screen will refresh, adding yet another Kbits/s.

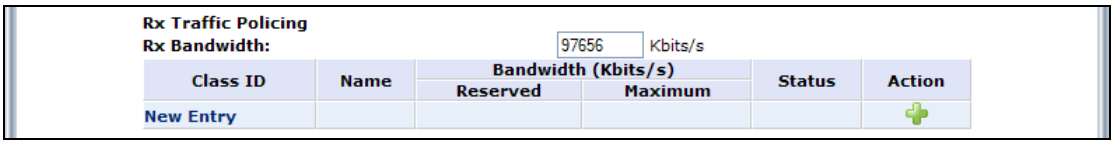
Policy—The class policy determines the policy of routing packets inside the class. Select one of the four options:

> 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 a 802.1p value.
>
> FIFO—The “First In, First Out” priority queue. This queue ignores any previously-marked priority that packets may have.
>
> Fairness—The fairness algorithm ensures no starvation by granting all packets a certain level of priority.
>
> RED— The 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 that would be lost when a queue overflows and a host is transmitting at a high rate.

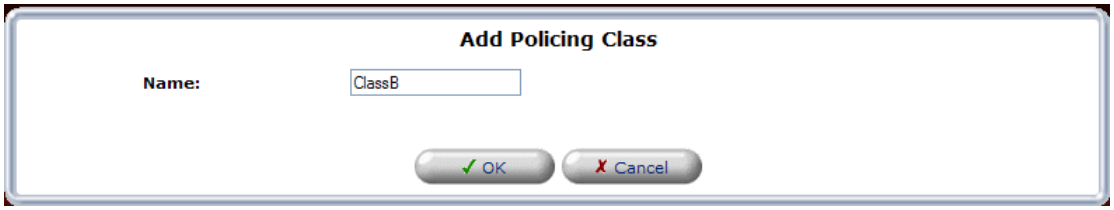
Schedule—By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. Refer to section 15.21, “Scheduler Rule,” for details on setting up schedule rules.

Rx Traffic Policing: Allows you to configure the following fields:

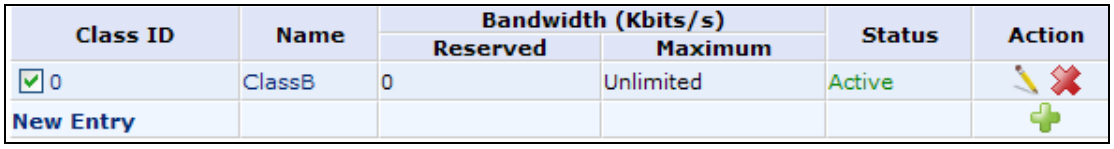
Rx Bandwidth This parameter specifies the maximum traffic the policing can receive from the ISP.



For example, if you click the **New Entry** link in the **Rx Traffic Policing** section of the **Edit Device Traffic Shaping** screen, the **Add Policing Class** screen will appear.

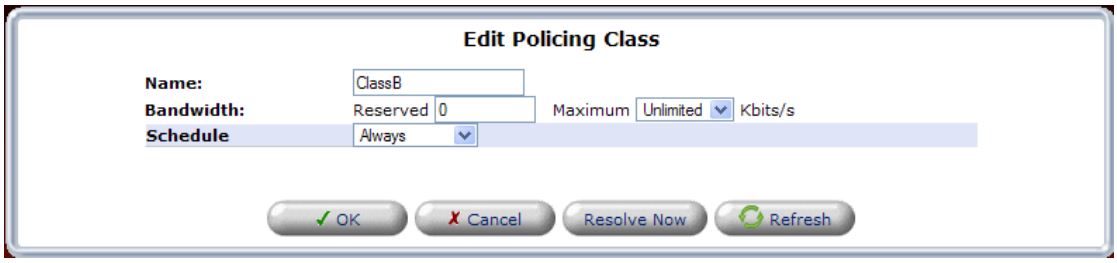


Name the new class and click **OK** to save the settings, e.g. Class B. Next, click the class name to edit the shaping class or alternatively, click its pencil (edit) action icon in the Action column.



Class ID	Name	Bandwidth (Kbits/s)		Status	Action
		Reserved	Maximum		
0	ClassB	0	Unlimited	Active	
New Entry					

The **Edit Policing Class** screen will appear.



Configure the following fields:

Name—The name of the class.
Bandwidth—The reserved reception bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the combo box. The screen will refresh, adding yet another Kbits/s field.
Schedule—By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. Refer to section 15.21, “Scheduler Rules,” for details on setting up schedule rules.

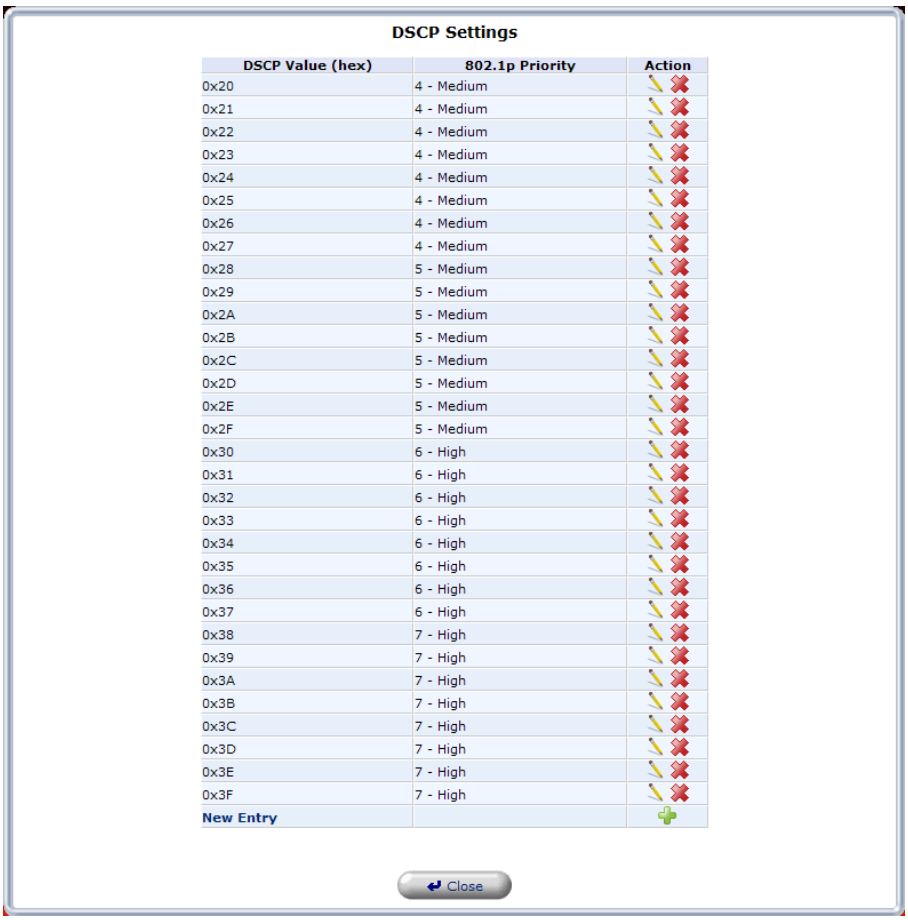
15.7.4 Differentiated Service Code Point (DSCP) Settings

If you click the **Quality of Service** link in the **Advanced** screen and then click **DSCP Settings** in the left submenu, the following screen appears.

Familiarity with the Differentiated Services model is essential to understanding DSCP. 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 a particular queue handling or scheduling behavior to packets.

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. To add a new DSCP value, press the **New Entry** link at the bottom of this screen.

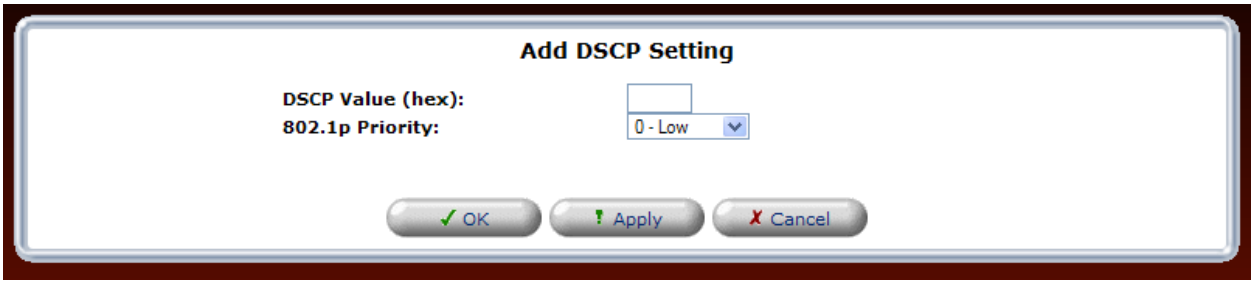


DSCP Settings

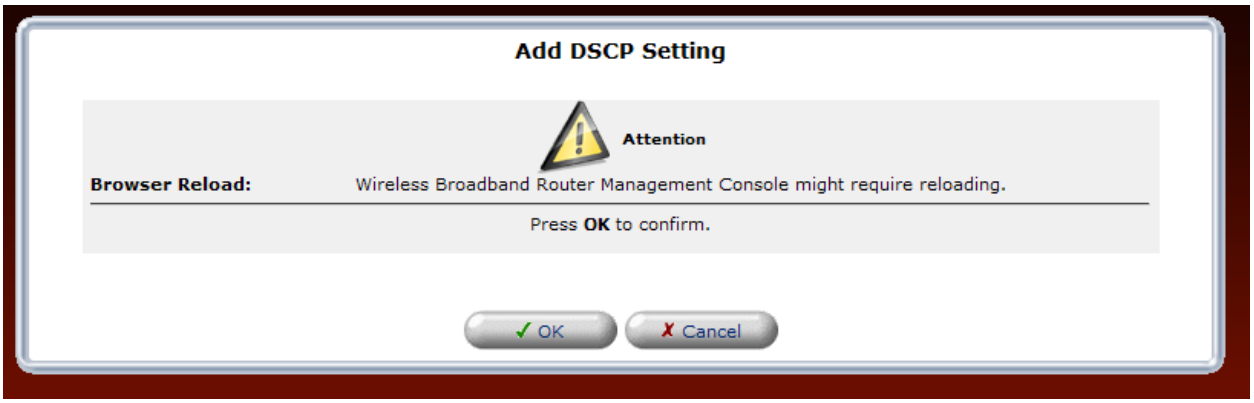
DSCP Value (hex)	802.1p Priority	Action
0x20	4 - Medium	
0x21	4 - Medium	
0x22	4 - Medium	
0x23	4 - Medium	
0x24	4 - Medium	
0x25	4 - Medium	
0x26	4 - Medium	
0x27	4 - Medium	
0x28	5 - Medium	
0x29	5 - Medium	
0x2A	5 - Medium	
0x2B	5 - Medium	
0x2C	5 - Medium	
0x2D	5 - Medium	
0x2E	5 - Medium	
0x2F	5 - Medium	
0x30	6 - High	
0x31	6 - High	
0x32	6 - High	
0x33	6 - High	
0x34	6 - High	
0x35	6 - High	
0x36	6 - High	
0x37	6 - High	
0x38	7 - High	
0x39	7 - High	
0x3A	7 - High	
0x3B	7 - High	
0x3C	7 - High	
0x3D	7 - High	
0x3E	7 - High	
0x3F	7 - High	
New Entry		

Close

If you clicked **New Entry**, the following screen appears. Enter your hexadecimal value, and then set the priority for this value. Click **Apply** to continue.



If you clicked **Apply**, the following screen appears. Click **OK** to confirm. Value will be added to the **DSCP Settings** screen.



15.7.5 802.1P Settings

If you click the **Quality of Service** link in the **Advanced** screen and then click **802.1P Settings** in the left submenu, the following screen appears.

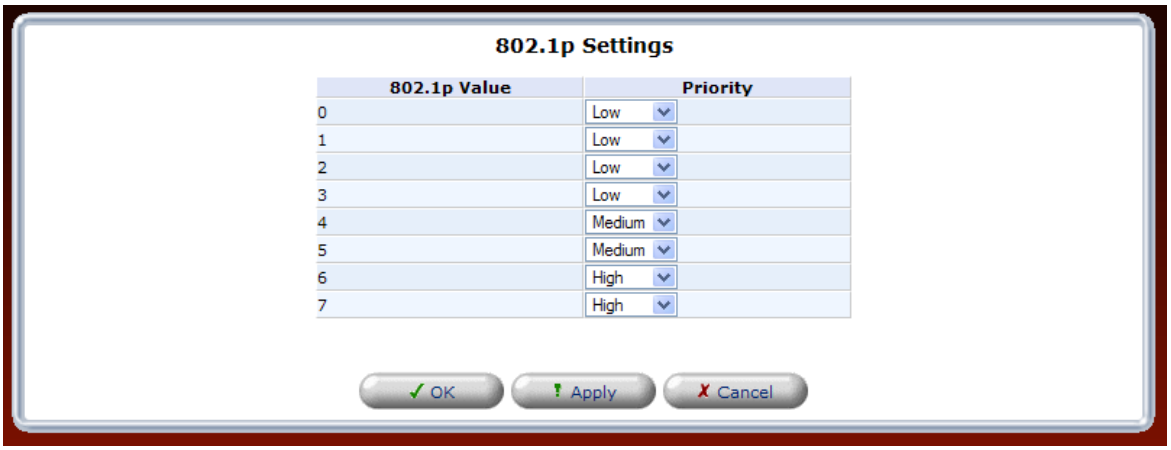
The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

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 might be assigned to network-critical traffic. Values five and six may 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 is 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 the following:

- 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.

Select the desired values from the drop-down lists, and then click **Apply** to save the settings.



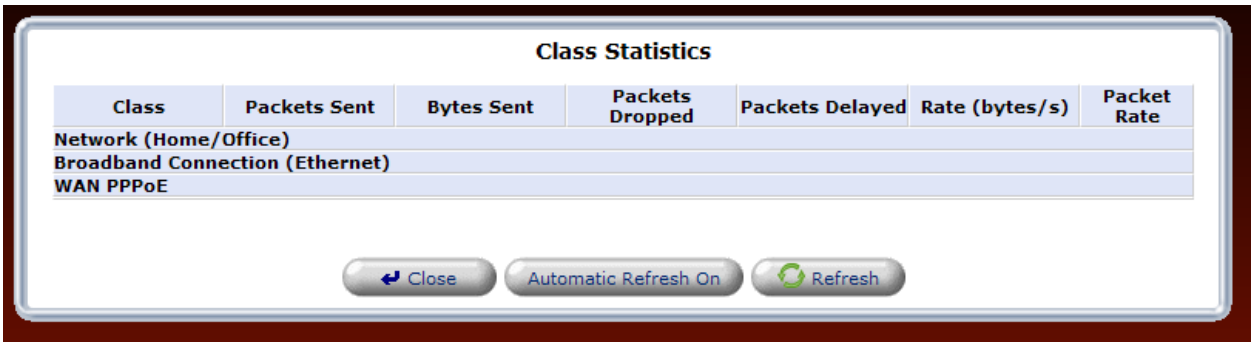
15.7.6 Class Statistics

If you click the **Quality of Service** link in the **Advanced** screen and then click **Class Statistics** in the left submenu, the following screen appears.

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.

NOTE: Class statistics will be available only after defining at least one class (otherwise the screen will not display any values).

If you do not want the screen to refresh automatically, click **Automatic Refresh Off.**



15.8 Remote Administration

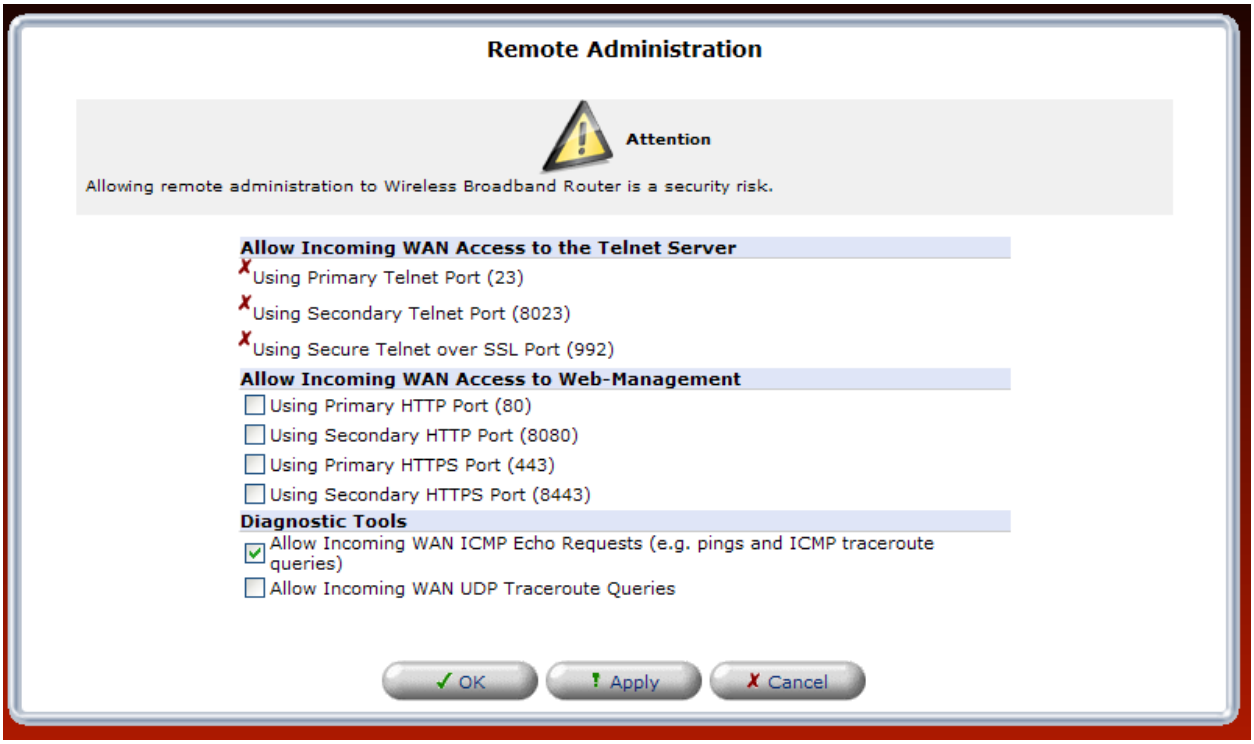
If you click **Advanced** in the top navigation menu and then select the **Remote Administration** link, the following screen appears.

It is possible to access and control your Router not only from within the home network, but also from the Internet. This allows you to view or change settings while traveling. It also enables you to allow Verizon to change settings or help you troubleshoot functionality or communication issues from a remote location. Remote access to your Router is blocked by default to ensure the security of your network. However, your Router supports the following services, and you may use the Remote Administration Security screen to selectively enable these services if they are needed.

WARNING: With Remote Administration enabled, your network will be at risk from outside attacks.

To configure Remote Administration, enter the appropriate settings, and then click **Apply** to save the settings.

NOTE: This Router ships with Telnet disabled.



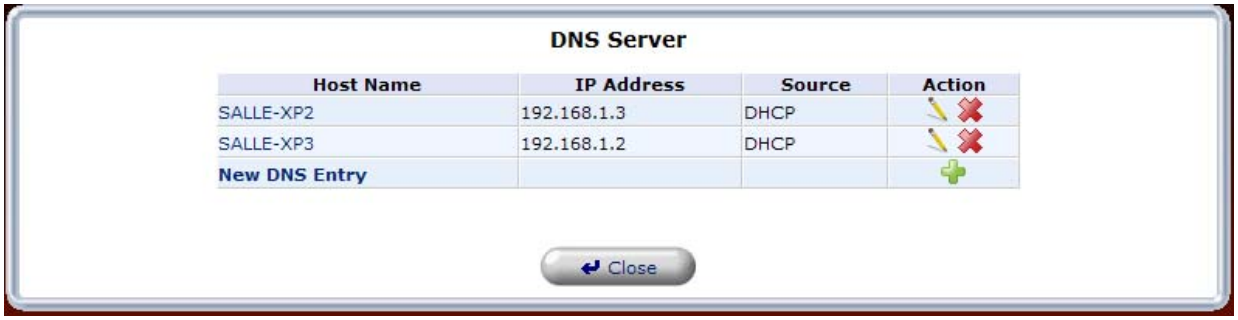
15.9 DNS

If you click **Advanced** in the top navigation menu and then select the **DNS** link, the following screen appears.

The Router contains a built-in DNS server. When an IP address is assigned, the Router will interrogate the new device for a machine name using several well-known networking protocols. Any names learned will dynamically be added to the DNS server's table of local hosts.

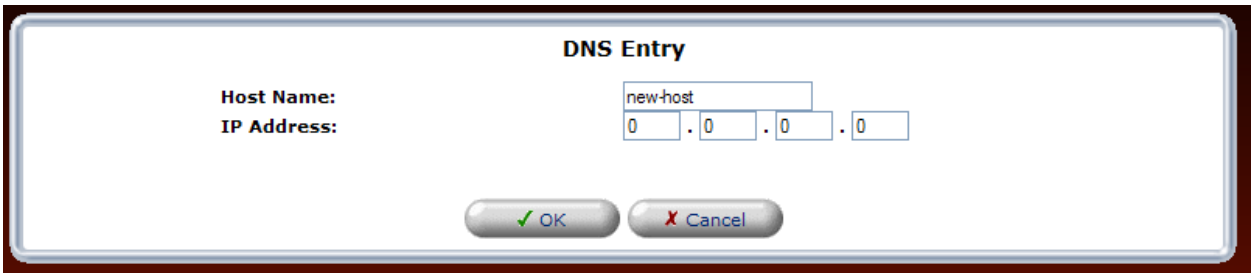
You can do any of the following:

- To rename the domain name, click a host name link.
- To add a host name, click the **New DNS Entry** link.

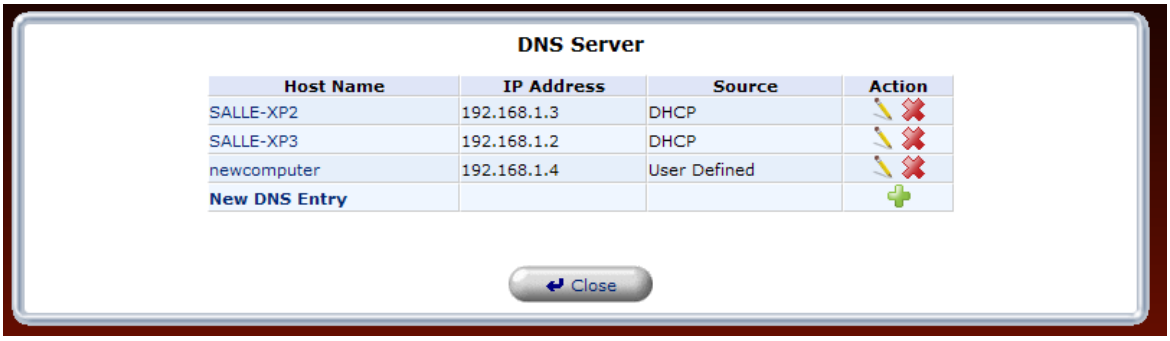


To add a new entry, click the **New DNS Entry** link. The following screen appears. Enter the desired host name, and then enter the appropriate IP address. Next, click **OK** to continue.

NOTE: Names may not contain spaces. Only letters, digits and the special characters dash (-), underscore (_) and dot (.) may be used. These special characters may not appear at the beginning or at the end of a name. The maximum length of a name can be is 63 characters.



If you have entered values in the preceding screen and clicked **OK**, the following screen appears. The changes have been saved to the Router.



15.10 Personal Domain (Dynamic DNS)

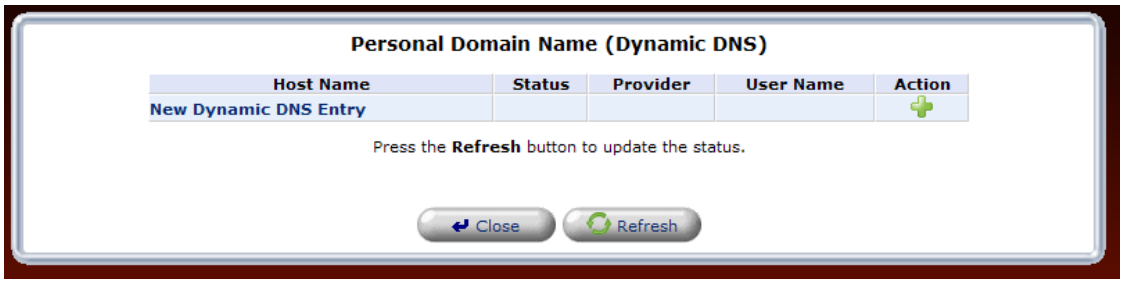
If you click **Advanced** in the top navigation menu and then select the **Personal Domain Name** link, the following screen appears.

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 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 service provider changes, the DNS database changes accordingly to reflect the change. If the IP address of the computer changes often, its domain name remains constant and accessible.

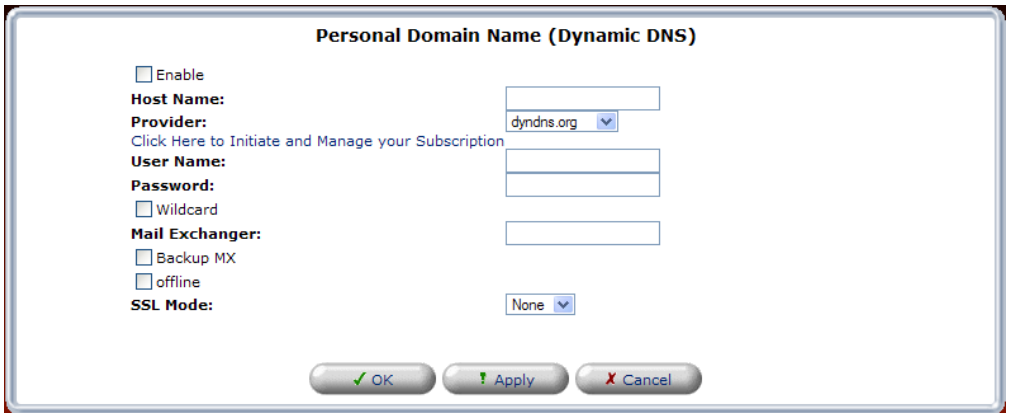
NOTE: To use Dynamic DNS, you must subscribe to this service via your service provider.

To configure a new dynamic DNS entry, click the **New Dynamic DNS Entry** link.



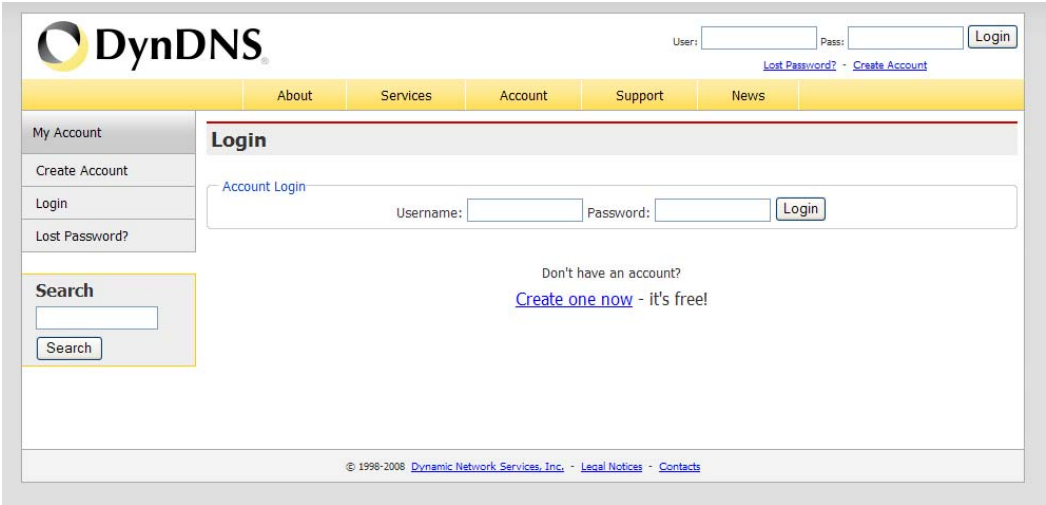
The following screen appears. Enter the appropriate values in the fields provided, and then click **OK** to continue.

NOTE: Your service provider will provide you with the appropriate values to use in this screen.



If you click the **Click Here to Initiate and Manage your Subscription** link, the following screen appears. Enter the user name and password (provided by your service provider) in the fields provided to access your account.

NOTE: The screen displayed in this document may differ from the actual screen.



15.11 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to one or more MAC address, IP address, and host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring the Router's security filtering settings such as IP address filtering, host name filtering or MAC address filtering. You can use network objects 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.

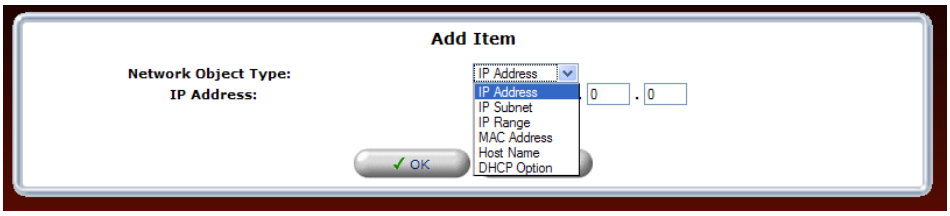
If you click **Advanced** in the top navigation menu and then select the **Network Objects** link, the following screen appears. To configure a new network object, click the **New Entry** link.

If you clicked **New Entry** in the preceding screen, the following screen appears. Enter a name for the network object in the **Network Object Description** field, and then click the **New Entry** link or the plus icon to create it.

If you clicked **New Entry**, the following screen appears. The source address can be entered using one of the following methods listed in the **IP Address** drop-down menu:

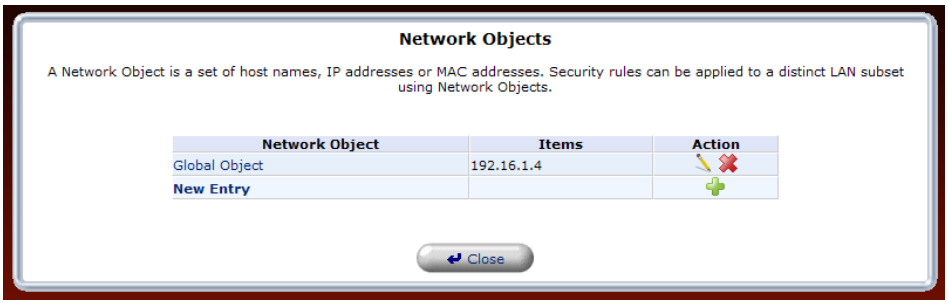
- IP Address
- IP Subnet
- IP Range
- MAC Address
- Host Name
- DHCP Option

After you select the desired method, the screen will refresh. Enter the appropriate values in the fields provided, and then click **OK** to save the settings.



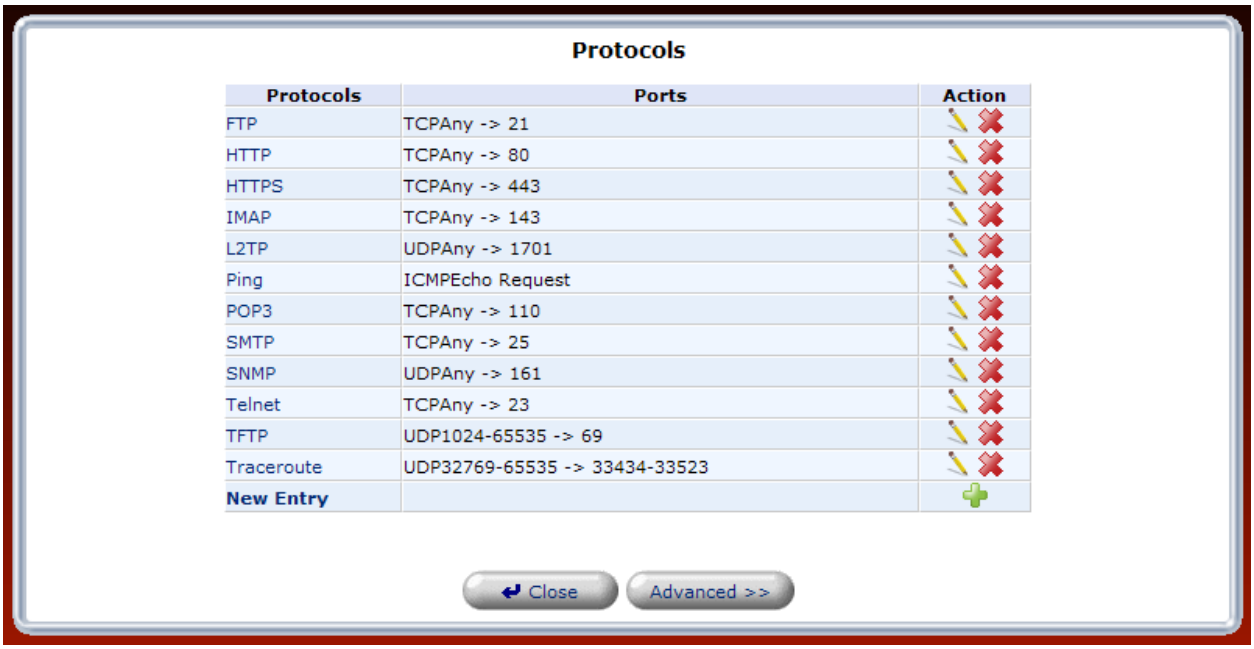
If you have entered the desired values in the preceding screen and clicked **OK**, the following screen appears. The network object has been configured. Click **OK** to save the configuration.

If you clicked **OK**, the following screen appears. The network object has been saved to the Router. Click **Close** to return to the **Advanced** screen.



15.12 Protocol

If you click **Advanced** in the top navigation menu and then select the **Protocol** link, the following screen appears. For your convenience, the Router supports protocols for Applications, Games, and VPN-specific programs. The following chart provides port/protocol information for the supported services. The Protocol screen allows you to select the desired view: Basic Service and Advanced Service. The following sections explain the features of each service.



Protocols

Protocols	Ports	Action
FTP	TCPAny -> 21	
HTTP	TCPAny -> 80	
HTTPS	TCPAny -> 443	
IMAP	TCPAny -> 143	
L2TP	UDPAny -> 1701	
Ping	ICMPEcho Request	
POP3	TCPAny -> 110	
SMTP	TCPAny -> 25	
SNMP	UDPAny -> 161	
Telnet	TCPAny -> 23	
TFTP	UDP1024-65535 -> 69	
Traceroute	UDP32769-65535 -> 33434-33523	
New Entry		

Close Advanced >>

15.12.1 Basic Service

To access the basic service **Protocols** screen (if you are in the **Advanced** screen), click the **Basic** button.

Protocols

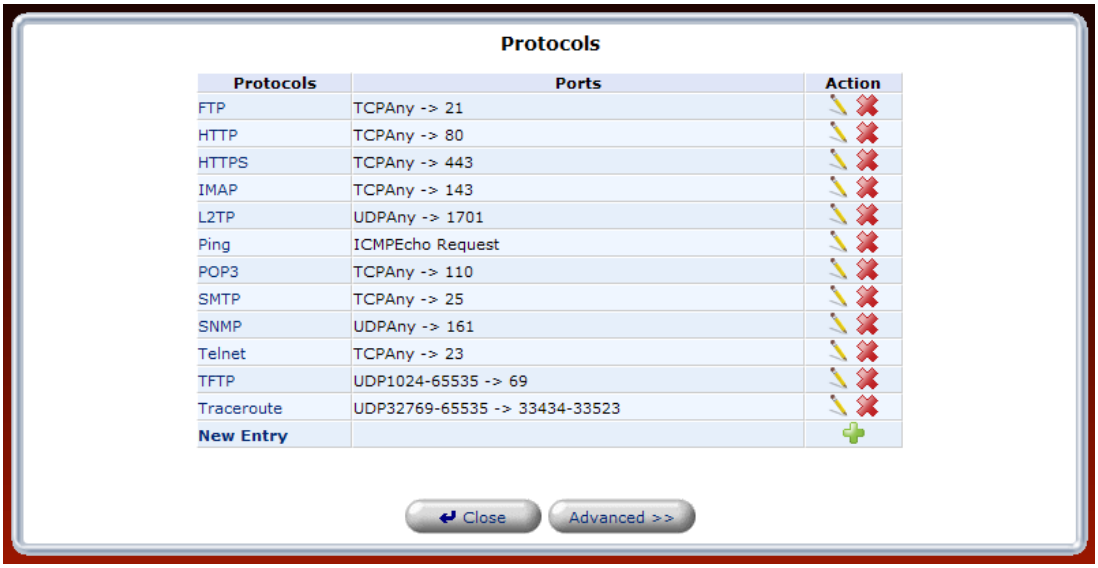
Protocols	Ports	Action
Alien vs. Predator	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80	
CuSeeMe	TCPAny -> 1503 Any -> 7640 Any -> 7642 Any -> 7648-7649 UDPAny -> 24032 Any -> 1414 Any -> 1424 Any -> 1812-1813 Any -> 7648 Any -> 56800	
Dark Reign	UDPAny -> 21154-21157	
Dark Reign 2	TCPAny -> 26214 UDPAny -> 26214	
Decent 3	TCPAny -> 7170 UDPAny -> 2092 Any -> 3445	
Decent Freespace	TCPAny -> 3999 UDPAny -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	
DHCP ALG	UDP67-68 -> 67	
Diablo, StarCraft(Battle.net)	TCPAny -> 6112 Any -> 116-118 UDPAny -> 6112	
DirectX Games	TCPAny -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912 UDPAny -> 47624-47625 Any -> 2300-2400	
DNS ALG	UDPAny -> 53	
FTP	TCPAny -> 21	
H.323 Call Signaling	TCPAny -> 1720 Any -> 1503	
Heat.net	TCPAny -> 8000-8999 UDPAny -> 1398 Any -> 5500-5600 Any -> 8000-9000	
HTTP	TCPAny -> 80	
HTTP Secondary	TCPAny -> 8080	
HTTP Web Access	TCPAny -> 3127-3128 Any -> 80-81 Any -> 8080 Any -> 8000 Any -> 8888	
HTTPS	TCPAny -> 443	
HTTPS Secondary	TCPAny -> 8443	
ICQ	UDPAny -> 4000	
IMAP	TCPAny -> 143	
IPSec	UDP500 -> 500 ESP AH	
L2TP	UDPAny -> 1701	
MGCP ALG	UDPAny -> 2727	
Microsoft Direct Play	UDPAny -> 1000-4999 Any -> 40000-60000	
Microsoft Windows Network / Samba	TCPAny -> 139 Any -> 445 UDPAny -> 137 Any -> 138	
MSN Messenger	TCPAny -> 1863	
Myth	TCPAny -> 3453	
Need for Speed 5 (Porsche)	UDPAny -> 9395-9405	
Ping	ICMPEcho Request	
Play-Station2	TCPAny -> 10070-10080 UDPAny -> 10070	
POP3	TCPAny -> 110	
PPTP	TCPAny -> 1723 GRE	
QuakeII	TCPAny -> 27910 UDPAny -> 27910	
QuakeIII	TCPAny -> 27660-27670 UDPAny -> 27660-27670	
Rainbow Six	TCPAny -> 2346	
Red Alert	UDPAny -> 5009	
RTSP	TCPAny -> 554 Any -> 7070 Any -> 5005 UDPAny -> 554 Any -> 7070 Any -> 5005	
SIP	UDPAny -> 5060	
SMTP	TCPAny -> 25	
SNMP	UDPAny -> 161	
SSH	TCPAny -> 22	
Telnet	TCPAny -> 23	
TFTP	UDP1024-65535 -> 69	
Tiberian Sun	TCPAny -> 4000 Any -> 1140-1234 UDPAny -> 1140-1234	
Total Annihilation	TCPAny -> 1000-4999 UDPAny -> 47624 Any -> 1000-4999	
Traceroute	UDP32769-65535 -> 33434-33523	
Unreal - Master Server List	UDPAny -> 27900	
Unreal, Unreal Tournament	UDPAny -> 7777-7779 Any -> 27900	
Vonage VoIP Phone Service	TCPAny -> 5060-5070 Any -> 10000-25000	
Worms 2	TCPAny -> 1031-2210 Any -> 2220-3212 UDPAny -> 1000-1029	
XBoX	TCPAny -> 3074 UDPAny -> 88 Any -> 3074	
New Entry		

Close Basic <<

If you clicked the **Basic** button in the preceding screen, the following screen appears.

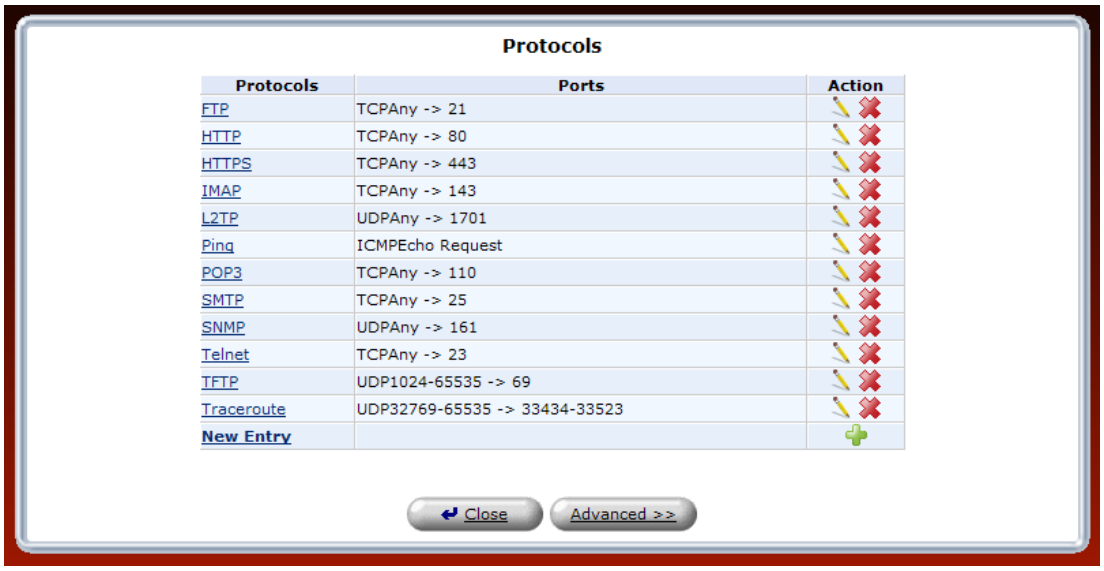
At this screen, you can:

- Configure ports for predefined protocols by clicking the desired link.
- Configure a new user-defined port for a protocol by clicking the **New Entry** link.



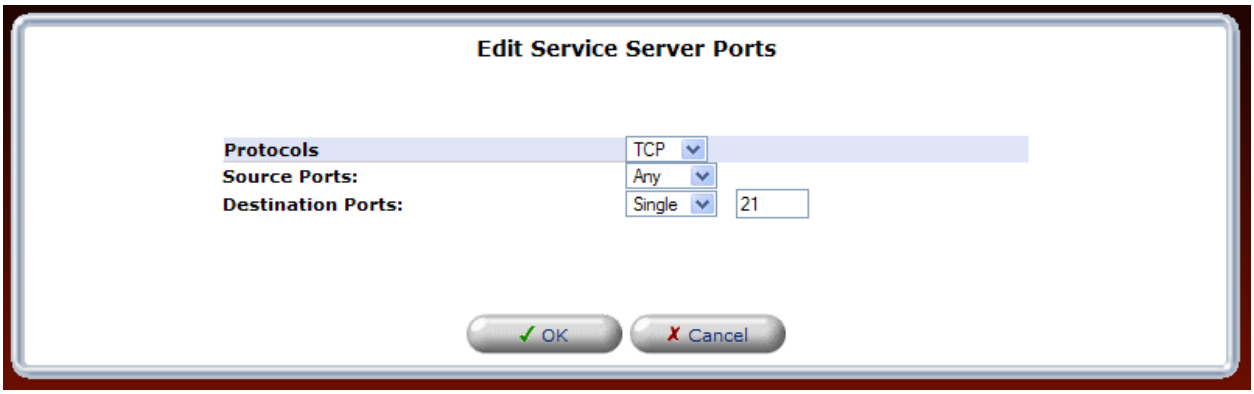
15.12.1.1 Configuring a Predefined Protocol Service

To configure the Router for a predefined protocol service, click the desired protocol link.

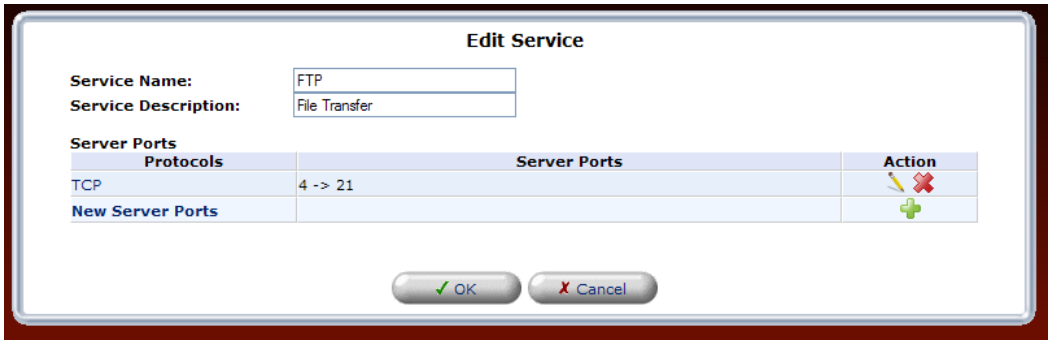


For example, if you clicked **FTP** in the preceding screen, the following screen appears. Next, click the **TCP** link to configure the service protocol values.

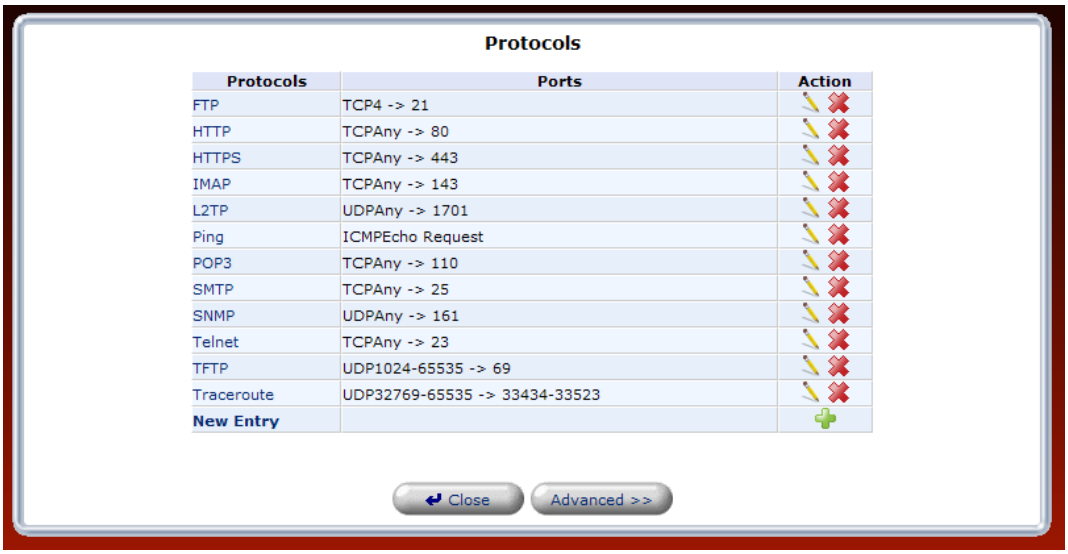
If you clicked **TCP** in the **Edit Service** screen, the following screen appears. Enter the desired values, and then click **OK** to continue.



If you have entered values and clicked **OK** in the preceding screen, the following screen appears. A protocol service has been configured. Click **OK** to save the settings.

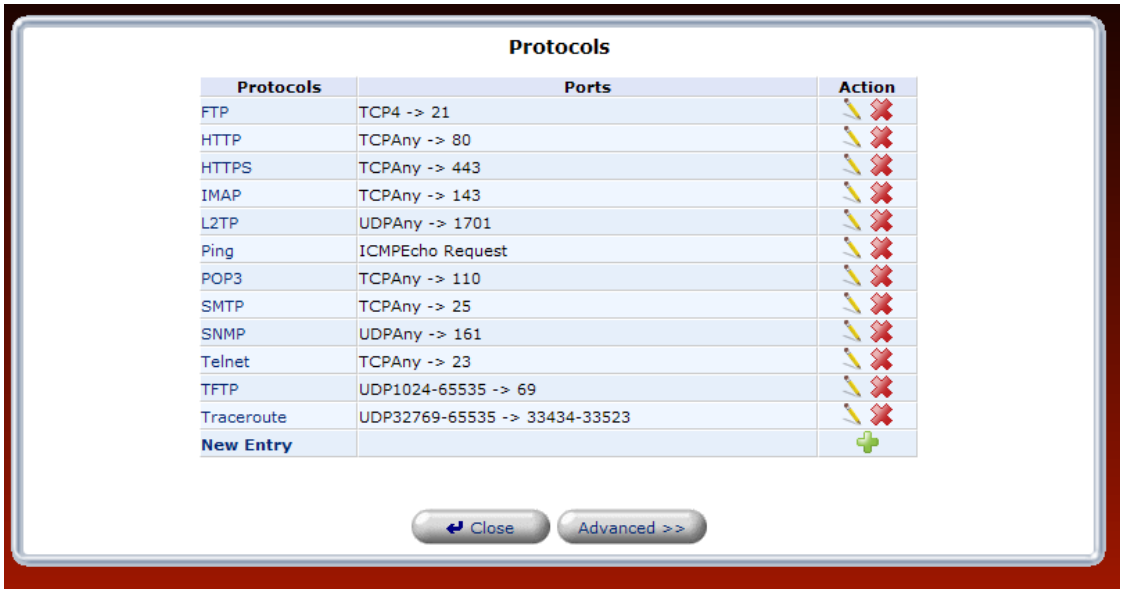


If you clicked **OK** in the preceding screen, the following screen appears. The protocol service has been saved to the Router.

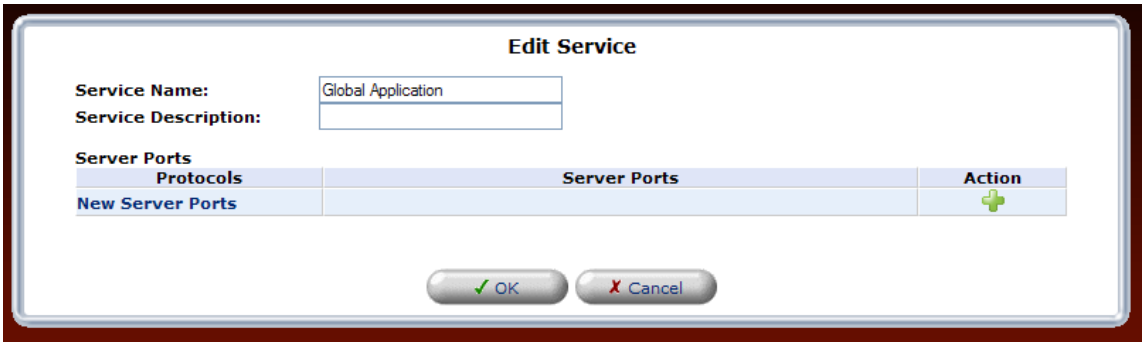


15.12.1.2 Configuring a User-defined Protocol Service

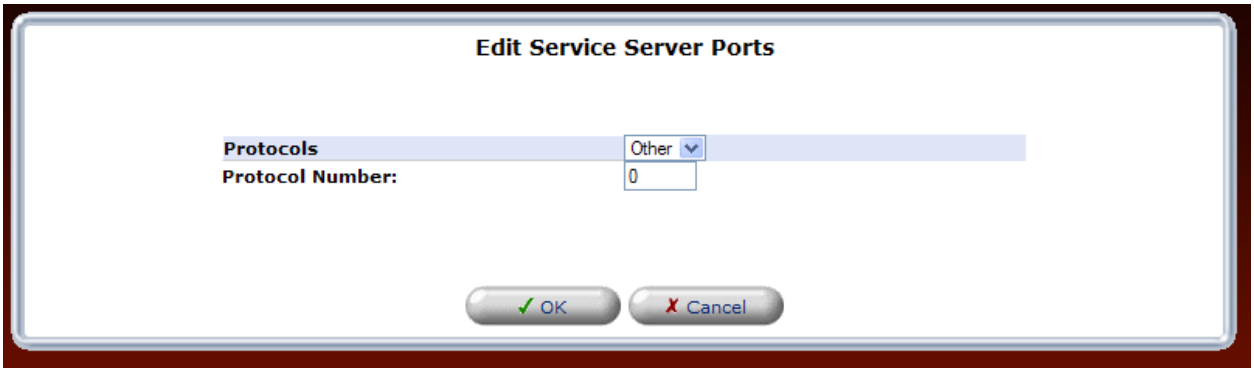
To configure the Router for a user-defined protocol service, click the **New Entry** link.



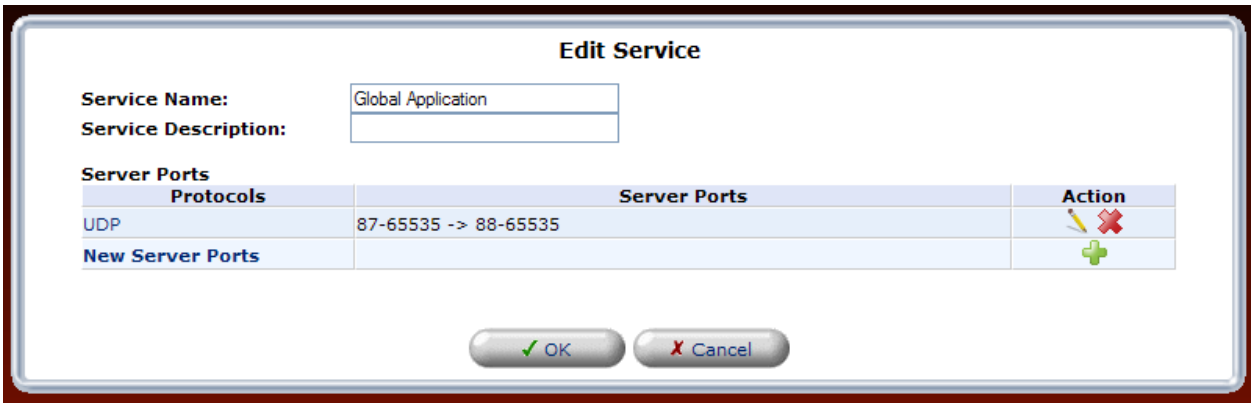
If you clicked **New Entry,** the following screen appears. Enter a service name and service description in the fields provided. Next, click the **New Server Ports** link.



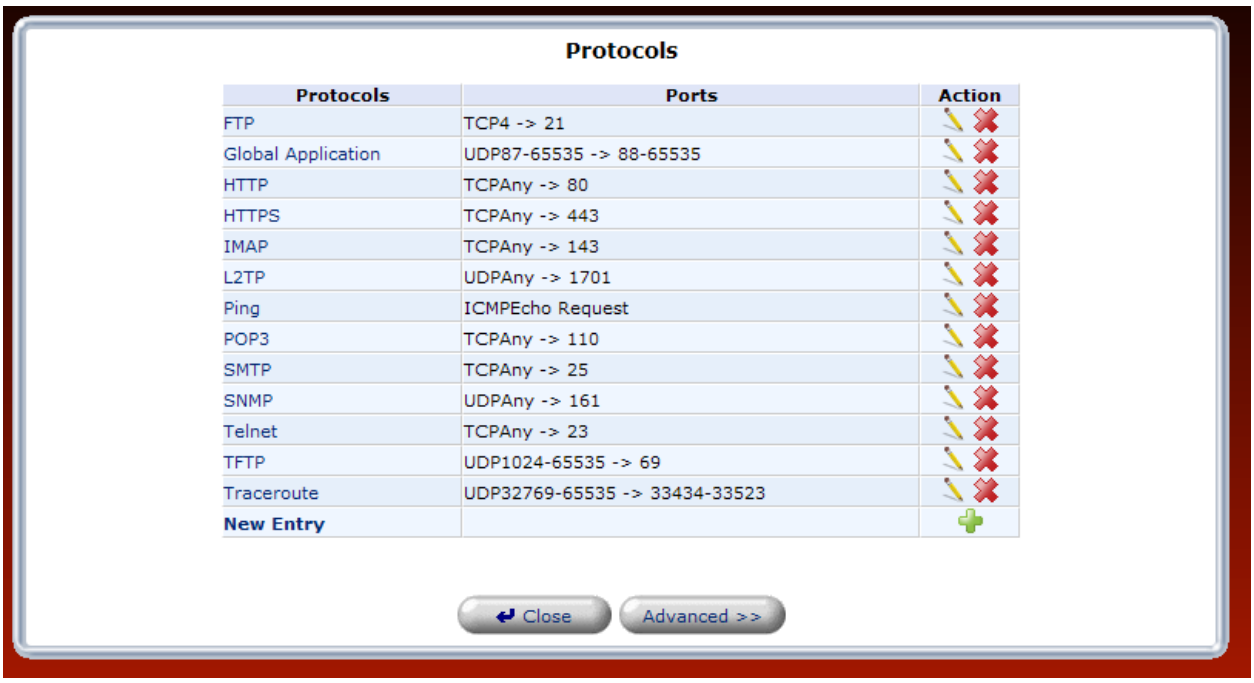
If you clicked **New Server Ports,** the following screen appears. Select a protocol from the drop-down list, and then enter a protocol number. Click **OK** to continue.



If you clicked **OK**, the following screen appears. Click **OK** to save the settings.



If you clicked **OK**, the following screen appears. The protocol settings have been saved to the Router.



15.12.2 Advanced Protocol Service

To access the advanced service **Protocols** screen (if you are in the Basic screen), click the **Advanced** button. The following advanced **Protocols** screen will appear.

At the Advanced screen, you can:

- Configure predefined application by clicking the desired link.
- Configure a new user-defined application by clicking the **New Entry** link.

15.12.2.1 Configuring a Predefined Application

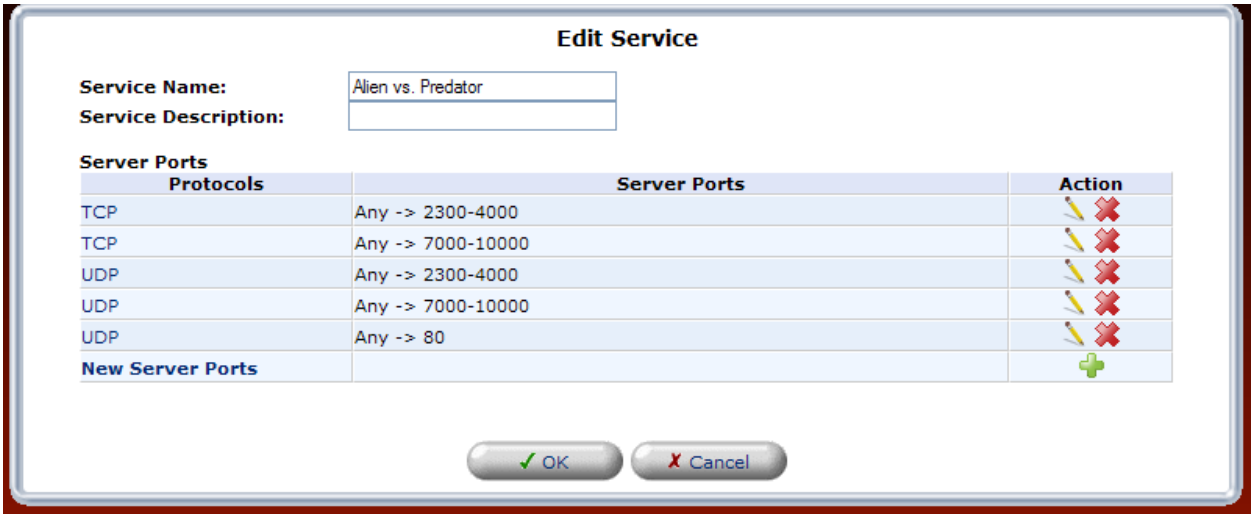
To configure the Router for a predefined application, click the desired link.

Protocols

Protocols	Ports	Action
Alien vs. Predator	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80	
CuSeeMe	TCPAny -> 1503 Any -> 7640 Any -> 7642 Any -> 7648-7649 UDPAny -> 24032 Any -> 1414 Any -> 1424 Any -> 1812-1813 Any -> 7648 Any -> 56800	
Dark Reign	UDPAny -> 21154-21157	
Dark Reign 2	TCPAny -> 26214 UDPAny -> 26214	
Decent 3	TCPAny -> 7170 UDPAny -> 2092 Any -> 3445	
Decent Freespace	TCPAny -> 3999 UDPAny -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	
DHCP ALG	UDP67-68 -> 67	
Diablo, StarCraft(Battle.net)	TCPAny -> 6112 Any -> 116-118 UDPAny -> 6112	
DirectX Games	TCPAny -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912 UDPAny -> 47624-47625 Any -> 2300-2400	
DNS ALG	UDPAny -> 53	
FTP	TCPAny -> 21	
H.323 Call Signaling	TCPAny -> 1720 Any -> 1503	
Heat.net	TCPAny -> 8000-8999 UDPAny -> 1398 Any -> 5500-5600 Any -> 8000-9000	
HTTP	TCPAny -> 80	
HTTP Secondary	TCPAny -> 8080	
HTTP Web Access	TCPAny -> 3127-3128 Any -> 80-81 Any -> 8080 Any -> 8000 Any -> 8888	
HTTPS	TCPAny -> 443	
HTTPS Secondary	TCPAny -> 8443	
ICQ	UDPAny -> 4000	
IMAP	TCPAny -> 143	
IPSec	UDP500 -> 500 ESP AH	
L2TP	UDPAny -> 1701	
MGCP ALG	UDPAny -> 2727	
Microsoft Direct Play	UDPAny -> 1000-4999 Any -> 40000-60000	
Microsoft Windows Network / Samba	TCPAny -> 139 Any -> 445 UDPAny -> 137 Any -> 138	
MSN Messenger	TCPAny -> 1863	
Myth	TCPAny -> 3453	
Need for Speed 5 (Porsche)	UDPAny -> 9395-9405	
Ping	ICMPEcho Request	
Play-Station2	TCPAny -> 10070-10080 UDPAny -> 10070	
POP3	TCPAny -> 110	
PPTP	TCPAny -> 1723 GRE	
QuakeII	TCPAny -> 27910 UDPAny -> 27910	
QuakeIII	TCPAny -> 27660-27670 UDPAny -> 27660-27670	
Rainbow Six	TCPAny -> 2346	
Red Alert	UDPAny -> 5009	
RTSP	TCPAny -> 554 Any -> 7070 Any -> 5005 UDPAny -> 554 Any -> 7070 Any -> 5005	
SIP	UDPAny -> 5060	
SMTP	TCPAny -> 25	
SNMP	UDPAny -> 161	
SSH	TCPAny -> 22	
Telnet	TCPAny -> 23	
TFTP	UDP1024-65535 -> 69	
Tiberian Sun	TCPAny -> 4000 Any -> 1140-1234 UDPAny -> 1140-1234	
Total Annihilation	TCPAny -> 1000-4999 UDPAny -> 47624 Any -> 1000-4999	
Traceroute	UDP32769-65535 -> 33434-33523	
Unreal - Master Server List	UDPAny -> 27900	
Unreal, Unreal Tournament	UDPAny -> 7777-7779 Any -> 27900	
Vonage VoIP Phone Service	TCPAny -> 5060-5070 Any -> 10000-25000	
Worms 2	TCPAny -> 1031-2210 Any -> 2220-3212 UDPAny -> 1000-1029	
XBoX	TCPAny -> 3074 UDPAny -> 88 Any -> 3074	
New Entry		

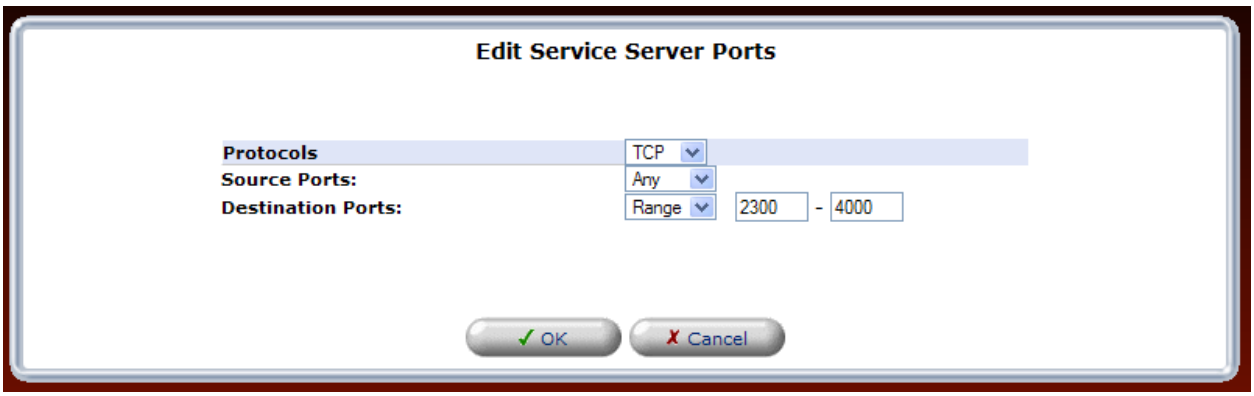
Close Apply

For example, if you clicked the link of a predefined service in the preceding screen, the following screen appears. If desired, enter a description in the **Service Description** field. Next, click the desired TCP or UDP link.

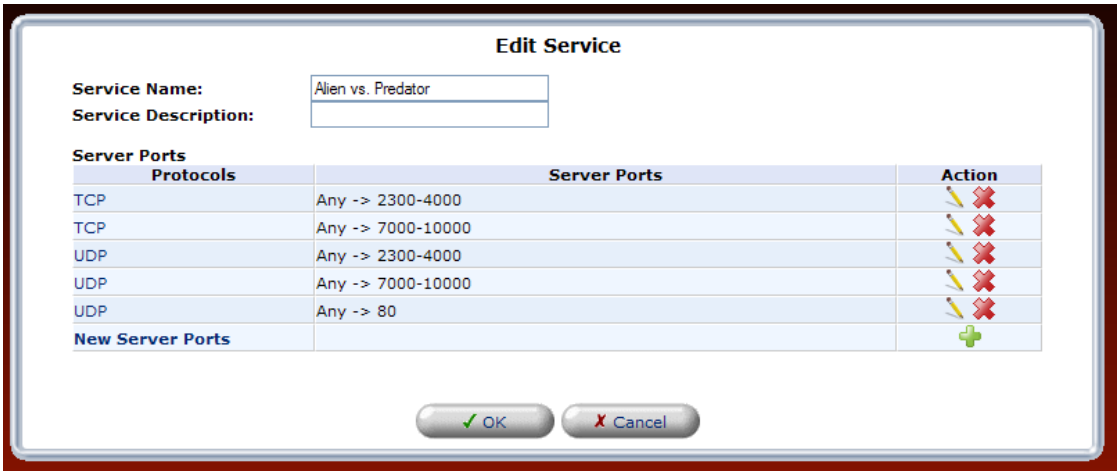


If you selected TCP (Any -> 2300-4000) the following screen appears. Select the desired source port and destination port values from the drop-down lists, and then click **OK**.

NOTE: For the Source and Destination ports, you can select a single port or a range of ports. In this example, the range for the Source port can be any value from 0 through 65535. And the range for the Destination port can be any value from 2300-4000.



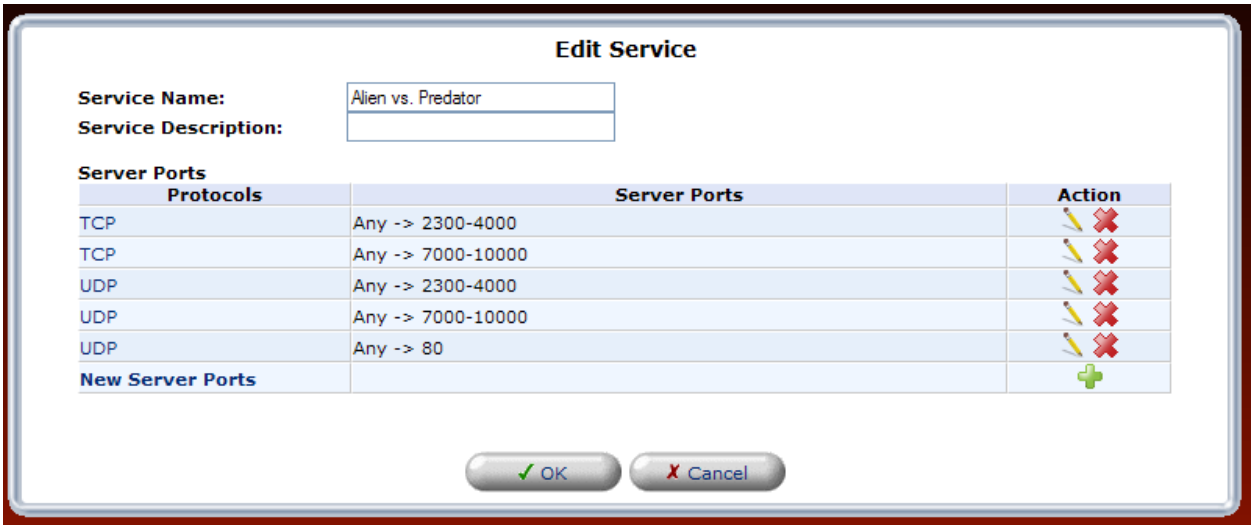
After you have entered the desired values and click **OK** in the preceding screen, the following screen appears. The TCP protocol values have been configured. Next, click **OK** to save the settings.



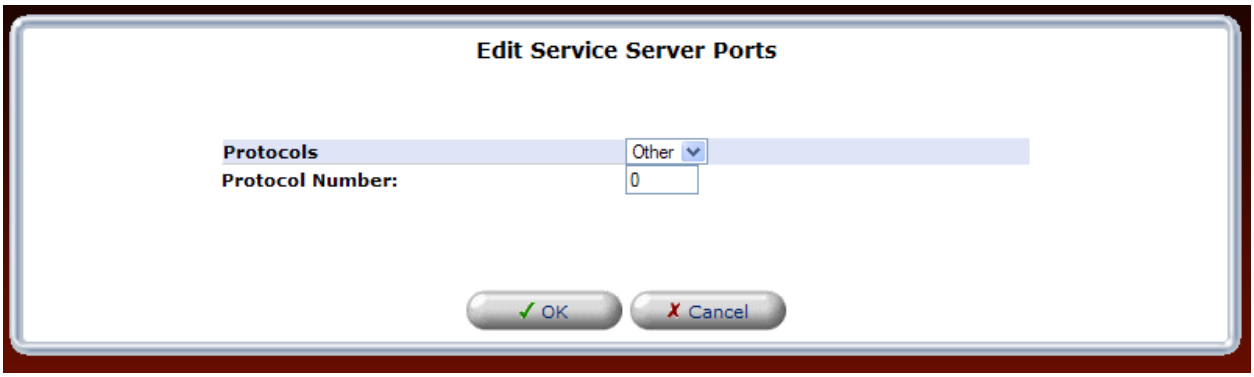
If you clicked **OK**, the protocol values will be saved to the Router, and the following screen will display the entry.

15.12.2.2 Configuring a New User-Defined Application

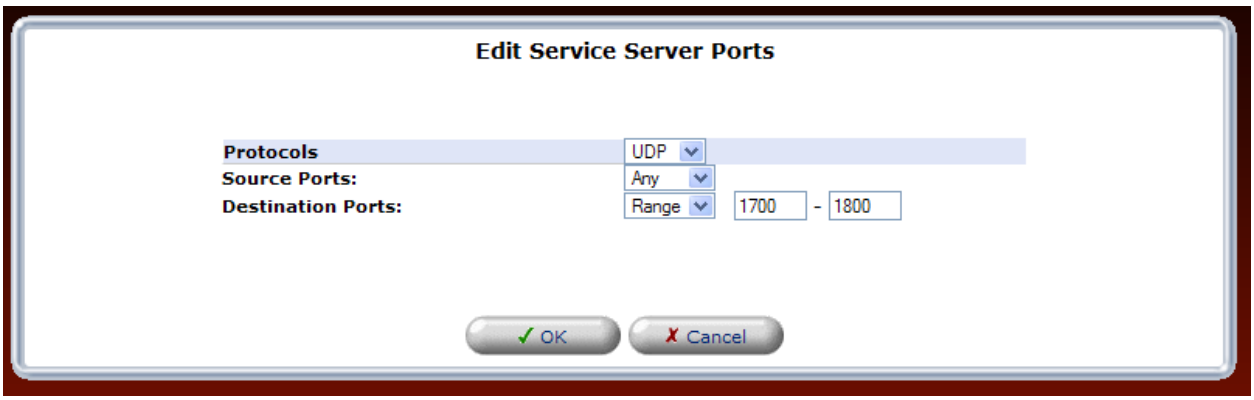
To configure new user-defined application, click the **New Server Ports** link in the **Edit Service** screen.



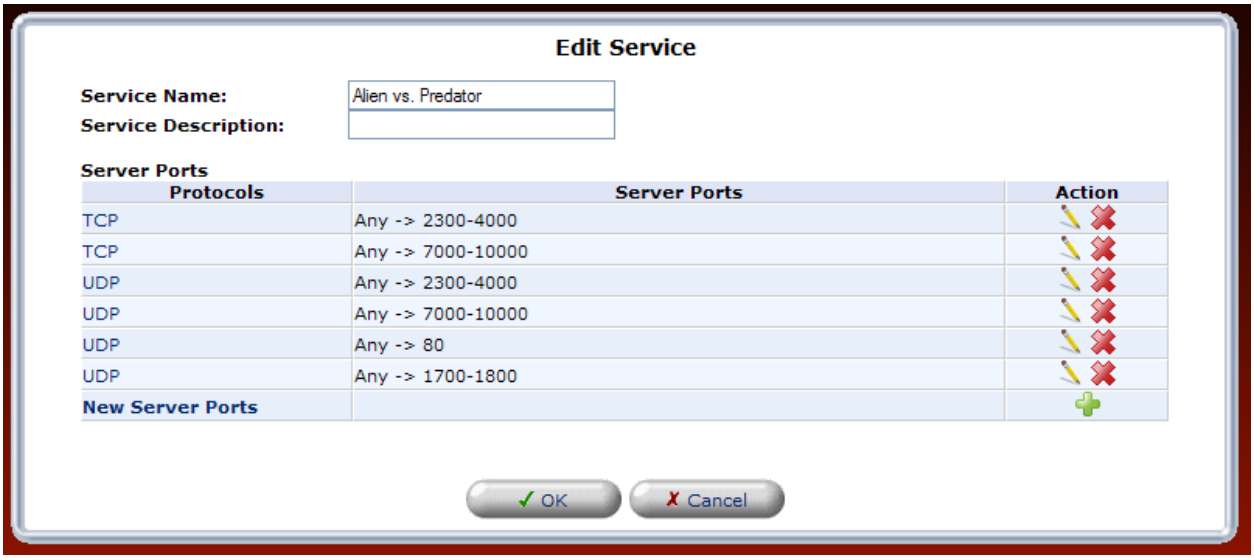
If you clicked **New Server Ports**, the following screen appears. Select the desired protocol from the **Protocol** drop-down list, and then enter the protocol number.



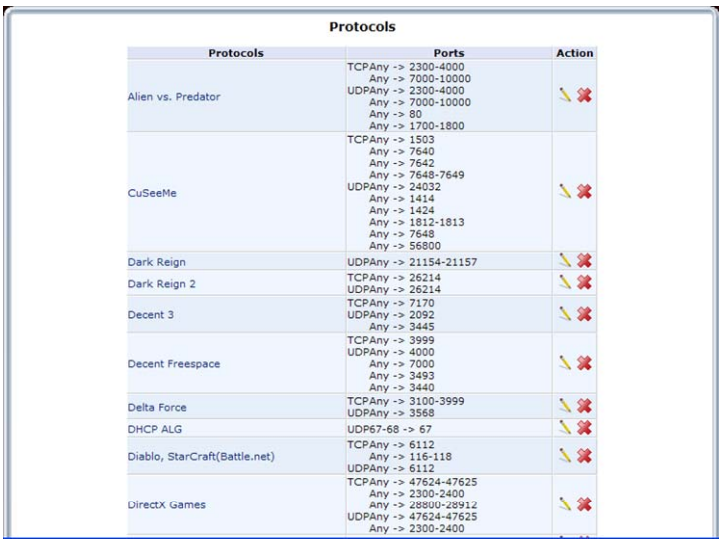
For example, this screen shows appropriate values, click **OK** to continue.



If you clicked **OK**, the following screen appears. The UDP port values have been configured. Next, click **OK** to save the settings.



If you clicked **OK**, the following screen appears. The user-defined UDP port settings are now saved to the Router.



Protocols

Protocols	Ports	Action
Alien vs. Predator	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80 Any -> 1700-1800	
CuSeeMe	TCPAny -> 1503 Any -> 7640 Any -> 7642 Any -> 7648-7649 UDPAny -> 24032 Any -> 1414 Any -> 1424 Any -> 1812-1813 Any -> 7648 Any -> 56800	
Dark Reign	UDPAny -> 21154-21157	
Dark Reign 2	TCPAny -> 26214 UDPAny -> 26214	
Decent 3	TCPAny -> 7170 UDPAny -> 2092 Any -> 3445	
Decent Freespace	TCPAny -> 3999 UDPAny -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	
DHCP ALG	UDP67-68 -> 67	
Diablo, StarCraft(Battle.net)	TCPAny -> 6112 Any -> 116-118 UDPAny -> 6112	
DirectX Games	TCPAny -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912 UDPAny -> 47624-47625 Any -> 2300-2400	

15.13 MGCP ALG

If you click **Advanced** in the top navigation menu and then select the **MGCP ALG** link, the following screen appears. The UltraLine Series3 includes a Media Gateway Control Protocol (MGCP) Application-level Gateway (ALG). MGCP is a signaling and call control protocol used by some Voice over IP (VoIP) systems. This ALG enables use of MGCP devices behind your firewall without the need to create pinholes or custom firewall rules for this specific type of traffic.

To enable the MGCP ALG, select **Enabled** from the MGCP ALG drop-down list. Then click **Apply** to save the setting.

NOTE: Do not enable this setting unless your service provider instructs you to do so.

15.14 SIP ALG

If you click **Advanced** in the top navigation menu and then select the **SIP ALG** link, the following screen appears. The UltraLine Series3 includes a Session Initiation Protocol (SIP) Application-level Gateway. SIP is a signaling protocol used by multimedia applications, most commonly a Voice over IP (VoIP) system. This ALG enables use of SIP devices behind your firewall without the need to create pinholes or custom firewall rules for this specific type of traffic.

To enable SIP ALG, select **Enabled** from the SIP ALG drop-down list. Then, click **Apply** to save the setting.

NOTE: Do not enable this setting unless your service provider instructs you to do so.

15.15 UPnP

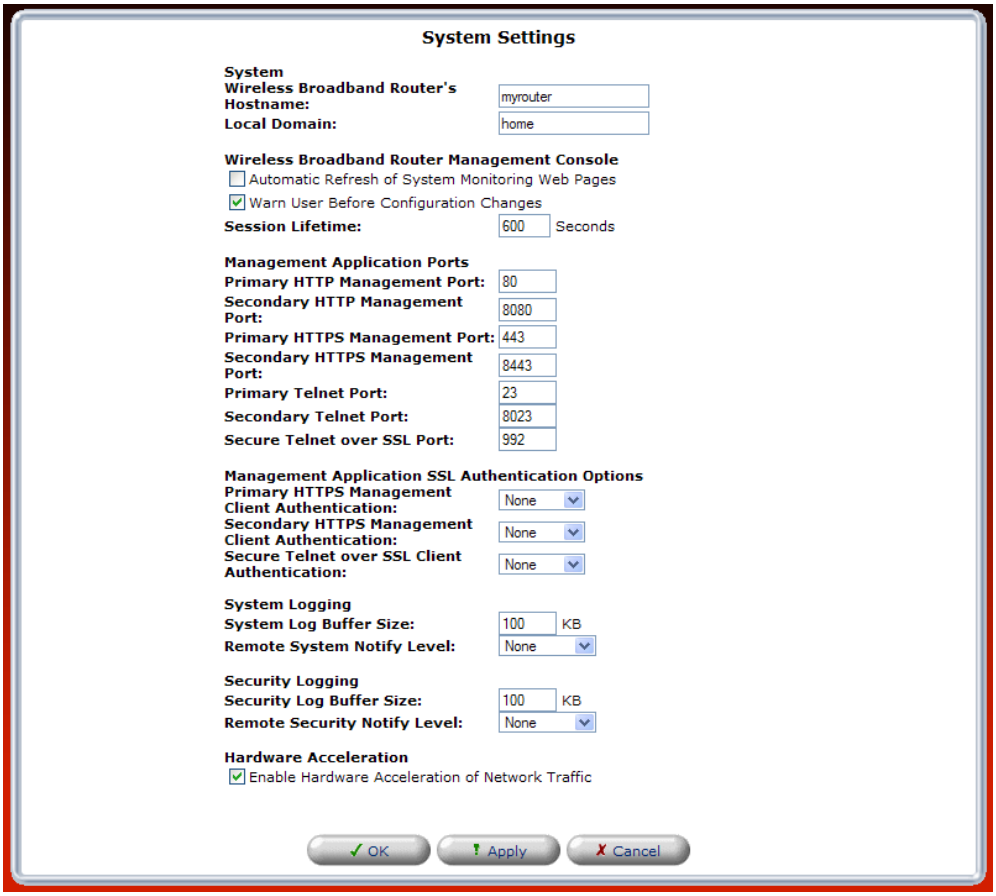
If you click **Advanced** in the top navigation menu and then select the **UPnP** link, the following screen appears. This feature advertises the presence of your Router on the LAN. Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. Products that have UPnP can seamlessly connect and communicate with other Universal Plug-and-Play enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers.

To configure UPnP enter the desired values and then click **Apply** to save the settings.

15.16 System Settings

If you click **Advanced** in the top navigation menu and then select the **System Settings** link, the following screen appears. Use this page to configure various system settings. Enter the desired system settings and then click **Apply** to save the settings.

NOTE: This Router ships with Telnet disabled. If Telnet is enabled, you can configure Secure Telnet over SSL Port/Client Authentication.



Hostname—Specify the Router's host name. The host name is the Router's URL address.
Local Domain—Specify your network's local domain.

Wireless Broadband Router Management Console

Automatic Refresh of System Monitoring Web Pages—select this check box to enable the automatic refresh of system monitoring web pages.

Warn User Before Network Configuration Changes—select this check box to activate user warnings before network configuration changes take effect.

Session Lifetime—this value represents duration of idle time (in seconds) in which the Router will remain active. When this duration times out, the user will have to re-login.

Management Application Ports

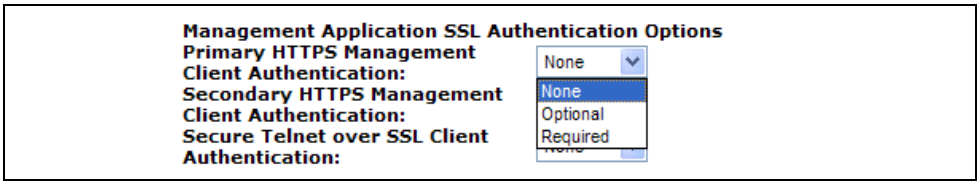
You can configure the following management application ports:

- Primary/Secondary HTTP Management Port
- Primary/Secondary HTTPS Management Port
- Primary/Secondary Telnet Port HTTPs
- Secure Telnet over SSL Port

Management Application SSL Authentication Options

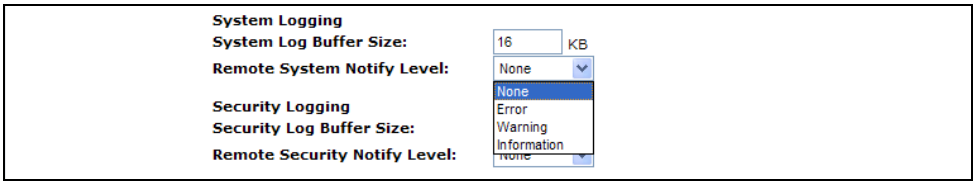
You can configure the Primary and Secondary HTTPS Management Client Authentication. Select the desired option from the drop-down lists:

- Select **None** if you do not want to use client authentication.
- Select **Optional** if you want client authentication to be optional.
- Select **Required** if you want client authentication to be required.



System Logging—configure system logging parameters.
System Log Buffer Size—set the size of the system log buffer in Kilobytes.
Remote System Notify Level—select one of the following remote system notification level from the drop-down list:

- None
- Error
- Warning
- Information

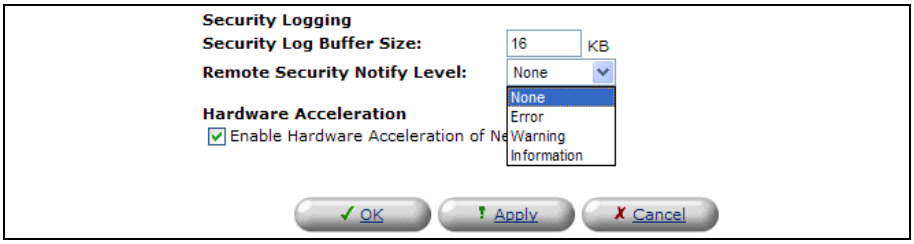


Security Logging—configure security logging parameters.
Security Log Buffer Size—set the size of the security log buffer in Kilobytes.
Remote Security Notify Level—select one of the following remote security notification levels from the drop-down list:

- None
- Error
- Warning
- Information

Hardware Acceleration—To enable this feature, click the **Enable Hardware Acceleration of Network Traffic** check box (if it is not already checked).

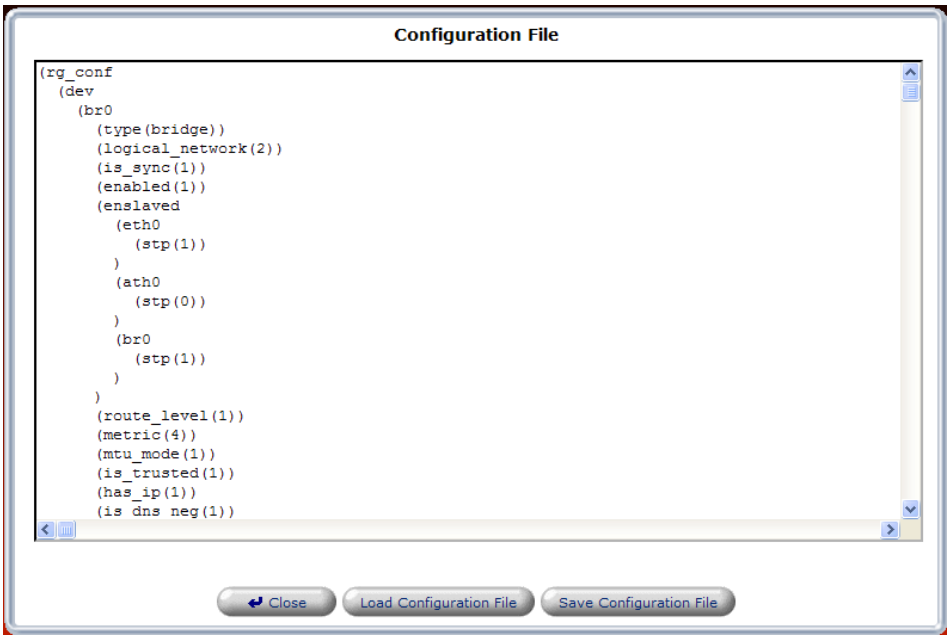
After you have configured the desired settings, click **Apply** to allow the settings to take effect in the Router.



15.17 Configuration File

If you click **Advanced** in the top navigation menu and then select the **Configuration File** link, the following screen appears.

IMPORTANT: Do not change the settings in this page unless instructed by Verizon.

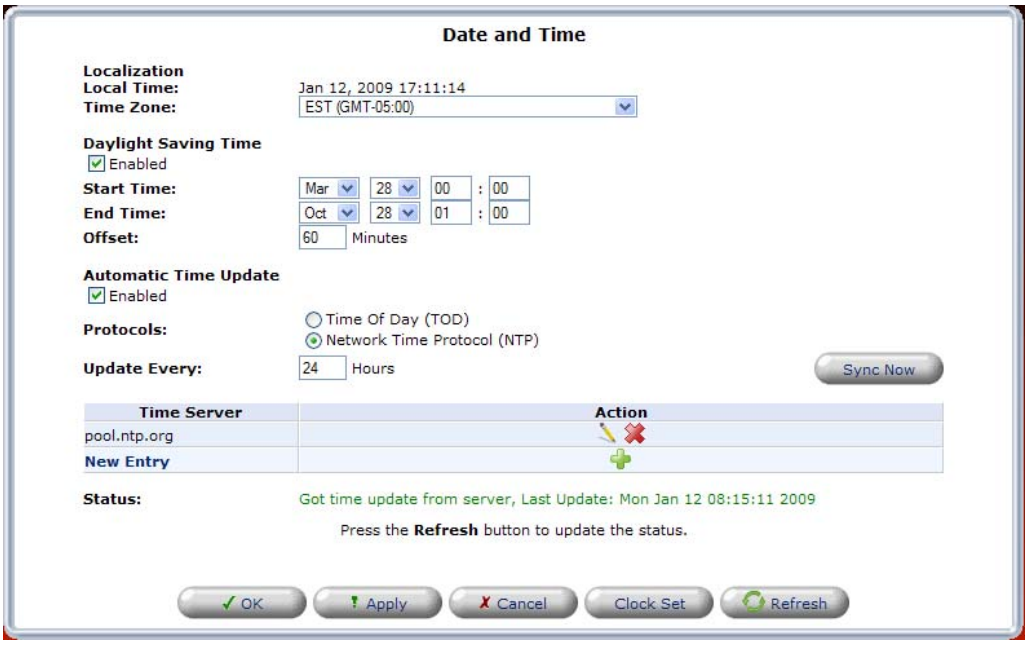


15.18 Date and Time Rules

If you click **Advanced** in the top navigation menu and then select the **Date and Time** link, the following screen appears. Enter the desired values in this screen, and then click **Apply** to save the settings.

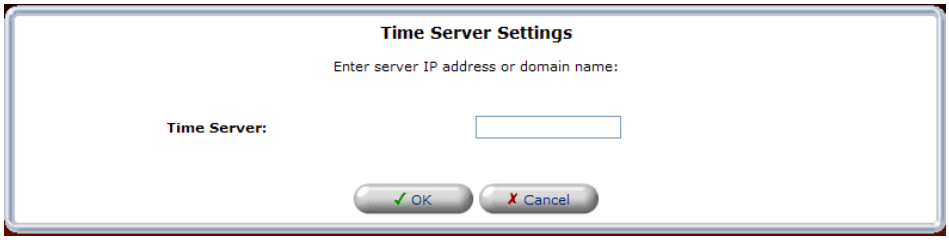
The Router can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for a time zone are not automatically detected, the following fields will be displayed:

- Enabled—Click this check box to enable daylight saving time (a check mark will appear in the box).
- Start—Enter the date and time when daylight saving starts.
- End—Enter the date and time when daylight saving ends.
- Offset—Enter the time amount daylight saving time changes.
- Automatic Time Update—Click the check box to activate automatic time update (a check mark will appear in the box).
- Protocols—Click the radio button for the protocol used to perform the time update.
- Update Every—Enter the desired value (in Hours) to specify how often to perform the update.
- Time Server—This table lists the address of the time server.
- Status—Displays a time update status.
- Sync Now—Click this button to synchronize the Router's time with your computer operating system's time.

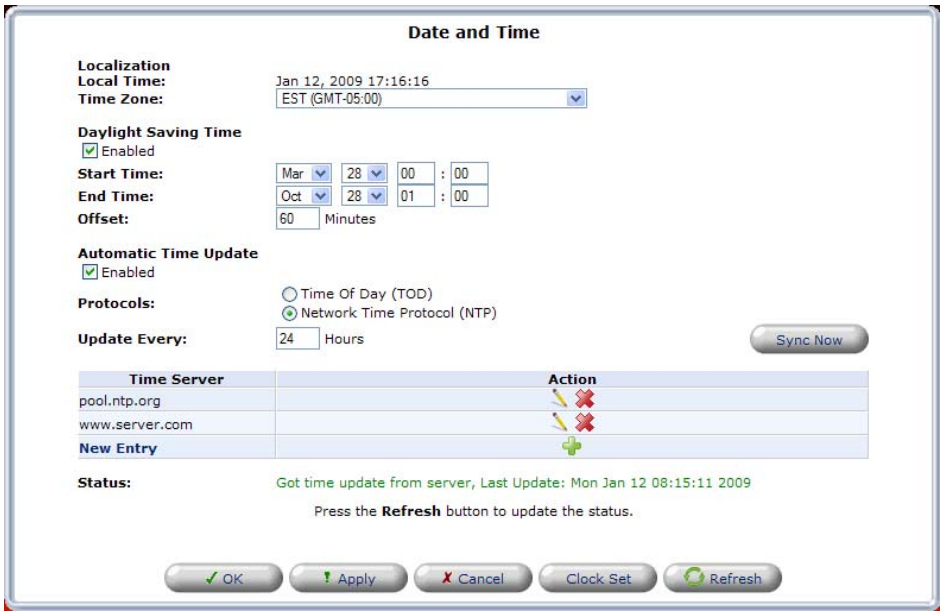


15.19 Editing the Time Server Table

If you click the **New Entry** link under **Time Server,** the following screen appears. Enter a server IP address or domain name in the field provided, and then click **OK** to continue.



The entry will be added to the time server table. To remove server address from the Time Server table, click the "X" icon next to the server to want to remove. Then, click **Apply** to save the changes.

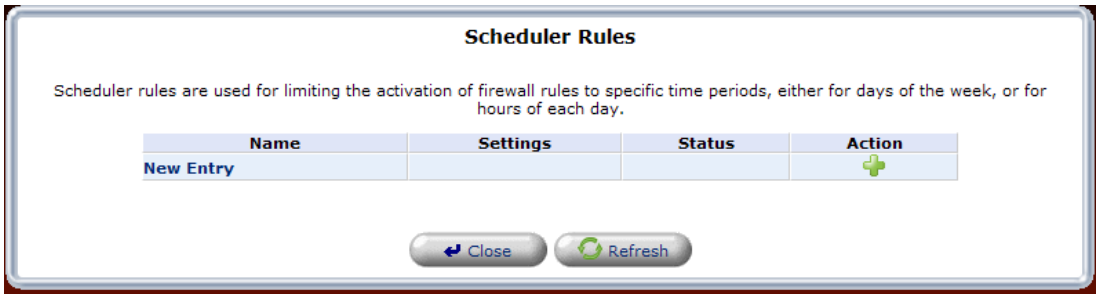


15.20 Editing Clock Set

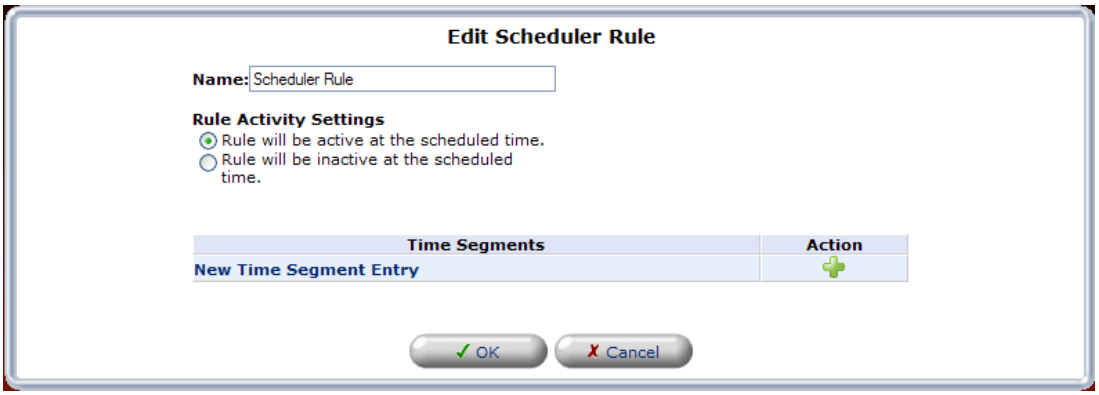
If you click the **Clock Set** button in the **Date and Time** screen, the following screen appears. Enter your local time by selecting the appropriate values from the month, day, and year drop-down lists. Next, enter your local time (starting with hours, minutes, and seconds) in the fields provided. Click **Apply** to save the settings. Then click **OK** to return to the **Date and Time** screen.

15.21 Scheduler Rules

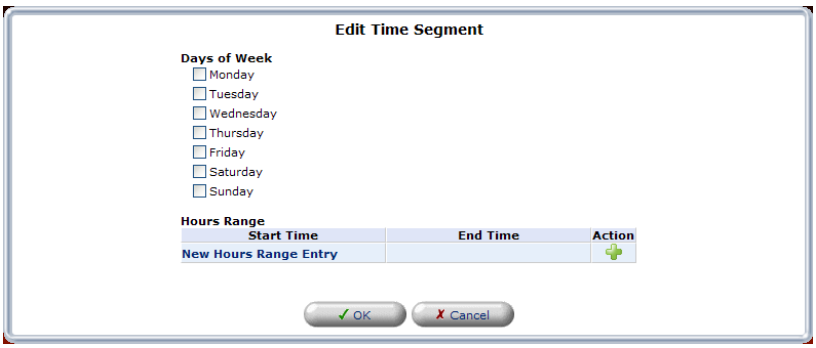
If you click **Advanced** in the top navigation menu and then select the **Scheduler Rules** link, the following screen appears. To configure a schedule rule, click the **New Entry** link.



The following screen appears. Click the **New Time Segment Entry** link or, alternatively, click the plus icon.

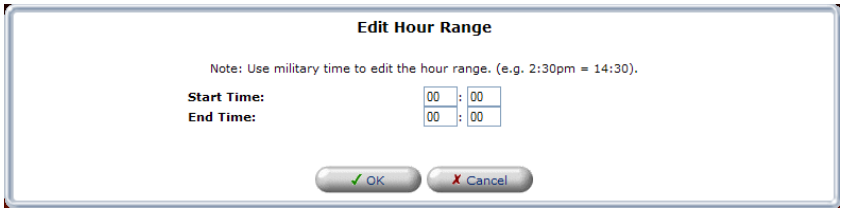


If you clicked **New Time Segment Entry,** the following appears. Click the **New Hours Range Entry** link.



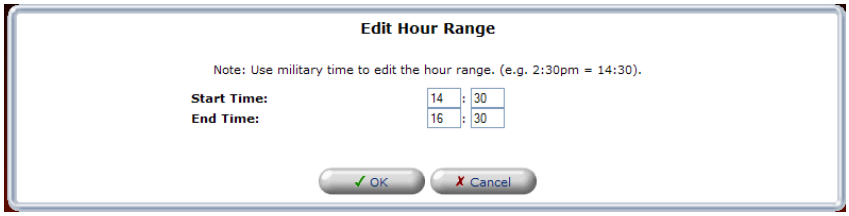
The following screen appears. Enter the desired start time and end time values in the fields provided.

Note: Use military time to edit the Hour range. For example, 2:00 P.M. standard time is equivalent to 14:00 military time, as indicated in the following chart.

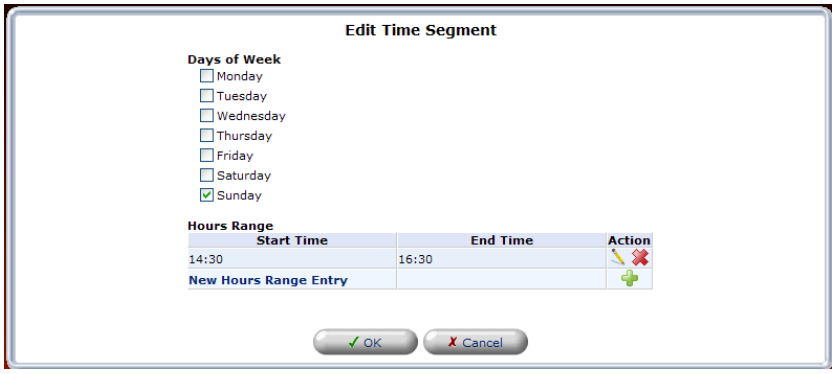


Military Time Chart	
Standard Time	**Military Time**
1:00 A.M.	0100
2:00 A.M.	0200
3:00 A.M.	0300
4:00 A.M.	0400
5:00 A.M.	0500
6:00 A.M.	0600
7:00 A.M.	0700
8:00 A.M.	0800
9:00 A.M.	0900
10:00 A.M.	1000
11:00 A.M.	1100
12:00 P.M. (Noon)	1200
1:00 P.M.	1300
2:00 P.M.	1400
3:00 P.M.	1500
4:00 P.M.	1600
5:00 P.M.	1700
6:00 P.M.	1800
7:00 P.M.	1900
8:00 P.M.	2000
9:00 P.M.	2100
10:00 P.M.	2200
11:00 P.M.	2300
12:00 A.M. (Midnight)	0000
A.M. = Ante Meridiem. The period from midnight until noon. *P.M. = Post Meridiem. The period between noon and midnight.*	

For an example, the values in the following screen represent military hours. After you have entered your desired values, click **OK** to continue.



If you clicked **OK** the following screen appears. Click the check box for each day that you want to apply the time segment (a check mark will appear in the box). Click **OK** to continue.

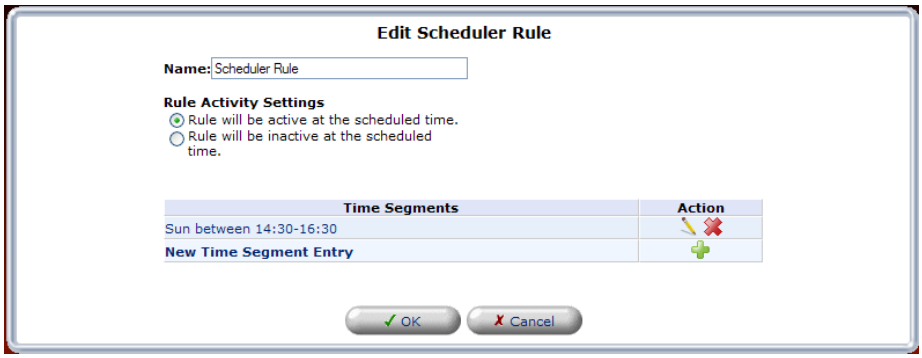


After you have set up the desired time segment and clicked **OK**, the following screen appears. If desired, you can enter a name for the schedule rule in the **Name** field.

Under **Rule Activity Settings,** be sure to click the setting that you want assigned to the rule:

- Click the first radio button to allow the rule to be active at the scheduled time.
- Click the second radio button to allow the rule to be inactive at the scheduled time.

For example, this screen shows that a schedule has been added to the **Time Segments** table, and that the rule will be active at the scheduled time. To add additional schedule rules to your Router, repeat the preceding scheduler rules instructions. Then, click **OK** in the **Edit Scheduler Rule** screen to allow the settings to take effect in the Router.



15.22 Firmware Upgrade

If you click **Advanced** in the top navigation menu and then select the **Firmware Upgrade** link, the following screen appears. This screen is used to update the firmware that controls the operation of your Router. The updated firmware may be loaded from a CD-ROM, from a file stored on a local hard drive within your network, or from an update file stored on an Internet server.

IMPORTANT: The configurable settings of your Router may be erased during the upgrade process.

Do any of the following:

- Select the desired option from the **Upgrade from the Internet** drop-down list. You can choose to perform an automatic check at the specified number of hours and URL. Or you can disable automatic check.

  NOTE: The URL must be in the format: protocol://user:password@host:port/path where protocol is one of http, https, ftp or tftp. Either user or password, or both, may be left out. The port number is also optional.

- Click **Check Now** to retrieve the firmware update file and display any available update information. You must be connected to the Internet to use this option.

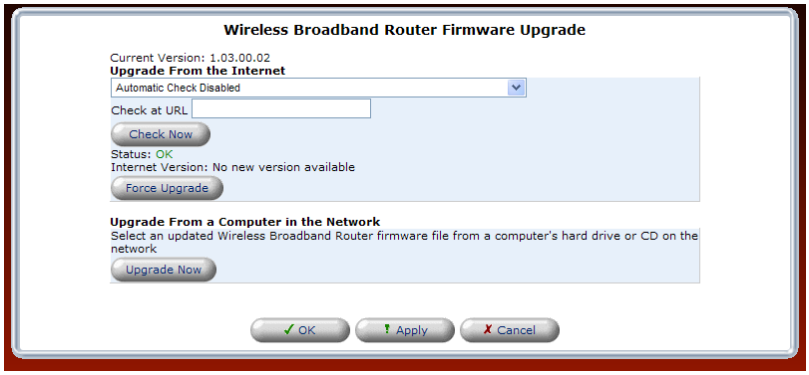
  NOTE: If you click **Check Now** and the page returns "No new version available," this indicates that the firmware update file is not available.

- Click **Force Upgrade** to download the firmware update file and to automatically update the Router firmware if an update is available and applicable. You must be connected to the Internet to use this option.

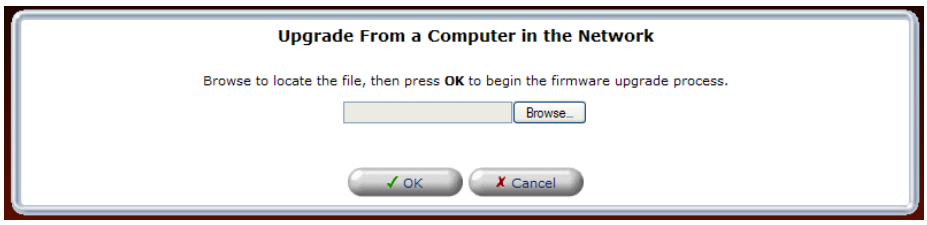
  NOTE: The URL must be in the format: protocol://user:password@host:port/path where protocol is one of http, https, ftp or tftp. Either user or password, or both, may be left out. The port number is also optional.

- Click Upgrade Now to retrieve the firmware update file from a local hard drive or CD-ROM on your Network. Internet connection is not required for this option.

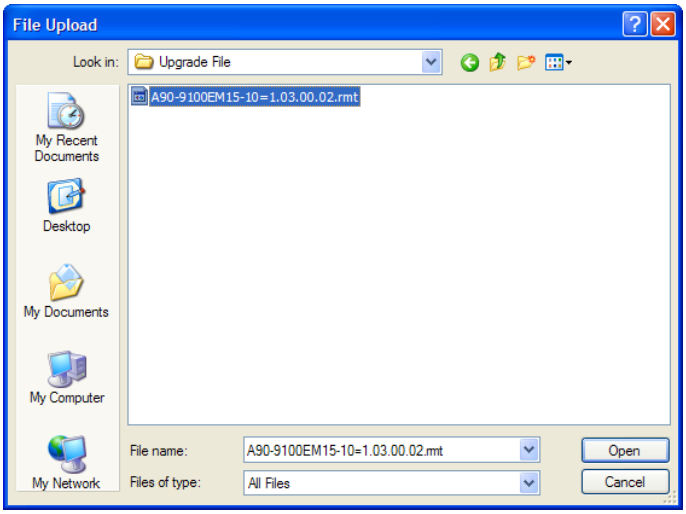
For example, to upgrade your Router, click the **Upgrade Now** button.



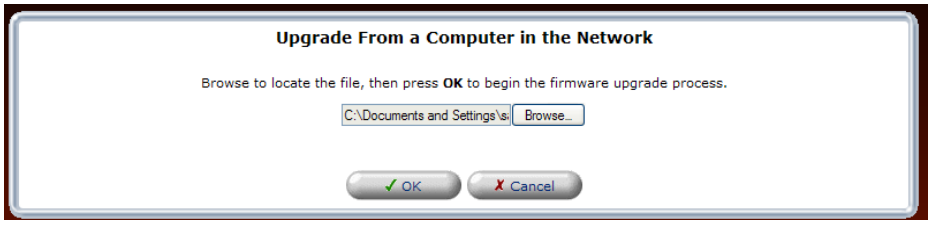
Next, click the **Browse** button to navigate to the location of the upgrade file.



Once you have located the file, double-click the file to select it.

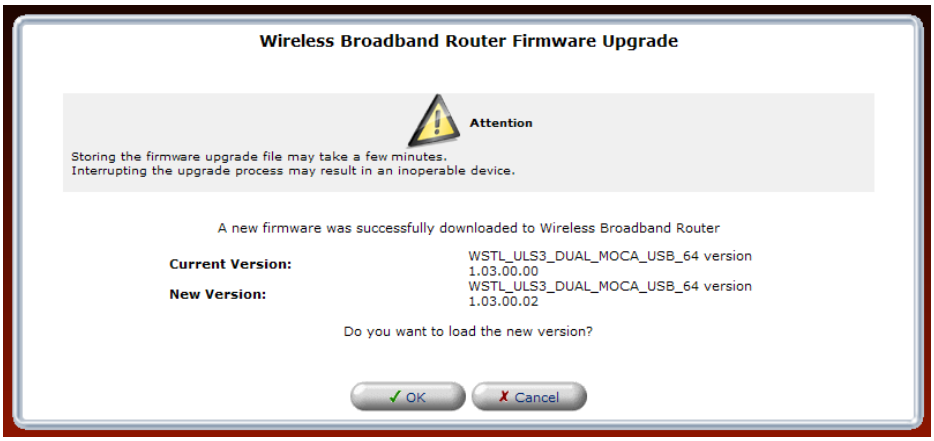


The pathname of the file will appear in the Browse field, as shown below. Click **OK** to continue.



Next, the Router will prompt you to confirm that you want to load the new version. Click **OK** to load the new version.

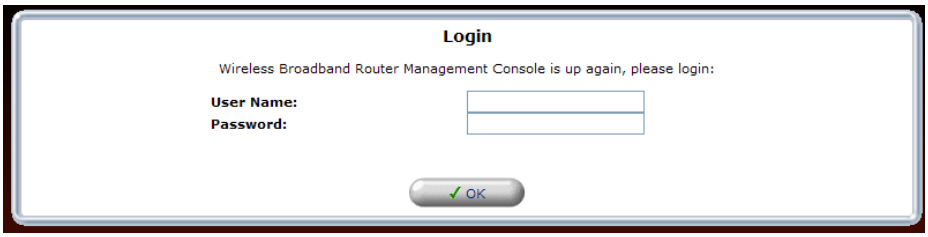
IMPORTANT: Please do not attempt to use the Router during the upgrade process. Interrupting the upgrade process may result in an inoperable device.



The Router will begin the upgrade process. Please wait a brief moment for the upgrade to complete.

NOTE: If the page does not refresh automatically in a minute, click the Login button.

After the upgrade has completed, the following screen will appear. Please type your user name and password to log in to your Router.

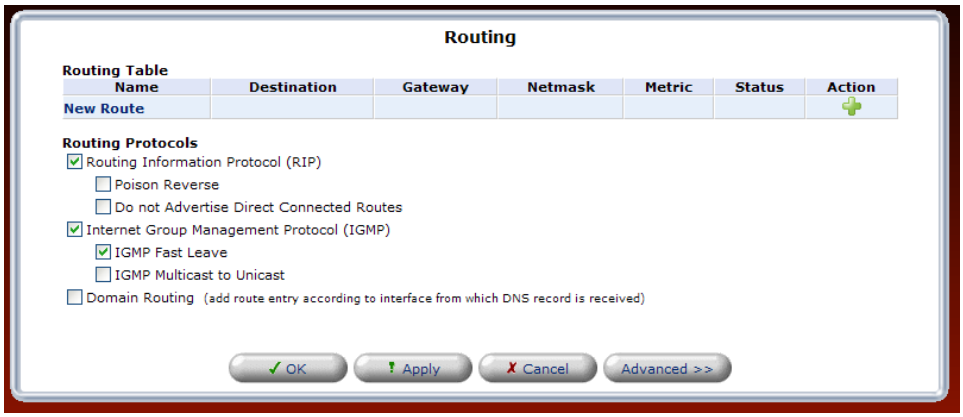


15.23 Routing

If you click **Advanced** in the top navigation menu and then select the **Routing** link, the following screen appears. You can choose to setup your Router to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

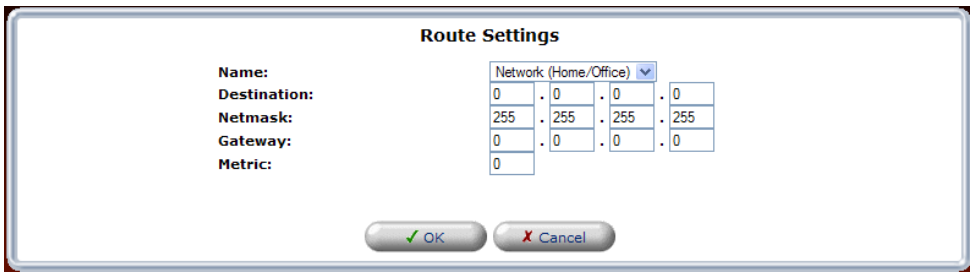
15.23.1 Basic Routing Settings

To create a new route, click the **New Route** link. If you change any settings in this screen, click **Apply** to save the settings.



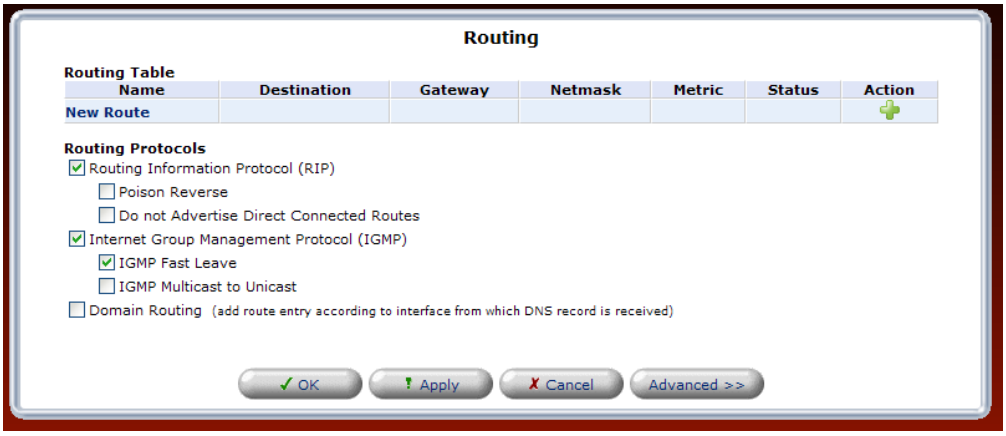
If you clicked **New Route,** the following screen appears. Configure the settings in this screen, and then click **OK** to continue.

- Rule Name—Select the type of network from the drop-down list.
- Destination—Enter 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—Enter 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—Enter the desired 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.



15.23.2 Advanced Routing Settings

To configure advanced routing settings, click the **Advanced** button in the **Routing** screen.



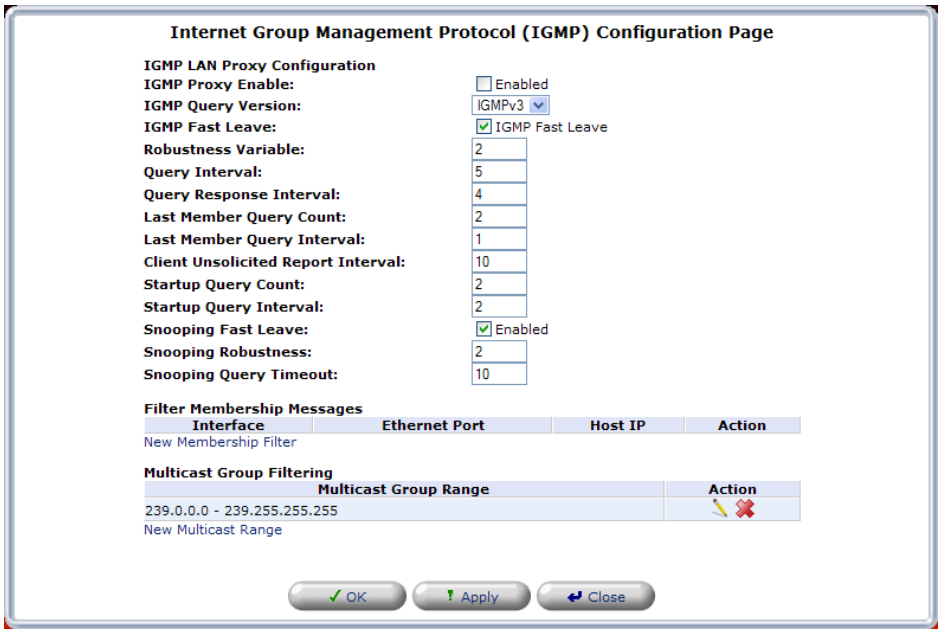
If you clicked the **Advanced** button, the following screen appears. If you change any settings in this screen, click **Apply** to save the settings.

15.24 IGMP Configuration

If you click **Advanced** in the top navigation menu and then select the **IGMP Configuration** link, the following screen appears. This screen allows you to configure IGMP LAN Proxy configuration settings in your Router.

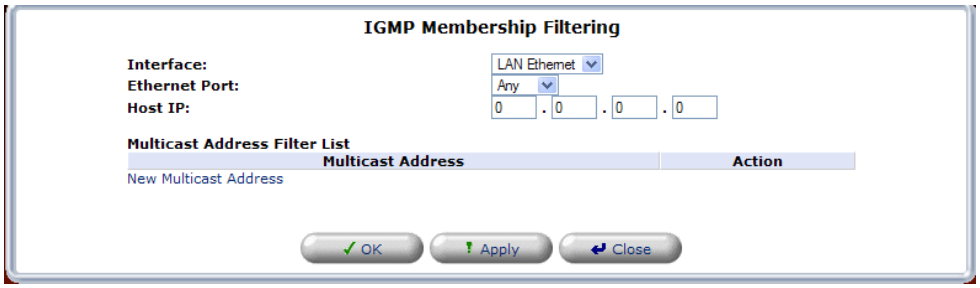
The Router supports IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a predefined group of recipients. Each member of the multicast group will receive all messages addressed to the group.

IGMP proxy enables multicast packets to be routed according to the IGMP requests of local network devices requesting to join multicast groups. To enable IGMP Proxy, click the adjacent check box, a check mark will appear in the box. Next, enter the appropriate values in the fields provided and click **Apply** to save the settings.

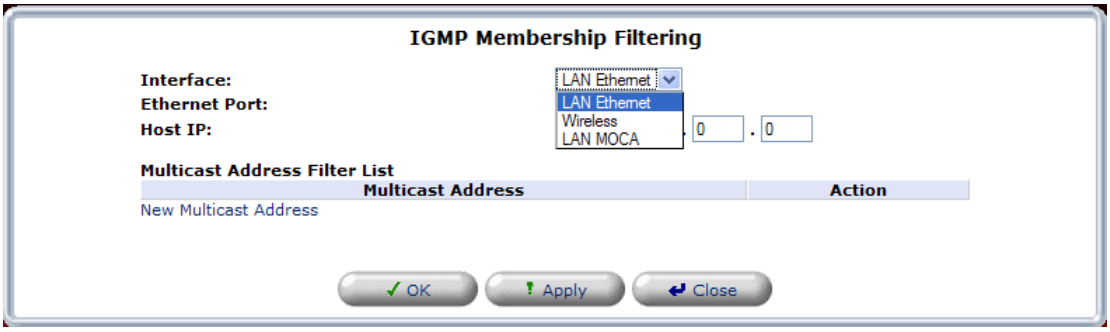


15.24.1 New Membership Filter

If you clicked the **New Membership Filter** link in the preceding screen, the following screen appears.

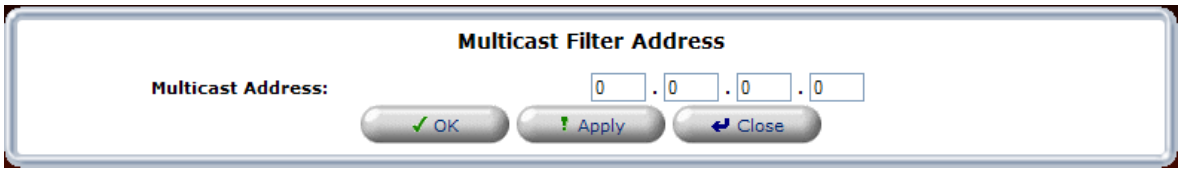


Select the desired settings for the membership filter you want to create. Then click **Apply** to save the settings.

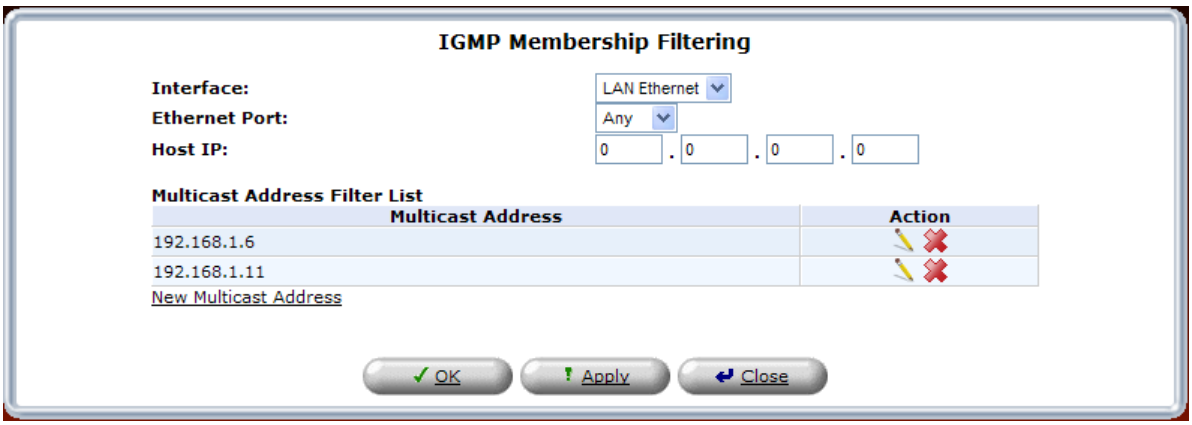


15.24.2 New Multicast Address

If you clicked the **New Multicast Address** link in the preceding screen, the following screen appears. Enter multicast address and then click **Apply**. If desired, repeat this process to enter additional multicast addresses. After you have finished entering addresses, click **Close** to return to the IGMP Membership Filtering screen.



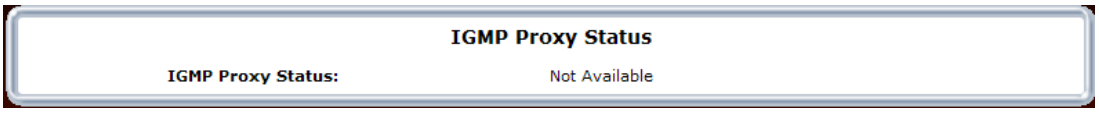
The addresses will be displayed in the list of Multicast Addresses.



15.25 IGMP Status

If you click **Advanced** in the top navigation menu and then select the **IGMP Status** link, the following screen appears.

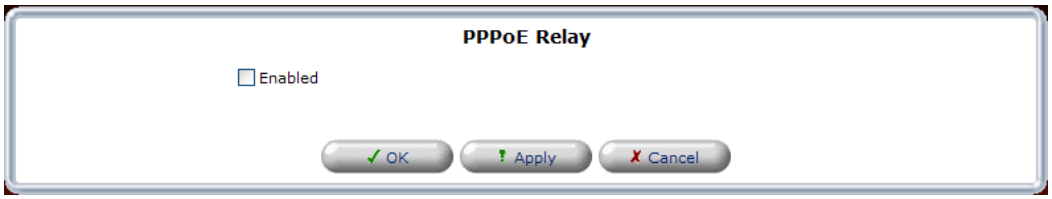
NOTE: If IGMP proxy is not enabled, the IGMP Proxy Status panel will be empty.



15.26 PPPoE Relay

If you click **Advanced** in the top navigation menu and then select the **PPPoE Relay** link, the following screen appears. PPPoE Relay enables the Router to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections.

To activate PPPoE Relay, click the check box (check mark will appear in the box). Click **Apply** to save the settings.

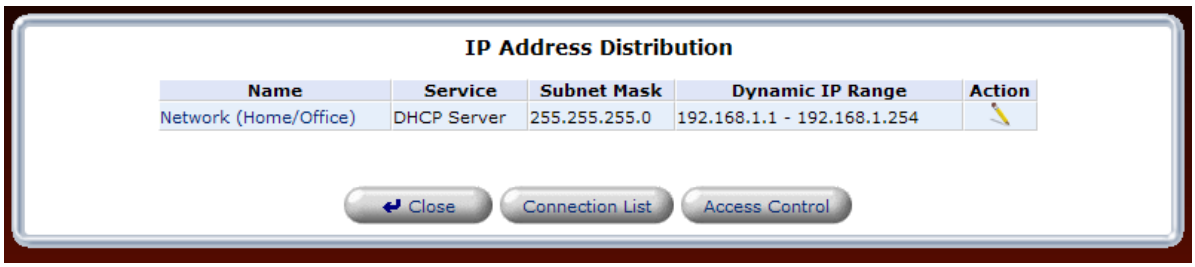


15.27 IP Address Distribution

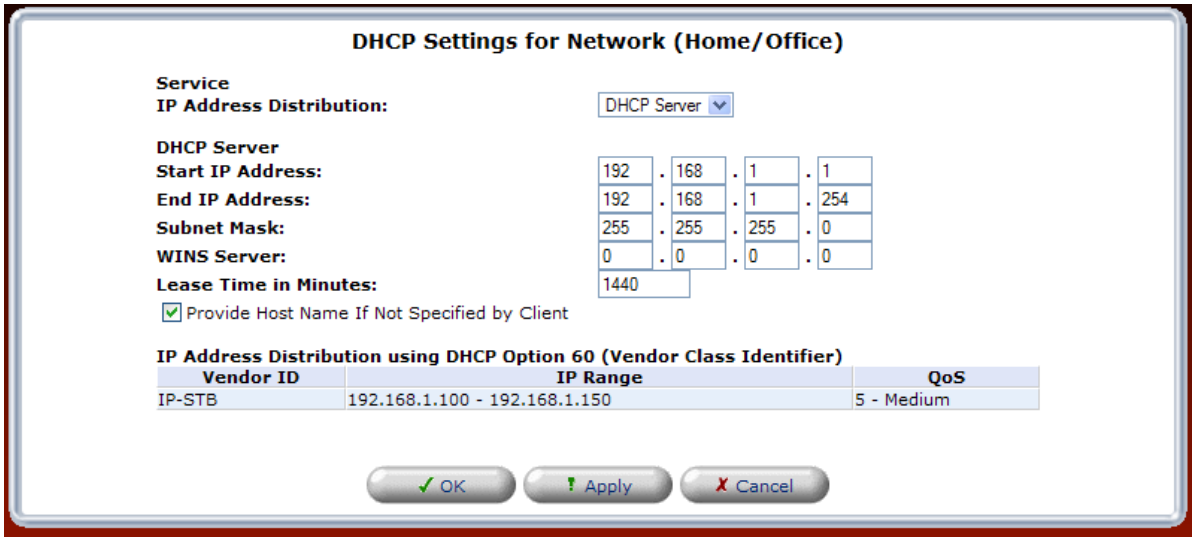
If you click **Advanced** in the top navigation menu and then select the **IP Address Distribution** link, the following screen appears.

Your Router's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. The Router's default DHCP server is the LAN bridge.

A client (host) sends out a broadcast message on the LAN 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 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.



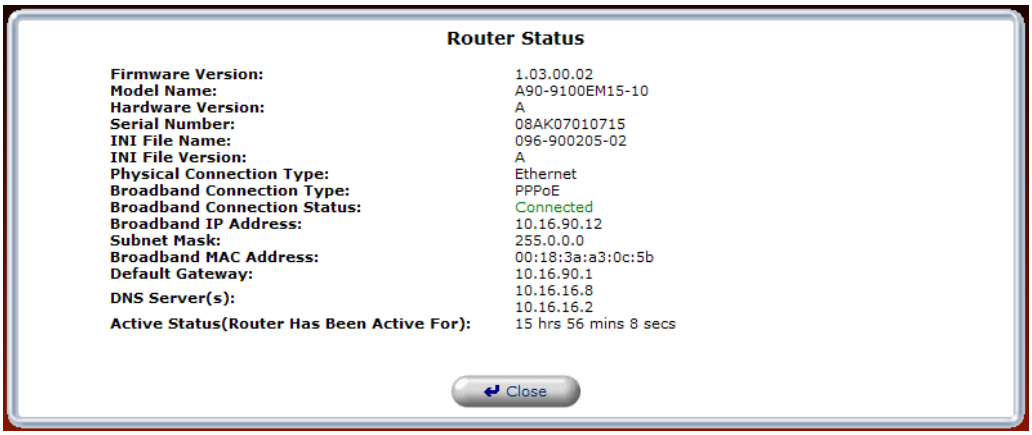
To configure the DHCP Sever settings, click the Network (Home/Office) link, the following screen appears. Enter the desired DHCP settings in the fields provided, and then click **Apply** to save the settings.



16. SYSTEM MONITORING

16.1 Router Status

If you click **System Monitoring** in the top navigation menu, the following screen appears. After you have finished viewing information about your Router, click **Close**.

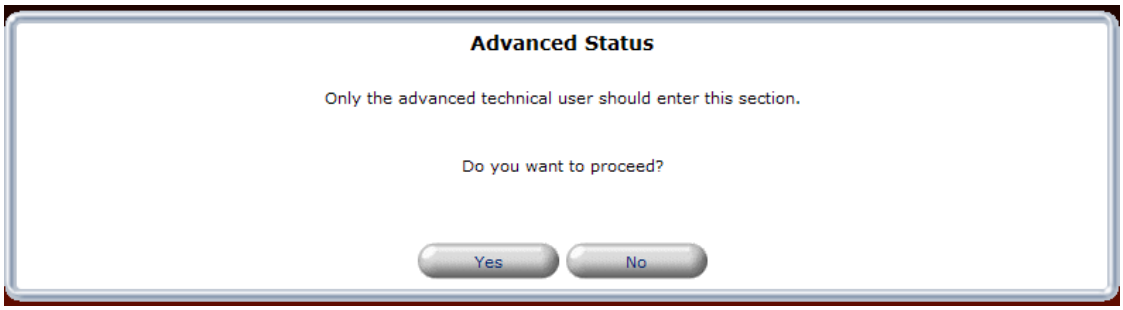


Router Status	
Firmware Version	The Router's software version.
Model Number	The Router manufacturer's model number.
Hardware Version	The Router manufacturer's hardware version.
Serial Number	The Router's serial number
INI File Name	The Router's INI file name.
INI File Version	The Router's INI file version.
Physical Connection Type	The Interface used for the Router's broadband connection.
Broadband Connection Type	The Protocol used for the Router's broadband connection
Broadband Connection Status	The status (connected or disconnected) of the Router's broadband connection.
Broadband IP Address	The Router's broadband (WAN) IP address.
Subnet Mask	The Router's subnet address.
Broadband MAC Address	The Router's media access controller address-hardware address of the Router.
Default Gateway	The Router's default gateway IP address.
DNS Server(s)	The gateway's DNS server(s) addresses.
Active Status	The period that the Router has had an active broadband connection.

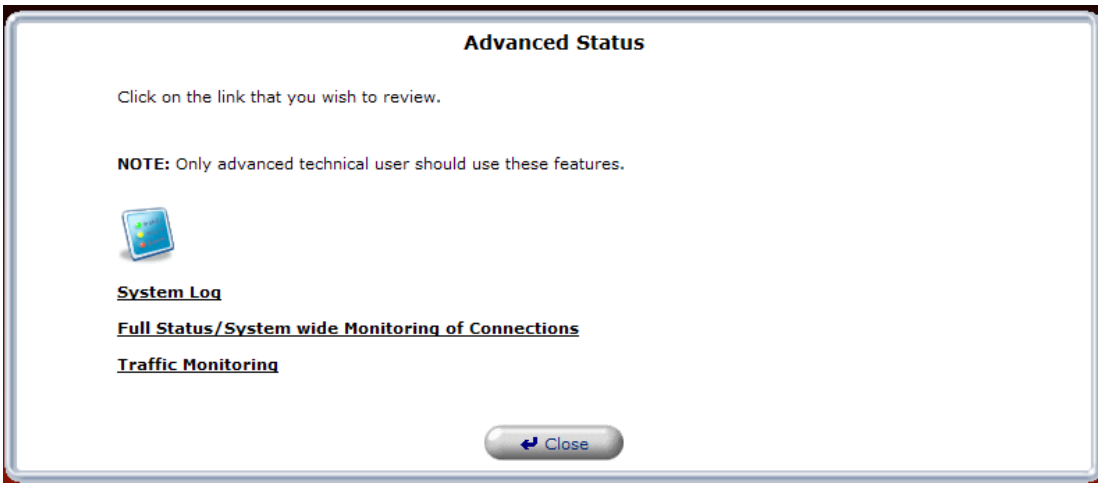
16.2 Advanced Status

If you click **System Monitoring** in the top navigation menu, and then click **Advanced Status** in the left submenu, the following screen appears. Click **Yes** to proceed.

NOTE: Only the advanced technical user should enter this section.



The following screen displays connection information for devices connected to your Router. Click the link that you wish to review.



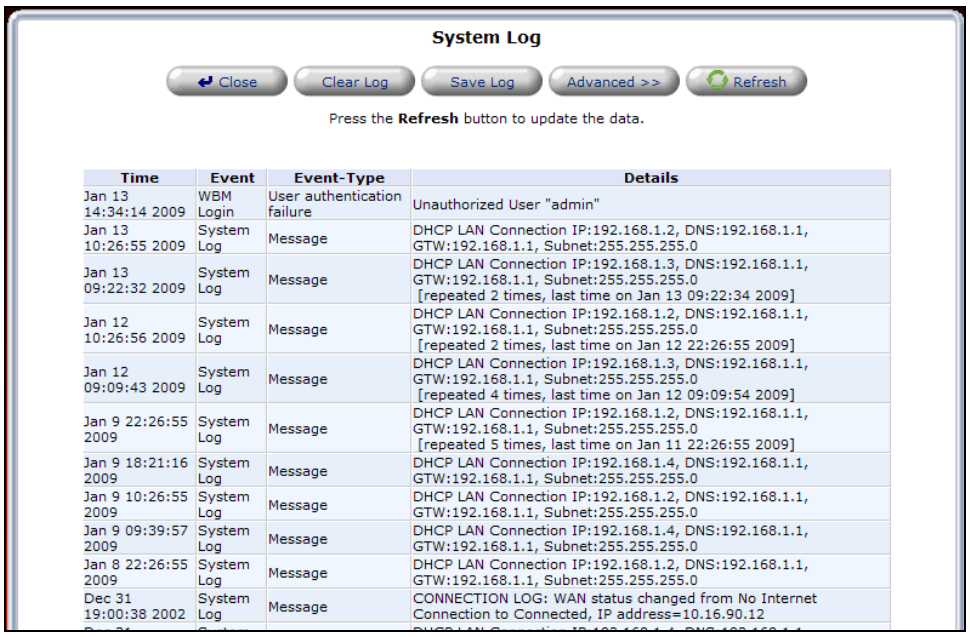
16.2.1 System Log

If you click the **System Log** link, the following screen appears. This screen displays the details of your system's logged events.

NOTE: Only the advanced technical user should enter this section.

At this screen, you can do any of the following:

- Click the **Refresh** button to manually update this screen to display the most current details.
- Click **Advanced** to go to the advanced System Log screen.
- Click **Save Log,** and then follow the instructions to save the system log to the desired location.
- Click **Clear Log** to remove all logs from the list.
- Click **Close** to return to the **Advanced Status** screen.



Time	Event	Event-Type	Details
Jan 13 14:34:14 2009	WBM Login	User authentication failure	Unauthorized User "admin"
Jan 13 10:26:55 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.2, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0
Jan 13 09:22:32 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.3, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0 [repeated 2 times, last time on Jan 13 09:22:34 2009]
Jan 12 10:26:56 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.2, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0 [repeated 2 times, last time on Jan 12 22:26:55 2009]
Jan 12 09:09:43 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.3, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0 [repeated 4 times, last time on Jan 12 09:09:54 2009]
Jan 9 22:26:55 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.2, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0 [repeated 5 times, last time on Jan 11 22:26:55 2009]
Jan 9 18:21:16 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.4, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0
Jan 9 10:26:55 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.2, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0
Jan 9 09:39:57 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.4, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0
Jan 8 22:26:55 2009	System Log	Message	DHCP LAN Connection IP:192.168.1.2, DNS:192.168.1.1, GTW:192.168.1.1, Subnet:255.255.255.0
Dec 31 19:00:38 2002	System Log	Message	CONNECTION LOG: WAN status changed from No Internet Connection to Connected, IP address=10.16.90.12

16.2.2 Full Status/System Wide Monitoring of Connection

If you click the **Full Status/System Wide Monitoring of Connections** link, the following screen appears. This screen displays the details of your system's logged connections.

NOTE: Only the advanced technical user should enter this section.

At this screen, you can do any of the following:

- Click the **Automatic Refresh On/Off** button to turn on/off Automatic Refresh. When Automatic Refresh is **On**, the screen will be updated automatically to display the most current statistics.
- Click **Refresh** to manually update this screen to display the most current details.
- Click the links in this screen to access the Router's settings.
- Click **Close** to return to the **Advanced Status** screen.

Full Status/System wide Monitoring of Connections

Name	Network (Home/Office)	Ethernet Switch	Broadband Connection (Ethernet)	Coax	Broadband Connection (Coax)	Wireless 802.11g Access Point	WAN PPPoE
Status	Connected	1 Ports Connected	Connected	Down	Down	Connected	Connected
Network	Network (Home/Office)	Network (Home/Office)	WAN	Network (Home/Office)	WAN	Network (Home/Office)	WAN
Underlying Device	Ethernet Switch Coax Wireless 802.11g Access Point						Broadband Connection (Ethernet)
Connection Type	Bridge	Hardware Ethernet Switch	Ethernet	Multimedia over Coax (MOCA)	Multimedia over Coax (MOCA)	Wireless 802.11g Access Point	PPPoE
MAC Address	00:18:3a:a3:0c:5a	00:18:3a:a3:0c:5a	00:18:3a:a3:0c:5b		00:18:3a:a3:0c:5b	00:21:63:22:19:de	
IP Address	192.168.1.1						10.16.90.12
Subnet Mask	255.255.255.0						
Default Gateway							10.16.90.1
DNS Server							10.16.16.8 10.16.16.2
IP Address Distribution	DHCP Server	Disabled	Disabled			Disabled	
Service Name							
User Name							verizonfios
Received Packets	75688	98888	191688	0	0	9240	0
Sent Packets	338611	298050	160320	0	0	41459	0
Time Span	124:23:11	124:23:11	124:22:47			124:23:03	124:22:35

Close | Automatic Refresh On | Refresh

16.2.3 Traffic Monitoring

If you click the **Traffic Monitoring** link, the following screen appears. This screen displays the details of your system's logged traffic.

NOTE: Only the advanced technical user should enter this section.

At this screen, you can do any of the following:

- Click the **Automatic Refresh On/Off** button to turn on/off Automatic Refresh. When Automatic Refresh is **On**, the screen will be updated automatically to display the most current statistics.
- Click **Refresh** to manually update this screen to display the most current details.
- Click the links in this screen to access the Router's settings.
- Click **Close** to return to the **Advanced Status** screen.

Traffic Monitoring

Name	Network (Home/Office)	Ethernet Switch	Broadband Connection (Ethernet)	Coax	Broadband Connection (Coax)	Wireless 802.11g Access Point	WAN PPPoE
Status	Connected	1 Ports Connected	Connected	Down	Down	Connected	Connected
Network	Network (Home/Office)	Network (Home/Office)	WAN	Network (Home/Office)	WAN	Network (Home/Office)	WAN
Underlying Device	Ethernet Switch Coax Wireless 802.11g Access Point						Broadband Connection (Ethernet)
Connection Type	Bridge	Hardware Ethernet Switch	Ethernet	Multimedia over Coax (MOCA)	Multimedia over Coax (MOCA)	Wireless 802.11g Access Point	PPPoE
IP Address	192.168.1.1						10.16.90.12
Received Packets	75753	98970	191897	0	0	9255	0
Sent Packets	338867	298291	160540	0	0	41484	0
Received Bytes	22189273	18032559	20090307	0	0	1202580	0
Sent Bytes	20049358	33704739	35426513	0	0	11582549	0
Receive Errors	0	0	0	0	0	0	0
Receive Drops	0	0	2	0	0	0	0
Time Span	124:30:02	124:30:02	124:29:38			124:29:54	124:29:26

Close | Automatic Refresh On | Refresh

17. TECHNICAL SUPPORT INFORMATION

Contact your Internet service provider for technical support.

18. PRODUCT SPECIFICATIONS

System Requirements for 10/100 Base-T/Ethernet

- Pentium® or equivalent class machines or higher
- Microsoft Windows (Vista, XP, 2000, ME, NT 4.0, 98 SE) Macintosh® OS X, or Linux installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- 10/100 Base-T Network Interface Card (NIC)
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer Operating System CD-ROM

System Requirements for Wireless

- Pentium® or equivalent class machines or higher
- Microsoft Windows (Vista, XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer operating system CD-ROM
- IEEE 802.11b/g PC adapter

System Requirements for Coax

- Pentium® or equivalent class machines or higher
- Microsoft Windows (Vista, XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or later or
- Netscape Navigator 7.x or higher or
- Firefox 1.0.7 or later
- Computer operating system CD-ROM

LEDs

- Power
- WAN Coax
- WAN Ethernet
- Internet
- Wi-Fi Protected Setup
- USB
- LAN Ethernet 1 through 4
- LAN Coax
- Wireless

Connectors

- COAX
- USB
- Ethernet: Four 8-pin RJ-45 modular jacks
- WAN: 8-pin RJ-45 modular jack
- Power: Barrel connector

Power

- Power Supply: 120 VAC to 12 VDC wall-mount power supply

Dimensions

- Height: 1.7 in. (4.3 cm)
- Width: 9.0 in. (22.9 cm)
- Depth: 5.75 in. (14.6 cm)

Weight

- Approx. 1.25 lb (0.57 kg)

Environmental

- Relative Humidity: 5 to 95%, non-condensing
- Storage Temperature: -20 °C to 85 °C (-4 °F to 185 °F)
- Ambient Temperature: 23 °C (73 °F)

EMC/Safety/Regulatory Certifications

- FCC Part 15, Class B
- FCC Part 68
- ANSI/UL Standard 60950-1
- CAN/CSA C22.2 No. 60950-1

19. SOFTWARE LICENSE AGREEMENT

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY. THIS SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY INSTALLING AND OPERATING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE SOFTWARE AND HARDWARE TO WESTELL TECHNOLOGIES, INC. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND WESTELL TECHNOLOGIES, INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Licensor hereby grants to you, and you accept, a nonexclusive license to use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. The SOFTWARE may be used only in connection with the number of systems for which you have paid license fees as dictated in your support agreement. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.

You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

2. Licensor's Rights. You acknowledge and agree that the SOFTWARE and the User's Manual are proprietary products of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the SOFTWARE, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the SOFTWARE, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The fees paid by you under the support agreement are paid in consideration of the licenses granted under this License Agreement.

4. Term. This License Agreement is effective upon your opening of this package and shall continue until terminated. You may terminate this License Agreement at any time by returning the SOFTWARE and all copies thereof and extracts there from to Licensor. Licensor may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to return to Licensor the SOFTWARE and all copies and portions thereof.

5. Limitation of Liability. Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the SOFTWARE. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

6. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of Illinois. You submit to the jurisdiction of the state and federal courts of the state of Illinois and agree that venue is proper in those courts with regard to any litigation arising under this Agreement.

7. Costs of Litigation. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

8. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

9. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

20. PUBLICATION INFORMATION

Verizon FiOS Router Model 9100EM
Document Part Number 030-300554 Rev. C