D-Link DSL-2750B Wireless Gateway

User Guide

Version 1.0
December 6, 2011

Table of Contents

Product Overview

Product Description

The Verizon® D-Link® DSL-2750B Wireless Gateway provides reliable, high-speed, Internet access to your existing small office phone line and is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, the Gateway allows you to use the same phone line for simultaneous voice/fax communications and high-speed Internet access, eliminating the need for dedicated phone lines for voice and data needs. In addition, it supports a variety of networking interfaces along with the following optional features:

- Four 10/100 Ethernet Ports
- 802.11n wireless technology to provide the best wireless performance
- Advanced firewall features including parental control, access control, and content filtering
- Wi-Fi Protected Setup (WPS) Push Button/PIN setup
- UPnP Support
- USB port for sharing music/video/images using a thumb drive or external hard drive

Safety Instructions

- Never install any telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

WARNING: Risk of electric shock. Voltages up to 140 Vdc (with reference to ground) may be present on telecommunications circuits.

Networking Requirements

The following system specifications are required for optimum performance of the Router via 10/100 Ethernet or 802.11n/g wireless.

ETHERNET:

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (7,Vista®, XP, 2000, ME, NT 4.0, 98 SE) Mac 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® 6.0, Firefox® 3.0, Safari® 3.0 or Chrome 2.0 or higher

WIRELESS:

- Pentium® or equivalent class or higher
- Microsoft® Windows® (7,Vista®, XP, 2000) or Mac OS® X installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer® 6.0, Firefox® 3.0, Safari® 3.0 or Chrome 2.0 or higher
- Available IEEE 802.11n/g wireless clients

LED Indicators

This section explains the LED states and descriptions. LED indicators are used to verify the unit's operation and status.

1	**Power**	A solid green light indicates the unit is powered on. A red light indicates a malfunction.
2	**Ethernet (1-4)**	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.
3	**Wireless**	A solid green light indicates the wireless function is operating correctly. A flashing green light indicates wireless traffic is passing through the router.
4	**USB**	A solid green light indicates a good connection to a USB device. This light will blink during data transmission.
5	**DSL**	A solid light indicates the DSL is synchronized. A flashing LED indicates the modem is attempting to synchronize with the DSL provider.
6	**Internet**	A solid green light indicates that the modem has an IP address and is connected to the Internet. A red light indicates that the modem does not have an IP address or authentication has failed. No light indicates that an ADSL connection is not present or the modem is in bridge mode.

Ports/Buttons

The following chart displays the Router's connector types:

1	**DSL Port**	Connect to an active telephone line (RJ-11).
2	**LAN Ports (1-4)**	Connect Ethernet devices such as computers, switches, and hubs.
3	**USB Port**	Connect a USB thumb drive or external hard drive and share files with users on your network.
4	**WLAN Button**	Pressing this button to turn the Wireless feature on or off.
5	**Reset Button**	Pressing the Reset button for 10 seconds restores the modem to its original factory default settings.
6	**ON/OFF**	Press this button to turn the unit on or off.
7	**Power Receptor**	Receptor for the supplied power adapter.
8	**WPS Button**	Press the WPS button located on the side to add your device to an existing network or to create a new network.

This section will explain how to configure your computers to connect to the gateway, configure the gateway to connect to the Internet, and set up your wireless clients.

DSL Filters/Microfilters

ADSL signals must be blocked from reaching each telephone, answering machine, fax machine, or any similar conventional device. Failure to do so may degrade telephone voice quality and ADSL performance.

Install a microfilter if you desire to use the DSL-equipped line jack for telephone, answering machine, fax machine or other telephone device connections. Microfilter installation requires no tools or telephone rewiring. Just unplug the telephone device from the baseboard or wall mount and plug in a microfilter and then plug in the telephone device.

You can purchase microfilters from your local electronics retailer, or contact the original provider of your DSL equipment.

Configure your Computer

Windows® 7/Vista®/XP/2000

Follow the steps below to configure your computer to automatically receive its IP settings from the Gateway:

1. Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center.**

   Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**

   Windows® XP - Click on **Start > Control Panel > Network Connections.**

   Windows® 2000 - From the desktop, right-click **My Network Places > Properties.**

2. Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties.**

3. Highlight **Internet Protocol (TCP/IP)** and click **Properties.**

4. In the Internet Protocol (TCP/IP) Properties dialog box, click on the radio buttons labeled **Obtain an IP address automatically** and **Obtain DNS server address automatically.**

5. Click **OK** twice to save your settings.

Mac OS® X

Below are instructions for configuring your Mac OS® X operating system

1. In the Mac OS X Dock, click on the **System Preferences** icon.
2. Under **Internet & Network**, click **Network**. In the **Show** menu, select **Built-in Ethernet** or Ethernet (Depending on your Mac OS version.)
3. Click the **TCP/IP** tab.
4. In the Configure menu, select **Using DHCP**.
5. Click **Apply Now and Save** if your computer prompts you to save changes.

If you want to assign a static IP address, please use the settings below:

- Your PC's TCP/IP address: 192.168.1.x (where "x" is any number between 2 and 254)
- The Default Gateway's IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- DNS server:192.168.1.1 (same IP as the Gateway) or supplied by Verizon

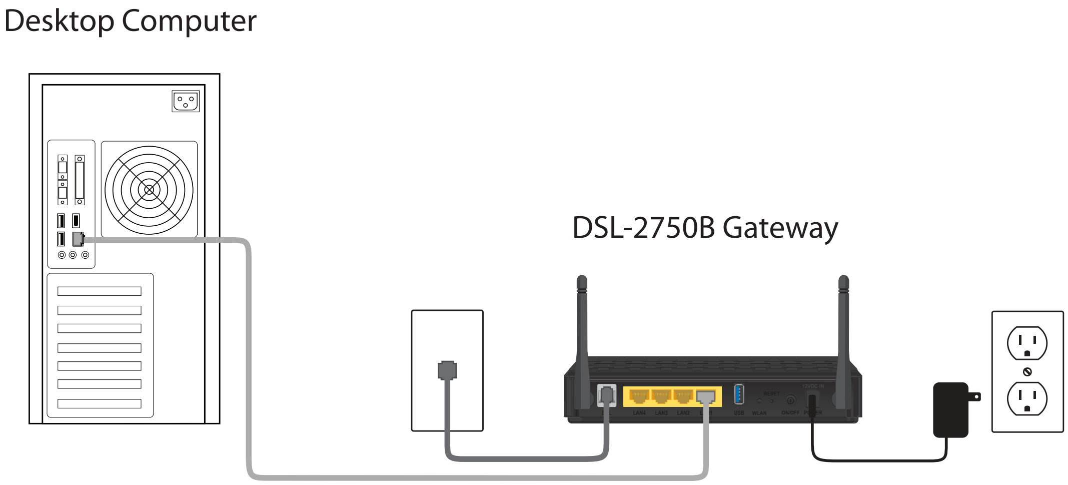
Connect your Gateway

1. Connect an RJ-11 (phone) cable from your wall phone jack to the DSL port on the back of the DSL-2750B gateway.

2. Connect an Ethernet cable from the LAN1 port on the back of the DSL-2750B to the Ethernet port on your computer.

3. Connect the supplied power adapter into the power receptor on the back of the DSL-2750B gateway to a power outlet or a surge protector (recommended).

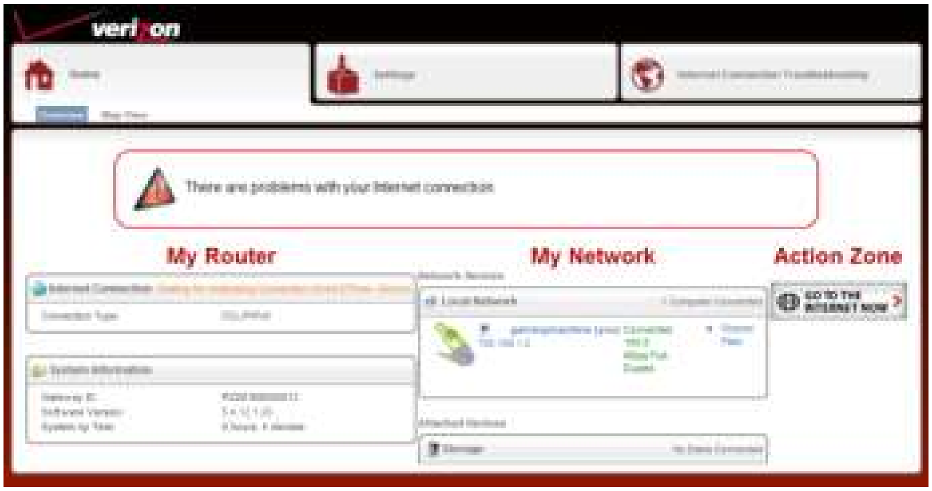
4. Once you connect the power adapter, press the ON/OFF button on the back of the gateway to turn the unit on.



Web-based Configuration Utility

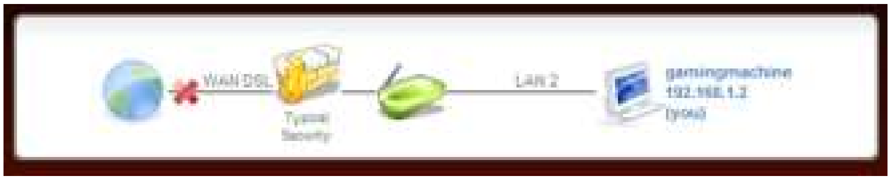
To log into the gateway, follow the steps below:

1. Launch your web browser such as Internet Explorer.
2. In the address bar enter **http://192.168.1.1** and press **Enter**.
3. The Home page will appear. The **Overview** screen displays the gateway status summary in one convenient location. The user can quickly and efficiently view important details of the connection status and hardware peripherals, as well as the status of different services. If you click any other link/tab, you will be asked to log in.

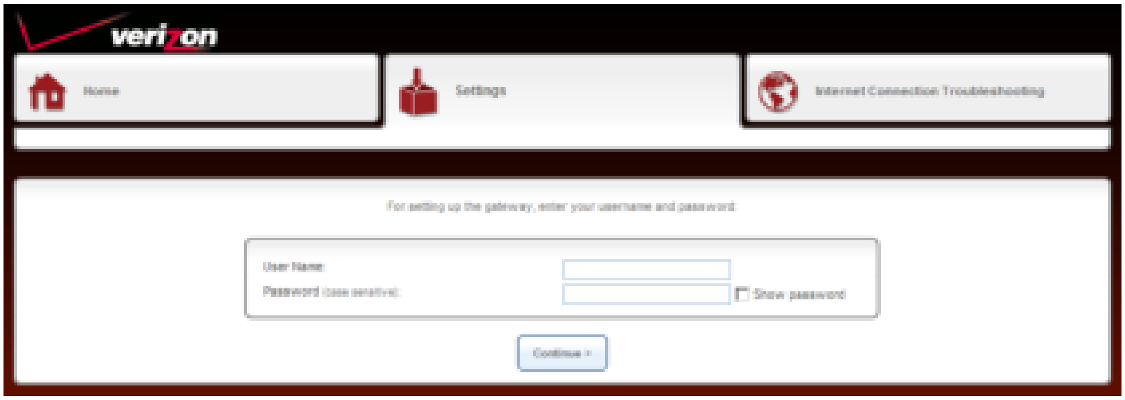


There are problems with your Internet connection

Map View depicts the various network elements, such as the Internet connection, firewall, gateway, internal network interface (Ethernet, USB, and Wireless), and local network computers and peripherals visually.



4. Click **Settings** to configure your router. Once the login screen appears, enter **Admin** next to *Username* and then enter your password (refer to “login password” on the label located on the bottom of the Gateway). Click **Continue**.



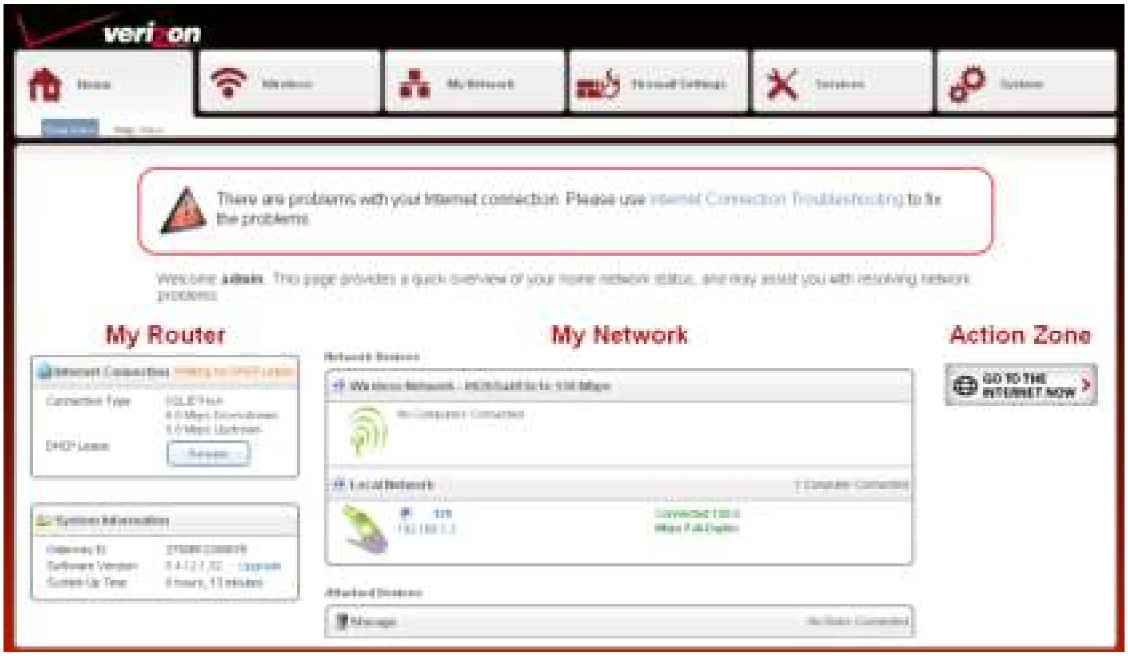
For setting up the gateway, enter your username and password.

User Name:

Password (case sensitive): □ Show password

The **Home** > **Overview** screen will appear. This screen gives you an overview of your Gateway including the Internet connection status, system information, local network information, and storage status.

When the router is configured with DHCP, you will be able to Release and Renew your WAN IP Address with the buttons located here.



There are problems with your Internet connection. Please use Internet Connection Troubleshooting to fix the problems.

Welcome **admin**. This page provides a quick overview of your home network status, and may assist you with resolving network problems.

Connection Type [illegible]
6.0 Mbps Downstream
[illegible] Mbps Upstream
DHCP Lease

Gateway ID [illegible]
Software Version [illegible]
System Up Time [illegible] hours, 13 minutes

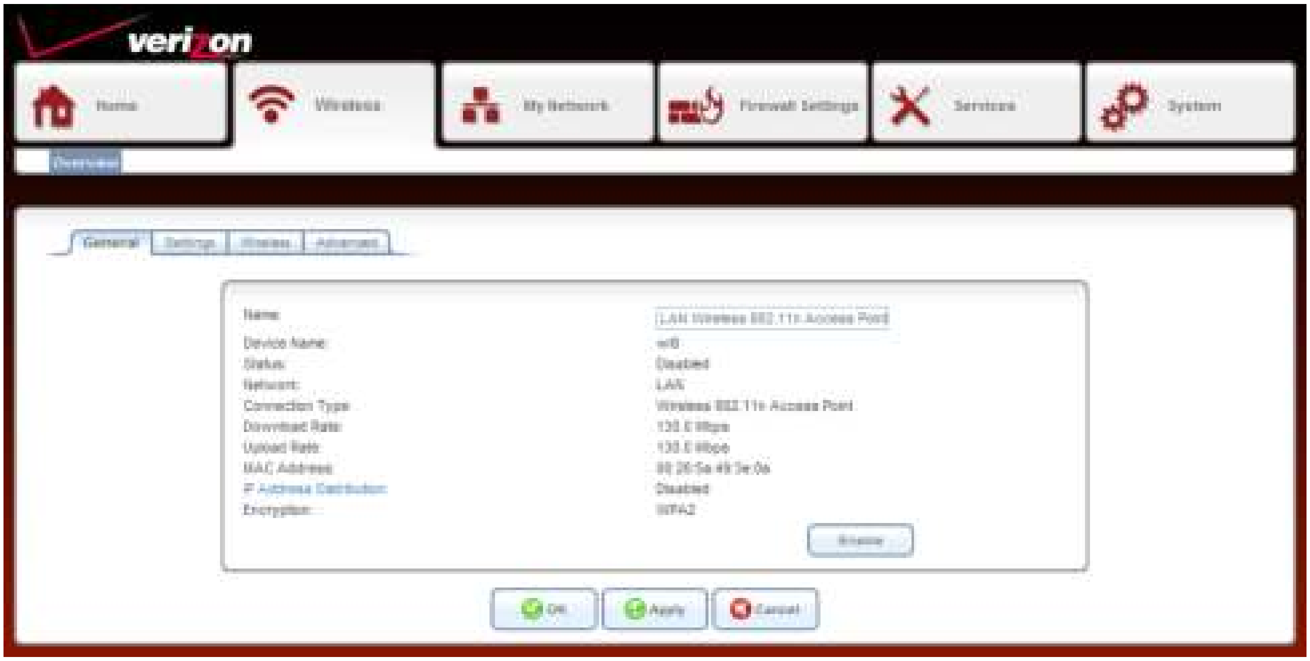
No Computer Connected

1 Computer Connected

No Disks Connected

Overview

The **Wireless > Overview** screen displays the Gateway’s current wireless settings.

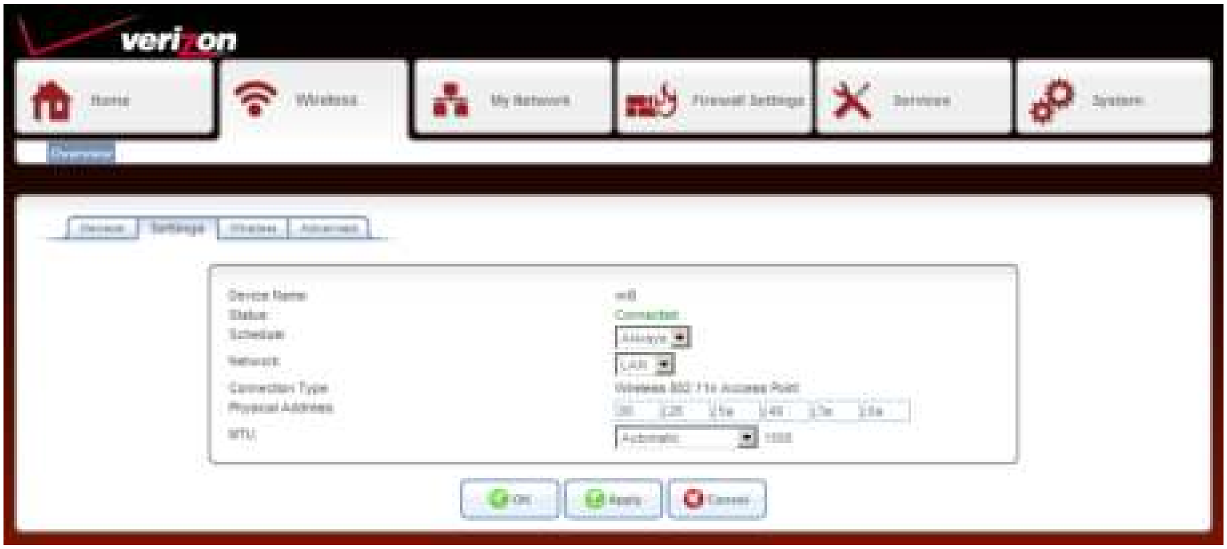


Name:	LAN Wireless 802.11n Access Point
Device Name:	wl0
Status:	Disabled
Network:	LAN
Connection Type:	Wireless 802.11n Access Point
Download Rate:	130.0 Mbps
Upload Rate:	130.0 Mbps
MAC Address:	00:26:5a:49:3e:0a
IP Address Distribution:	Disabled
Encryption:	WPA2

Enable Button: Click the Enable button to turn on the wireless function.

Settings

The **Wireless > Settings** screen allows you to change the Gateway's wireless settings.



Device Name: wl0
Status: Connected
Schedule: Always
Network: LAN
Connection Type: Wireless 802.11n Access Point
Physical Address: 00 : 26 : 5a : 48 : 7e : 8a
MTU: Automatic 1500

Device Name: Displays the name of the Interface.

Status: Displays the current connection state.

Schedule: Select a time frame from the drop-down menu to have the wireless function active.

Network: LAN is selected.

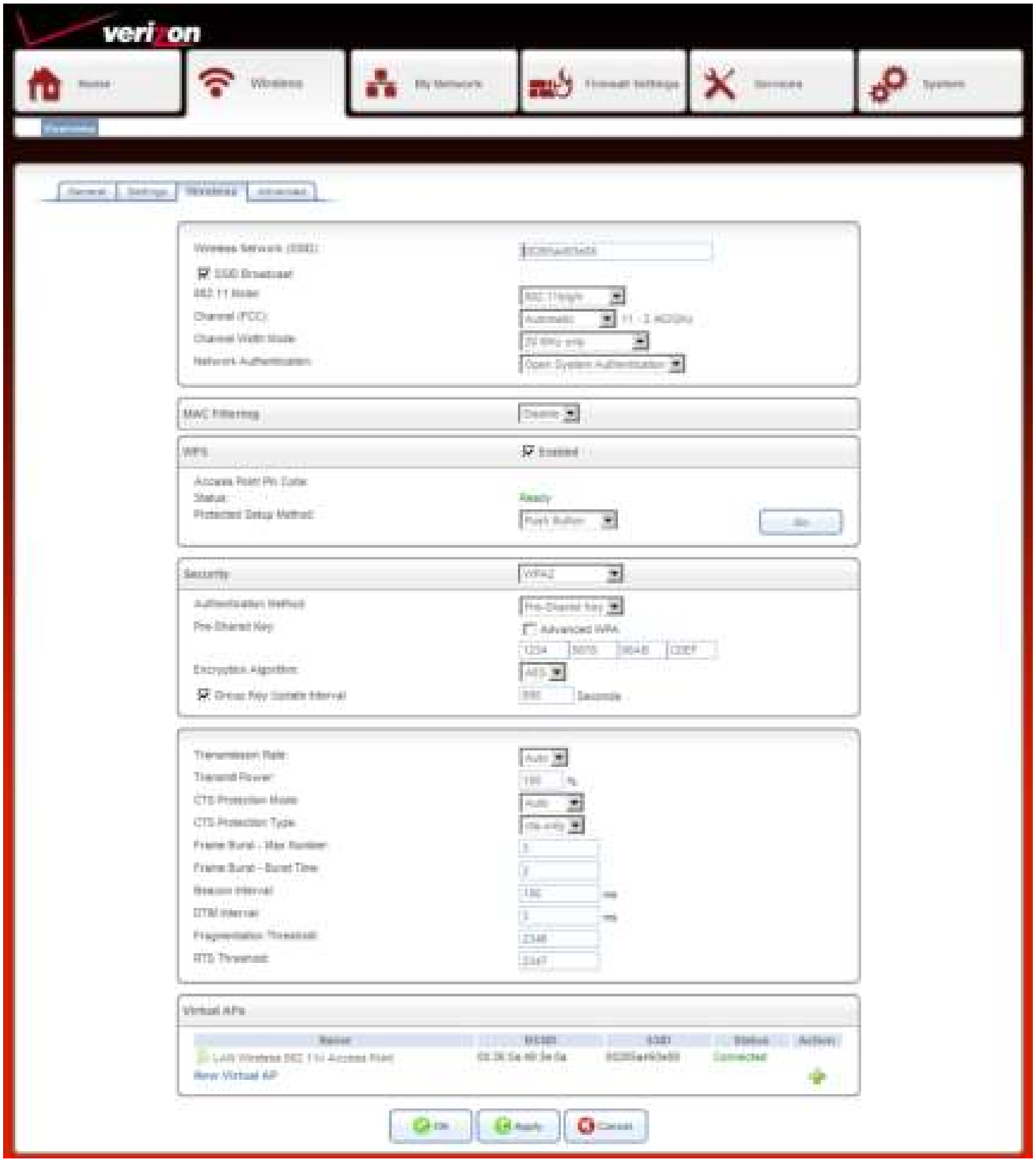
Connection Type: Displays the wireless mode the Gateway is set to.

Physical Address: Displays the MAC address of the Gateway (wireless side).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

Wireless

The **Wireless > Wireless** screen allows you to change the Gateway's wireless network settings.



Wireless Network (SSID): [illegible]

☑ SSID Broadcast

802.11 Mode: 802.11b/g/n

Channel (FCC): Automatic 11 - 2.462GHz

Channel Width Mode: 20 MHz only

Network Authentication: Open System Authentication

MAC Filtering: Disable

WPS ☑ Enabled

Access Point Pin Code

Status: Ready

Protected Setup Method: Push Button Go

Security: WPA2

Authentication Method: Pre-Shared Key

Pre-Shared Key: □ Advanced WPA

1234 5678 90AB CDEF

Encryption Algorithm: AES

☑ Group Key Update Interval 900 Seconds

Transmission Rate: Auto

Transmit Power: 100 %

CTS Protection Mode: Auto

CTS Protection Type: cts-only

Frame Burst - Max Number: 3

Frame Burst - Burst Time: 2

Beacon Interval: 100 ms

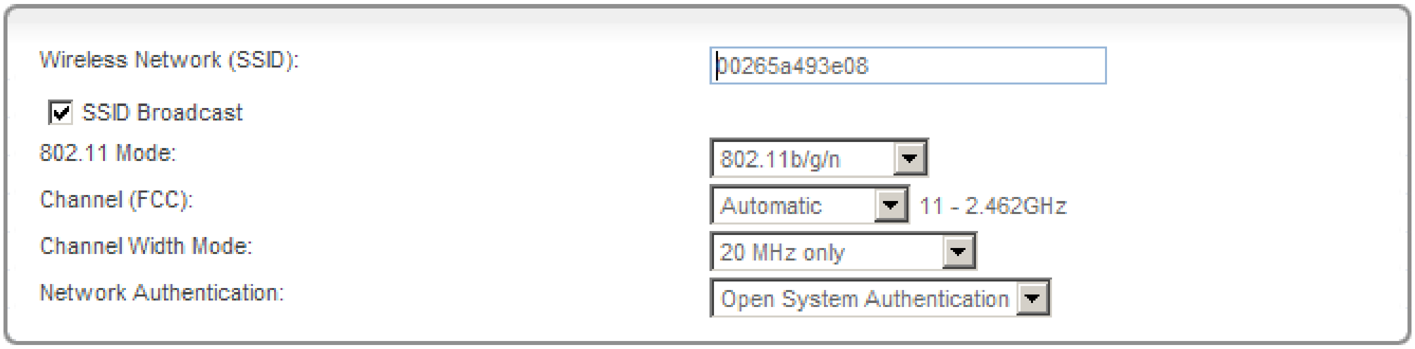
DTIM Interval: 1 ms

Fragmentation Threshold: 2346

RTS Threshold: 2347

Virtual APs

Name	BSSID	SSID	Status	Action
LAN Wireless 802.11n Access Point	[illegible]	[illegible]	Connected	
New Virtual AP				



Wireless Network (SSID): 00265a493e08

☑ SSID Broadcast

802.11 Mode: 802.11b/g/n

Channel (FCC): Automatic 11 - 2.462GHz

Channel Width Mode: 20 MHz only

Network Authentication: Open System Authentication

Wireless Network (SSID): Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive. For security reasons, do not choose a name with personal information.

SSID Broadcast: When this box is checked, the SSID (name of your wireless network) will broadcast. Wireless clients within range of your Gateway will be able to see your network. For added security, you may uncheck this box but will have to manually enter the SSID on your wireless clients.

802.11 Mode: Select the type of wireless clients that will connect to your wireless network.
802.11b/g Mixed - Select if you are using a mix of 802.11b and 11g wireless clients.
802.11g Only - Select if all of your wireless clients are 802.11g.
802.11b Only - Select if all of your wireless clients are 802.11b.
802.11b/g/n - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.
802.11n Only - Select only if all of your wireless clients are 802.11n.
802.11g/n - Select if you are using a mix of 802.11n and 11g wireless clients.

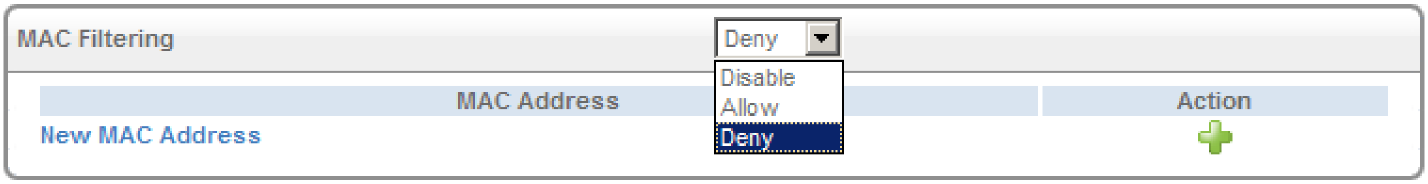
Channel (FCC): Select the wireless channel. It is strongly recommended to select **Automatic**.

Channel Width Mode: Select the Channel Width:
20MHz - This is the default setting. Select if you are not using any 802.11n wireless clients.
20/40MHz (dynamic) - Select if you are using both 802.11n and non-802.11n wireless devices.
40MHz - Select if using only 802.11n wireless clients.

Network Authentication: Select the authentication mode from the drop-down. **Open System** is the default settings. When using WEP encryption, it is recommended to select **Shared Key**.

MAC Filtering

Use MAC (Media Access Control) Filtering to allow or deny wireless computers and devices by their MAC addresses from accessing the Network. You will need to manually add the MAC address of your wireless client you want to filter.



MAC Filtering: Deny

MAC Address	Action
New MAC Address	+

MAC Filtering: Select from the drop-down menu:

Disable - turn off MAC filtering.

Allow - Allows only the computers/devices you want from your network to access the Internet. All other computers will be blocked if not added.

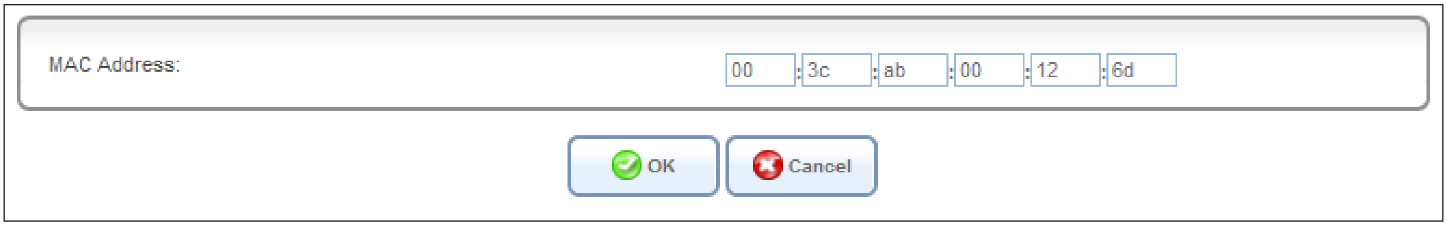
Deny - Blocks computers/devices you want from your network from accessing the Internet. All other computers will be allowed to connect.

Action/New MAC Address: Click the green **+** icon or **New MAC Address** to add your wireless clients. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

Add New MAC Address

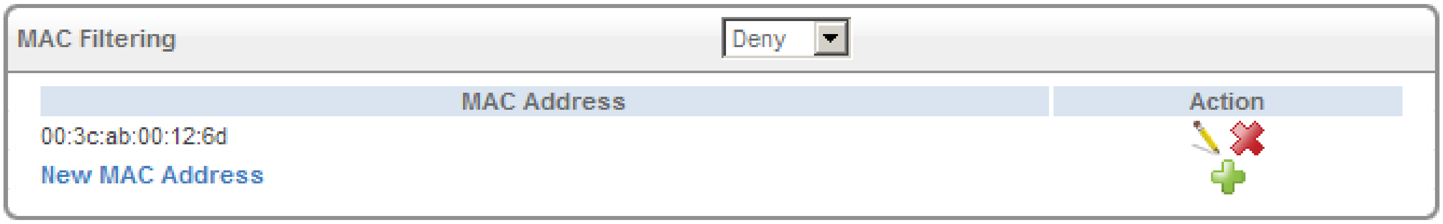
Step 1: Click the green + icon under *Action*.

Step 2: Enter the MAC Address of your computer or device and click **OK**.



MAC Address: 00 : 3c : ab : 00 : 12 : 6d

Step 3: Your newly added device will now be displayed in the list. Click the red X to remove the device from the list. To add more, repeat steps 1 and 2.



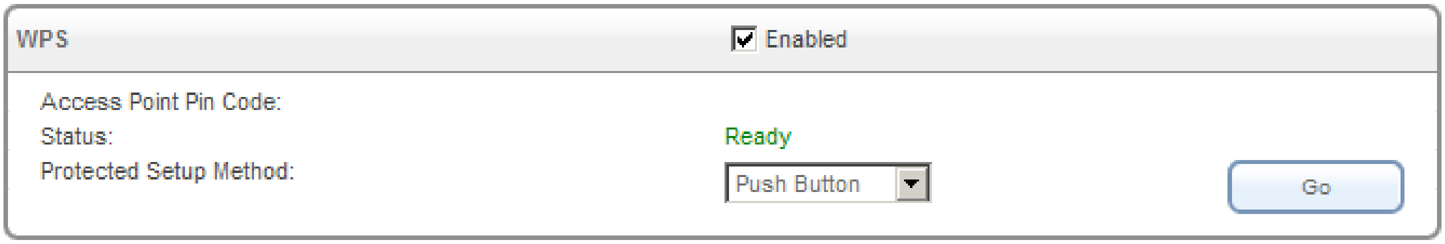
MAC Filtering: Deny

MAC Address	Action
00:3c:ab:00:12:6d	✎ ✖
New MAC Address	+

WPS

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy, as pressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin-Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

Push Button


WPS ☑ Enabled

Access Point Pin Code:

Status: Ready

Protected Setup Method: Push Button

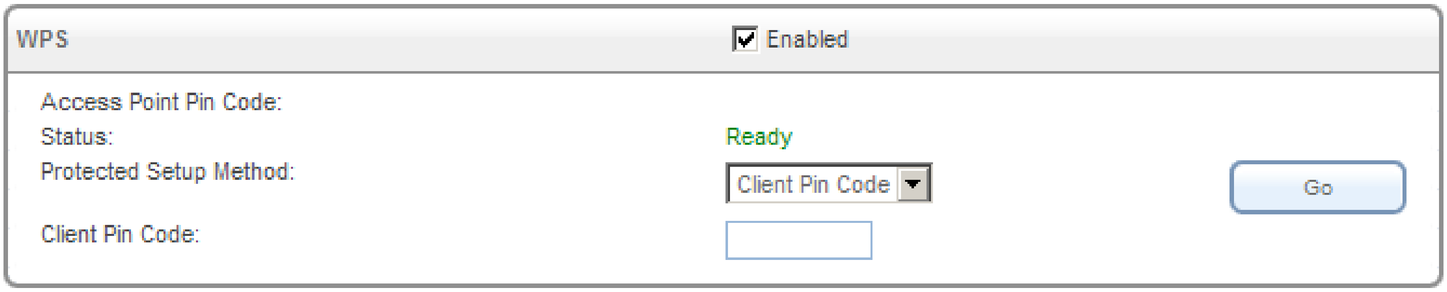
Step 1: Select **Push Button** from the drop-down and then click the **Go** button to start the WPS process.

Step 2: Within 2 minutes, press the WPS button on your wireless client. Some clients may require you to launch its software utility and click a WPS button. Please refer to your wireless client’s user guide for more information.

Step 3: Allow 1-2 minutes for the devices to communicate. Once complete your client will connect to the gateway.

Client PIN Code

A PIN is a unique number that can be used to add the router to an existing network or to create a new network. You will need to get the PIN number from one of your wireless clients. Please refer to your wireless client’s user guide for more information.


WPS ☑ Enabled

Access Point Pin Code:

Status: Ready

Protected Setup Method: Client Pin Code

Client Pin Code:

Step 1: From your wireless client, write down the PIN and activate/start the WPS process.

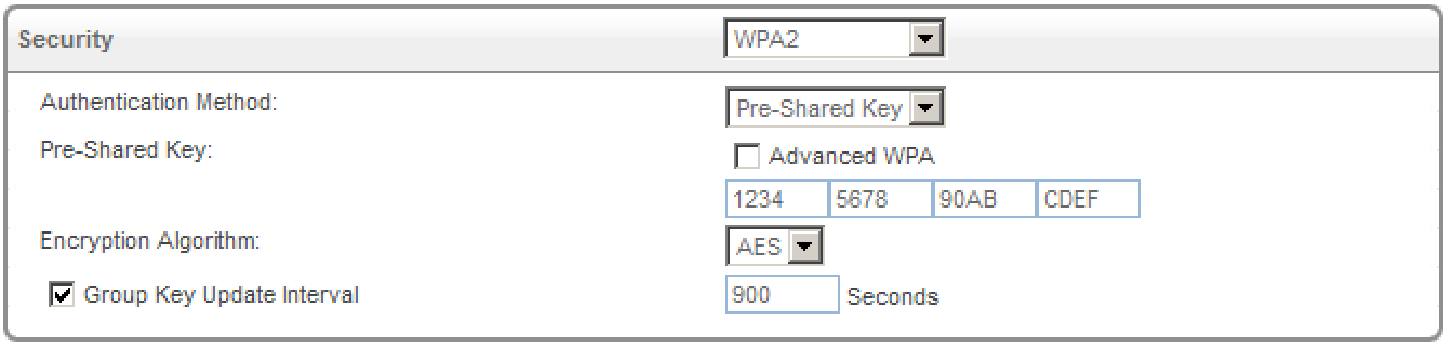
Step 2: Within 2 minutes from the Gateway, select **Client Pin Code** from the drop-down, enter the PIN number in the box, and then click the **Go** button.

Step 3: Allow 1-2 minutes for the devices to communicate. Once complete your client will connect to the gateway.

WPA/WPA2 Security

This section will allow you to secure your wireless network using WEP, WPA, or WPA2 encryption. When using these options, you must disable WPS. Refer to the previous page and uncheck the WPS box.

The default setting and recommended level of security is WPA2.



Security: WPA2

Authentication Method: Pre-Shared Key

Pre-Shared Key: □ Advanced WPA

1234 | 5678 | 90AB | CDEF

Encryption Algorithm: AES

☑ Group Key Update Interval: 900 Seconds

Authentication Method: Select **WPA** or **WPA2**.

Advanced WPA: Check this box to change the pre-shared key (passphrase).

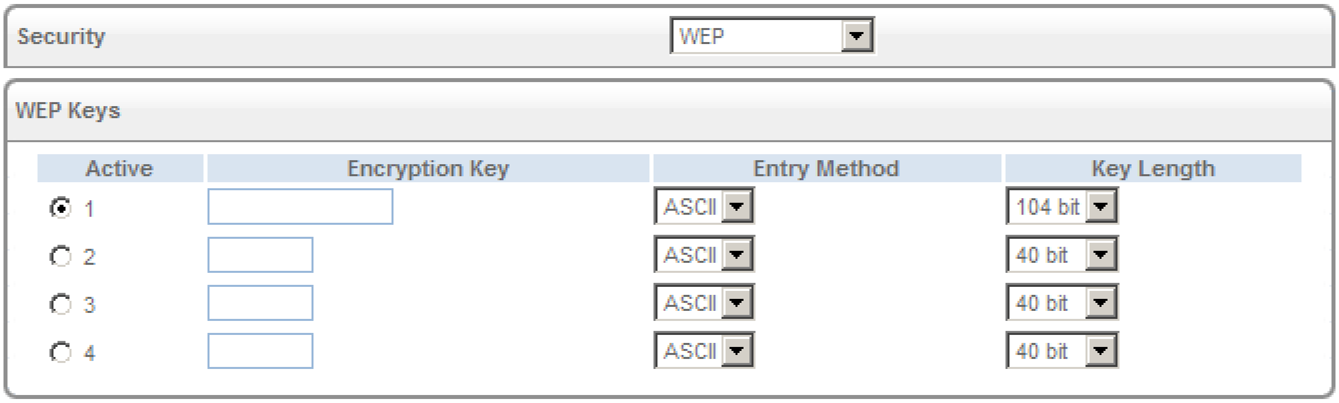
Pre-Shared Key: Displays the current WPA/WPA2 passphrase.

Encryption Algorithm: Select **AES**, **TKIP**, or **AES and TKIP**.

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

WEP Security

WEP is an older, less-secure encryption option. It is strongly recommended to use WPA or WPA2.



Security: WEP

WEP Keys

Active	Encryption Key	Entry Method	Key Length
● 1		ASCII	104 bit
○ 2		ASCII	40 bit
○ 3		ASCII	40 bit
○ 4		ASCII	40 bit

Authentication Method: Select **WEP** from the drop-down menu.

WEP Keys: You may enter up to 4 different keys. Select the key you want to use.

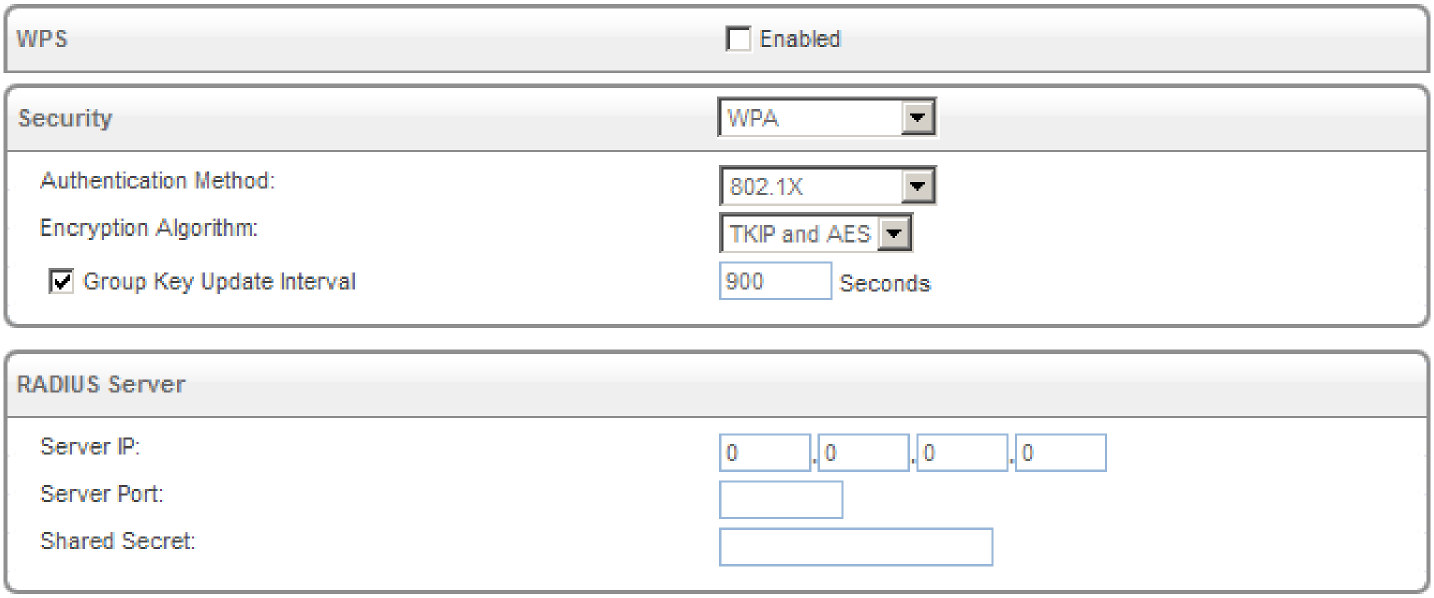
Encryption Key: Enter a WEP key.

Entry Method: Select the type of key from the drop-down menu.
Hex - letters A-F and numbers 0-9 are valid.
ASCII - all letters and numbers are valid.

Key Length: Select the level of encryption (40 or 104-bit).

802.1x Authentication

This section will allow you to secure your wireless network using 802.1x authentication. When using this option, you must disable WPS.



WPS ☐ Enabled

Security: WPA

Authentication Method: 802.1X

Encryption Algorithm: TKIP and AES

☑ Group Key Update Interval: 900 Seconds

RADIUS Server

Server IP: 0 . 0 . 0 . 0

Server Port:

Shared Secret:

Authentication Method: Select **802.1x WEP**, **WPA** or **WPA2**.

Encryption Method: If you selected WPA or WPA2, you will need to select 802.1x from the drop-down menu.

Encryption Algorithm: If you selected WPA or WPA2, Select the type of encryption you want to use - **AES**, **TKIP**, or **AES and TKIP**.

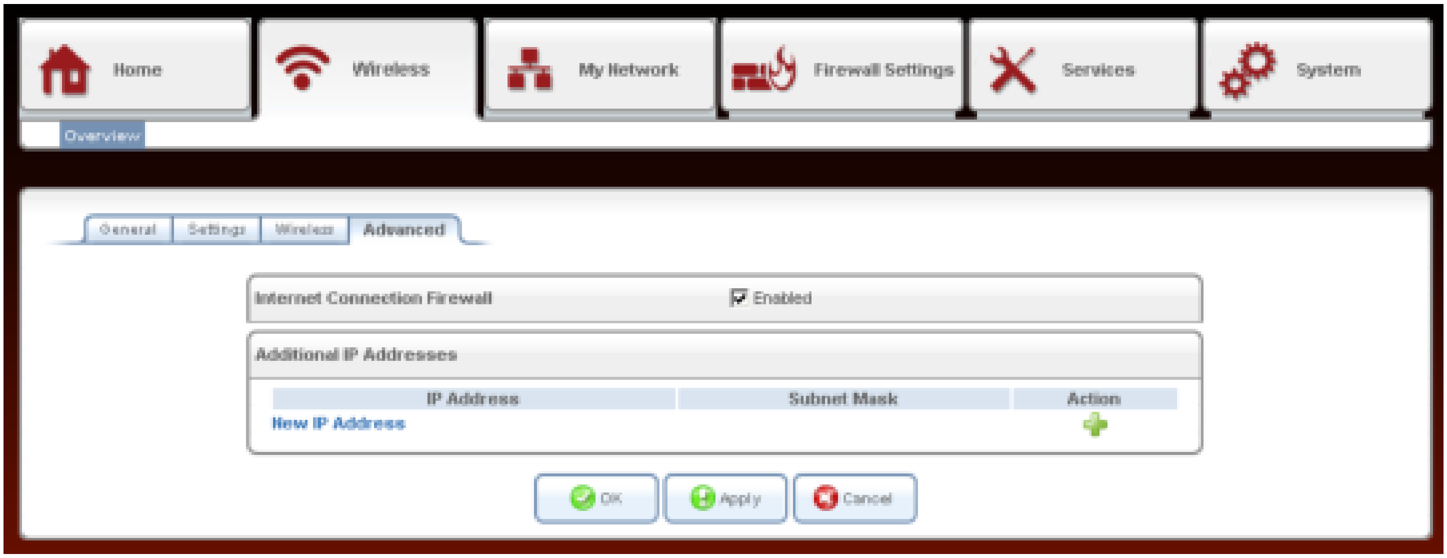
Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Server IP: Enter the IP address of the RADIUS server.

Server Port: Enter the port you want to use.

Shared Secret: Enter the Shared Secret passphrase.

Advanced



Internet Connection Firewall ☑ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		+

Internet Connection Firewall: Check the Enable box to enable the firewall feature for your wireless computers/devices.

New IP Address: Click to add a new device.

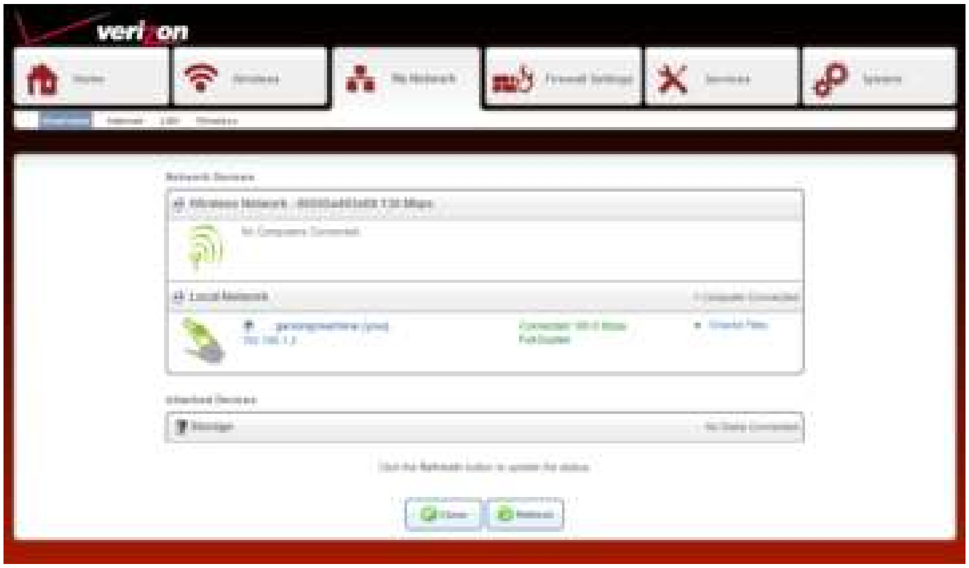
IP Address: The IP address of the computer or device.

Subnet Mask: The subnet mask of the computer or device.

Action: Click the green + sign to add a computer or device, or click the red X to delete the computer or device.

My Network
Overview

The **My Network > Overview** screen displays your network devices on your network and any attached storage devices.



Wireless Network: This section will display any wireless device connected to your Gateway.

Local Network: This section will display any Ethernet device connected to your Gateway.

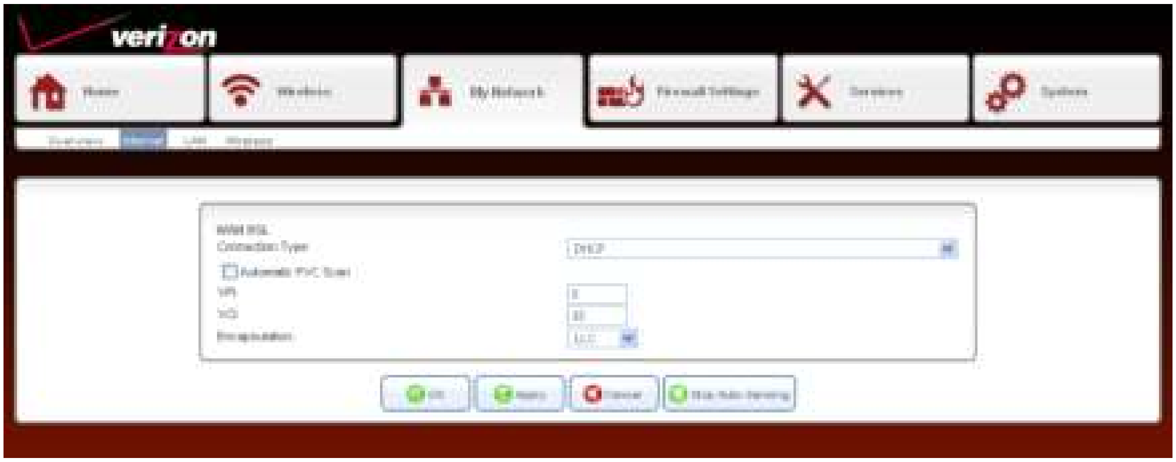
You can click the computer name, IP address or "Shared Files" to access any shares on that computer.

Attached Devices: This section will display if any USB storage devices (thumb drive/external hard drive) are connected to your Gateway.

Internet

The **My Network > Internet** screen allows you to change your Internet settings. This section should only be configured by Verizon technicians.

Auto-Sense will automatically detect your Internet settings. It is not recommended to manually make changes to your Internet settings. However, if you choose to do so, you must disable Auto-Sense by clicking the Stop Auto-Sense button from this page. Note: Once you disable Auto-Sense, you can only re-enable it by restoring factory settings.



WAN DSL

Connection Type: DHCP

□ Automatic PVC Scan

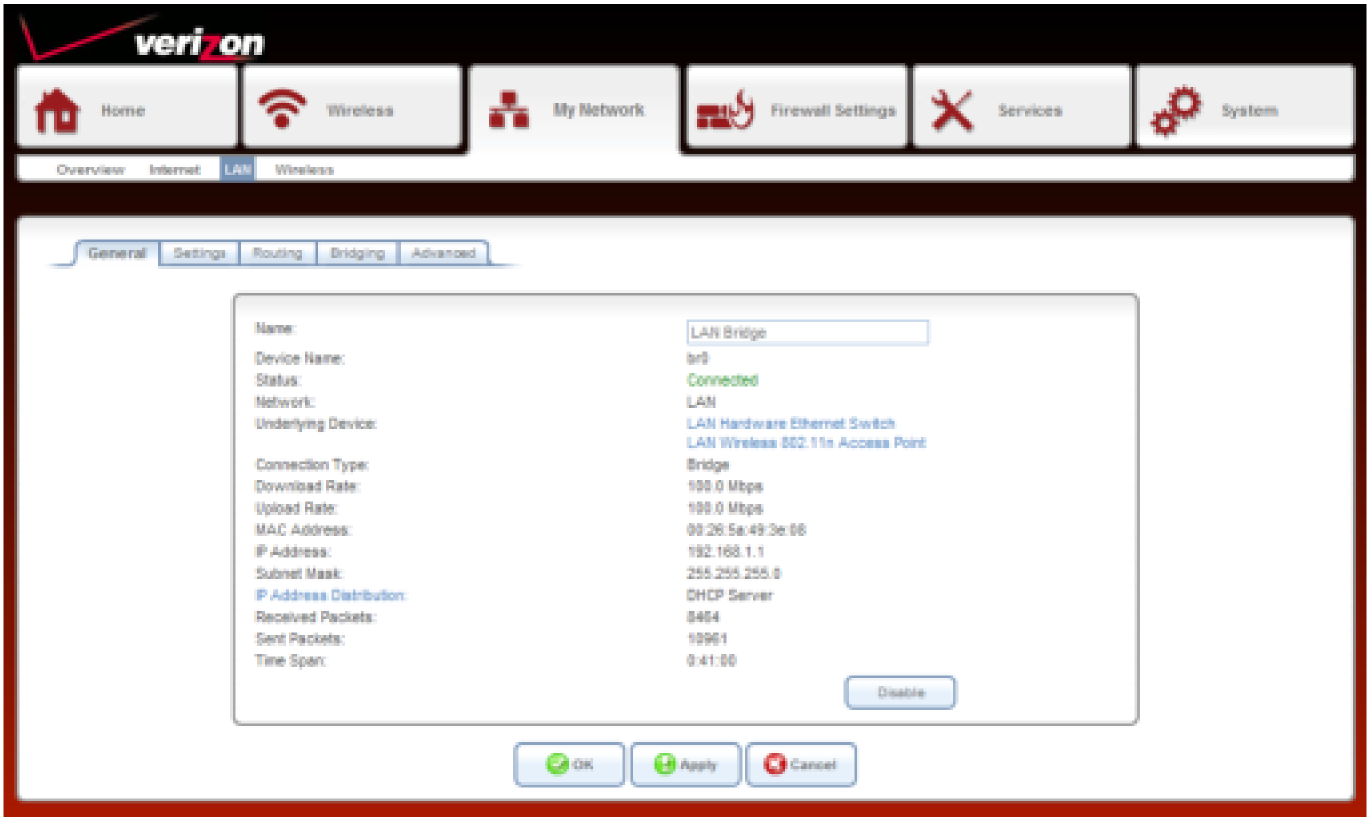
VPI: 0

VCI: 35

Encapsulation: LLC

LAN
General

The **My Network > LAN** screen displays a summary of the Gateway's local (router) settings.



Name:	LAN Bridge
Device Name:	br0
Status:	Connected
Network:	LAN
Underlying Device:	LAN Hardware Ethernet Switch LAN Wireless 802.11n Access Point
Connection Type:	Bridge
Download Rate:	100.0 Mbps
Upload Rate:	100.0 Mbps
MAC Address:	00:26:5a:49:3e:08
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IP Address Distribution:	DHCP Server
Received Packets:	8464
Sent Packets:	10961
Time Span:	0:41:00

Name: The name of the LAN side of the Gateway.

Device Name: Displays the name of the Interface.

Status: The current status of the LAN side of the Gateway.

Underlying Device: You may click **LAN Hardware Ethernet Switch** or **LAN Wireless 802.11n Access Point** to configure their settings.

Connection Type: Displays the connection type.

Download Rate: Displays the Ethernet download speed.

Upload Rate: Displays the Ethernet upload speed.

MAC Address: The MAC address of the LAN side of the Gateway.

IP Address: The IP address of the LAN side of the Gateway.

Subnet Mask: The subnet mask of the Gateway.

IP Address Distribution: Click to change the DHCP settings.

Received Packets: Amount of packets received.

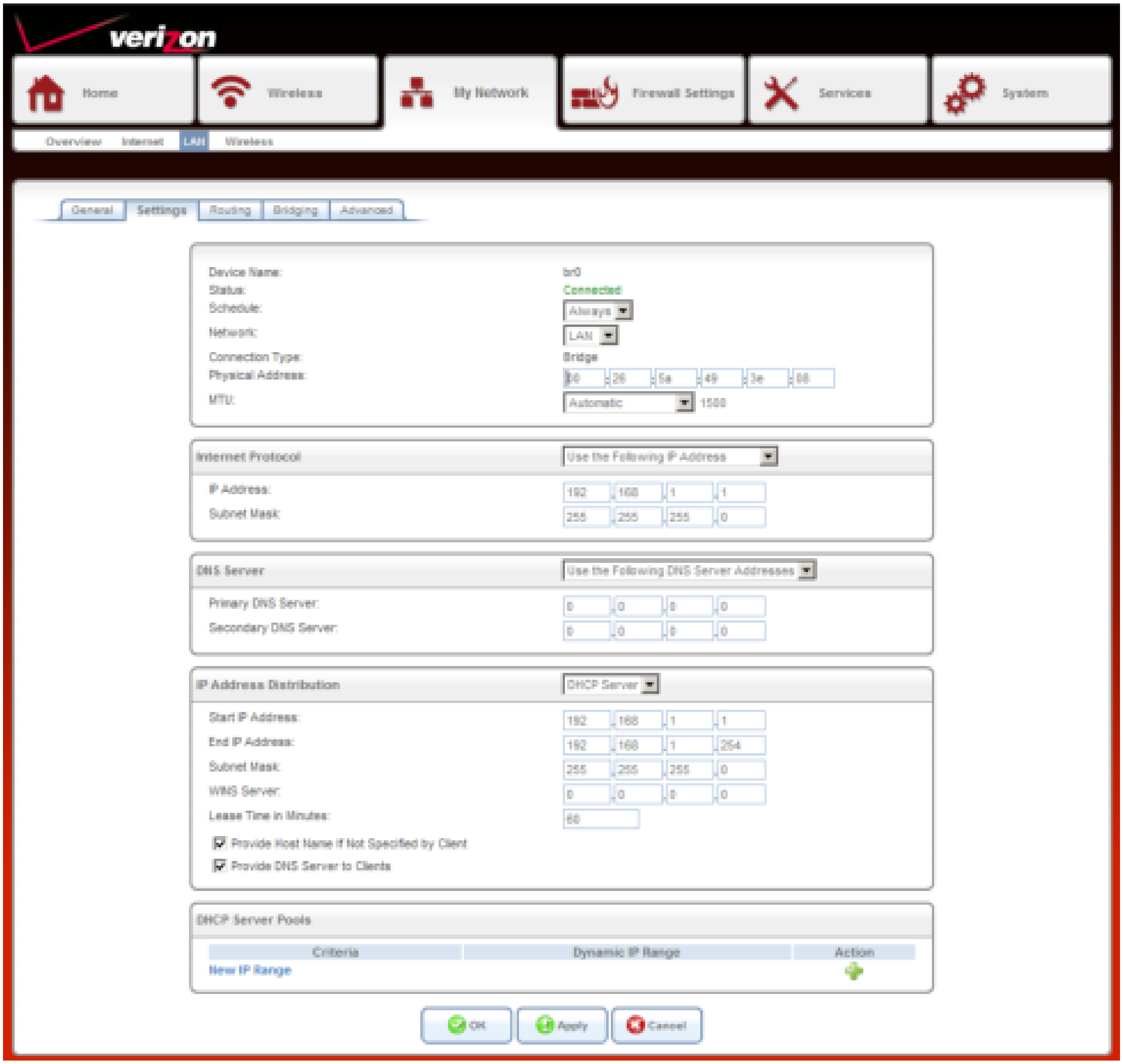
Sent Packets: Amount of packets sent.

Time Span: Displays the time connected.

Disable Button: Click to disable the use of the Ethernet ports (LAN) on your Gateway.

Settings

This section allows you to change the network settings (LAN) of your Gateway.



Device Name:	br0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Bridge
Physical Address:	00 : 26 : 5a : 49 : 3e : 08
MTU:	Automatic 1500

Internet Protocol Use the Following IP Address

IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255 . 255 . 255 . 0

DNS Server Use the Following DNS Server Addresses

Primary DNS Server:	0 . 0 . 0 . 0
Secondary DNS Server:	0 . 0 . 0 . 0

IP Address Distribution DHCP Server

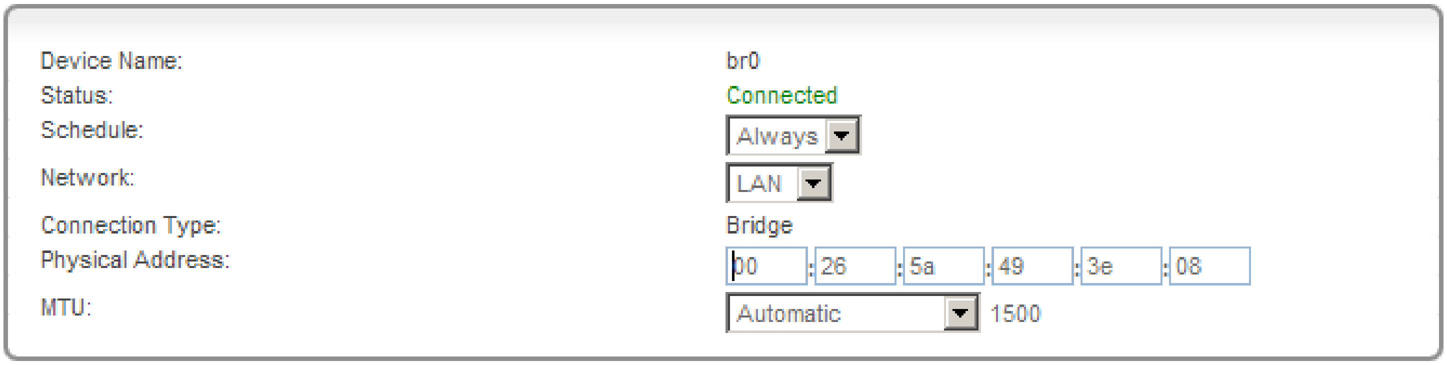
Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 254
Subnet Mask:	255 . 255 . 255 . 0
WINS Server:	0 . 0 . 0 . 0
Lease Time in Minutes:	60

☑ Provide Host Name If Not Specified by Client

☑ Provide DNS Server to Clients

DHCP Server Pools

Criteria	Dynamic IP Range	Action
New IP Range		✚



Device Name:	br0
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Bridge
Physical Address:	00 : 26 : 5a : 49 : 3e : 08
MTU:	Automatic 1500

Device Name: Displays the name of the Interface.

Status: Displays the current connection state.

Schedule: Select a time frame from the drop-down menu to have your wired devices able to connect to the Internet.

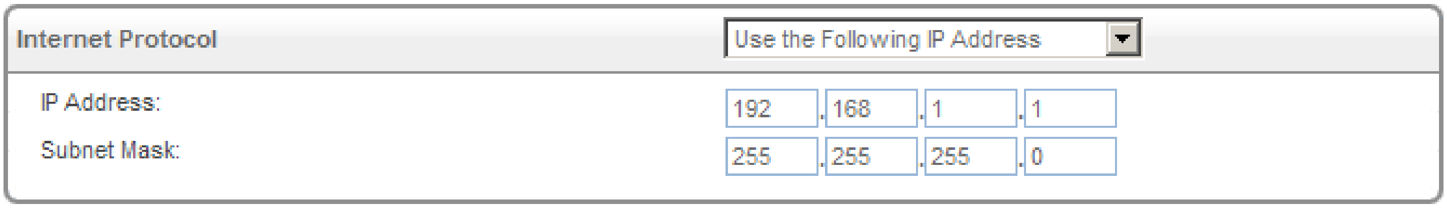
Network: LAN is selected.

Connection Type: Displays the connection type the Gateway is set to.

Physical Address: Displays the MAC address of the Gateway (LAN side).

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

Internet Protocol



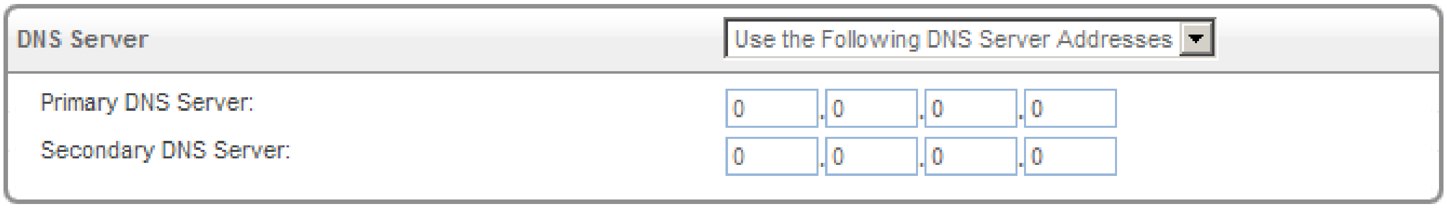
Internet Protocol	Use the Following IP Address
IP Address:	192 . 168 . 1 . 1
Subnet Mask:	255 . 255 . 255 . 0

Internet Protocol: Select **Use the Following IP Address** from the drop-down menu.

IP Address: If you want to change the Gateway IP address, enter it here. If you do change this IP address, you must use it in the future to log into the Gateway.

Subnet Mask: Enter the Subnet Mask of your local network.

DNS Server



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

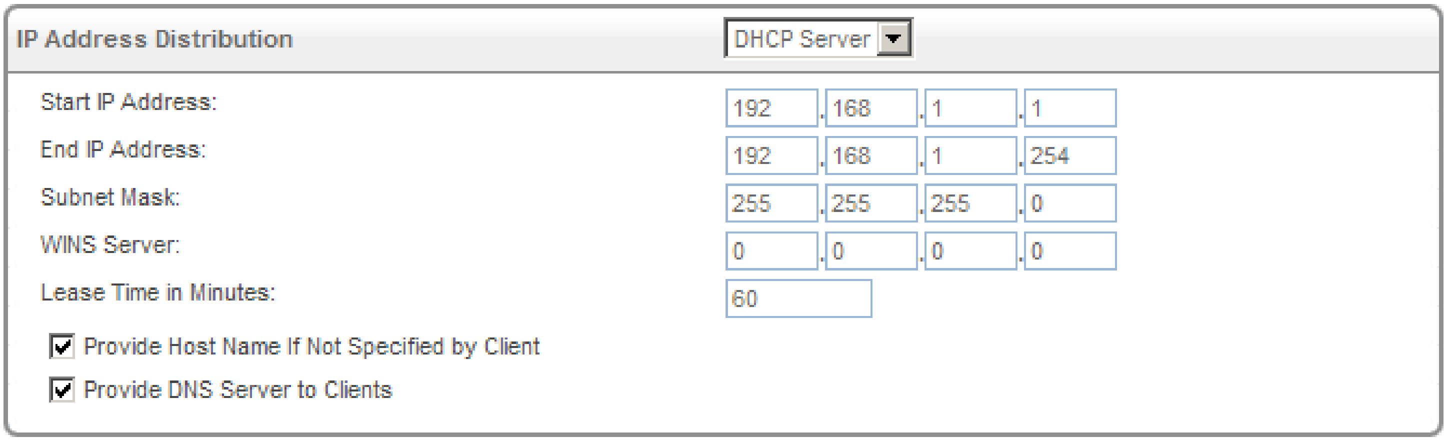
DNS Server: Select **Use the Following DNS Server Addresses** from the drop-down menu.

Primary DNS Server: Enter the IP Address of your primary DNS server.

Secondary DNS Server: Enter the IP Address of your secondary DNS server.

IP Address Distribution (DHCP)

DHCP stands for Dynamic Host Control Protocol. The Gateway has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers /devices on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the Gateway. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer/device. You must specify the starting and ending address of the IP address pool (refer to the next page).



IP Address Distribution: DHCP Server

Start IP Address:	192 . 168 . 1 . 1
End IP Address:	192 . 168 . 1 . 254
Subnet Mask:	255 . 255 . 255 . 0
WINS Server:	0 . 0 . 0 . 0
Lease Time in Minutes:	60

☑ Provide Host Name If Not Specified by Client

☑ Provide DNS Server to Clients

DNS Server: Select **DHCP Server** from the drop-down menu (default setting) if you want the Gateway to automatically assign your wired and wireless clients their network settings automatically. If you disable this function, you will have to statically assign the IP/network settings on your clients.

Start IP Address: Enter the starting IP address of the DHCP range.

End IP Address: Enter the end IP address of the DHCP range.

Subnet Mask: Enter the subnet mask of your local network.

WINS Server: Enter the IP address of your WINS server (if one).

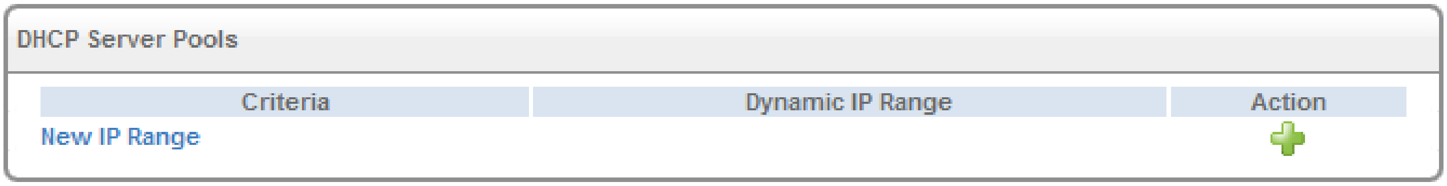
Lease Time in Minutes: Enter the DHCP lease time (in minutes).

Provide Host Name if Not Specified by Client: If the DHCP client does not have a host name, the Gateway will automatically assign one.

Provide DNS Server to Clients: Check this box if you want the Gateway to assign your clients the IP address(es) of the ISPs DNS servers.

DHCP Server Pools (DHCP Reservation)

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.



DHCP Server Pools

Criteria	Dynamic IP Range	Action
New IP Range		➕

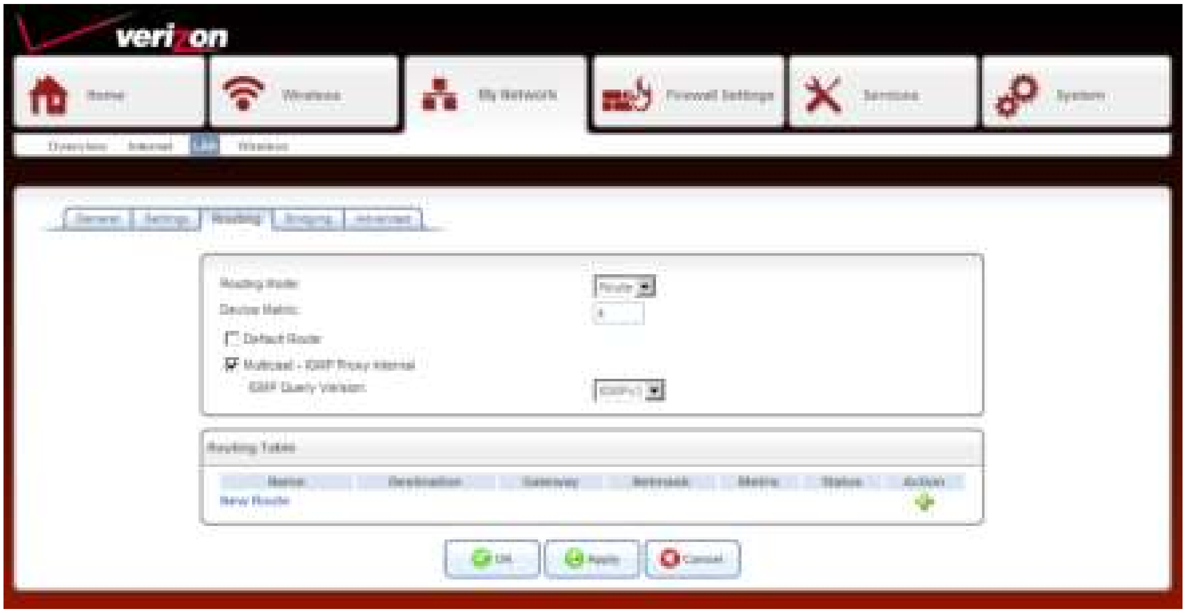
Criteria: Displays the current created server pool.

Dynamic IP Range: Displays the IP address range.

Action: Click the green + sign to add a new rule, click the pencil icon to edit, or click the red X to remove the rule.

New IP Range: Click to add a new entry.

Routing



Routing Mode: Route

Device Metric: 4

□ Default Route

☑ Multicast - IGMP Proxy Internal

IGMP Query Version: IGMPv3

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						+

Routing Mode: Select the routing mode from the drop-down menu.

Device Metric: Enter the metric value. The route metric is a value from 1 to 15 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

Default Route: Check this box to use the default route.

Multicast - IGMP Proxy Internal: This box is checked by default.

IGMP Query Version: Select the IGMP Query version from the drop-down menu.

Routing Table: Displays the entered routes.

Name: Displays the name of the route you created.

Destination: The IP address of the destination location.

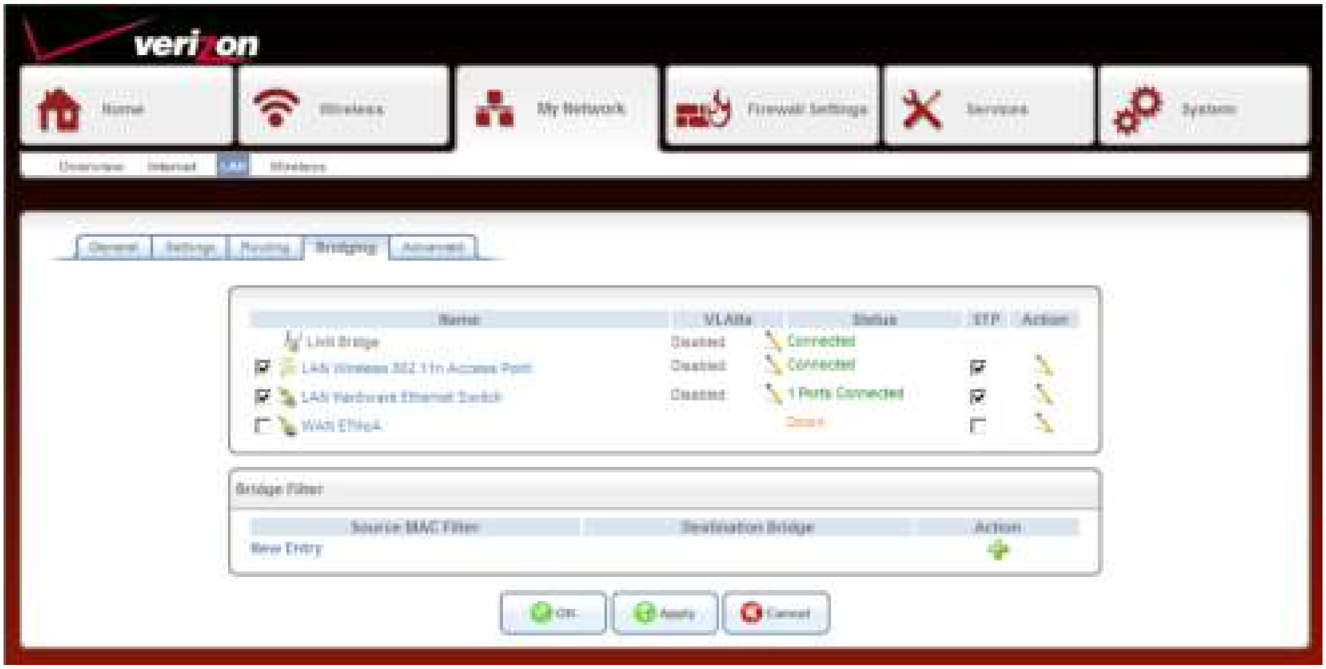
Gateway: The gateway IP address of the destination location.

Netmask: The netmask of the destination location.

Metric: The metric value assigned to this route.

Status: Displays the status of the route.

Action: Click the green + icon to add a new route, click the pencil icon to edit the route, or click the red X to delete the route.



Name	VLANs	Status	STP	Action
LAN Bridge	Disabled	Connected		
☑ LAN Wireless 802.11n Access Point	Disabled	Connected	☑	✎
☑ LAN Hardware Ethernet Switch	Disabled	1 Ports Connected	☑	✎
□ WAN ETHoA		Down	□	✎

Bridge Filter

Source MAC Filter	Destination Bridge	Action
New Entry		+

Bridging: Displays the default segments of the Gateway. Click the pencil icon to edit the settings.

Name: The name of the segment.

VLANs: The VLAN status of the segment.

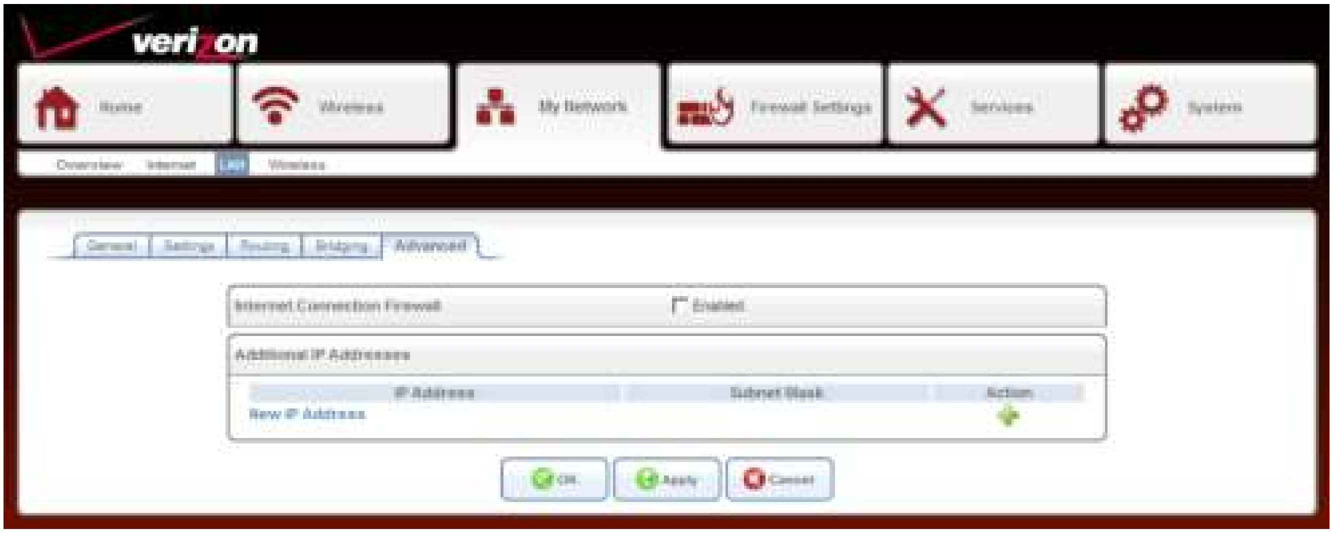
Status: The connection status of the segment.

STP: (Spanning Tree Protocol) is a method for automatically calculating the best route of a network with or without loops.

Action: Click the pencil icon to edit the segment.

Bridge Filter: You can enter your own devices to add to the bridge filter table. Click **New Entry** to add a device to the LAN Bridge.

Action: Click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.



Internet Connection Firewall □ Enabled

Additional IP Addresses

IP Address	Subnet Mask	Action
New IP Address		✚

Internet Connection Firewall: Check the Enable box to enable the firewall feature for your wired computers/devices.

New IP Address: Click to add a new device.

IP Address: The IP address of the computer or device.

Subnet Mask: The subnet mask of the computer or device.

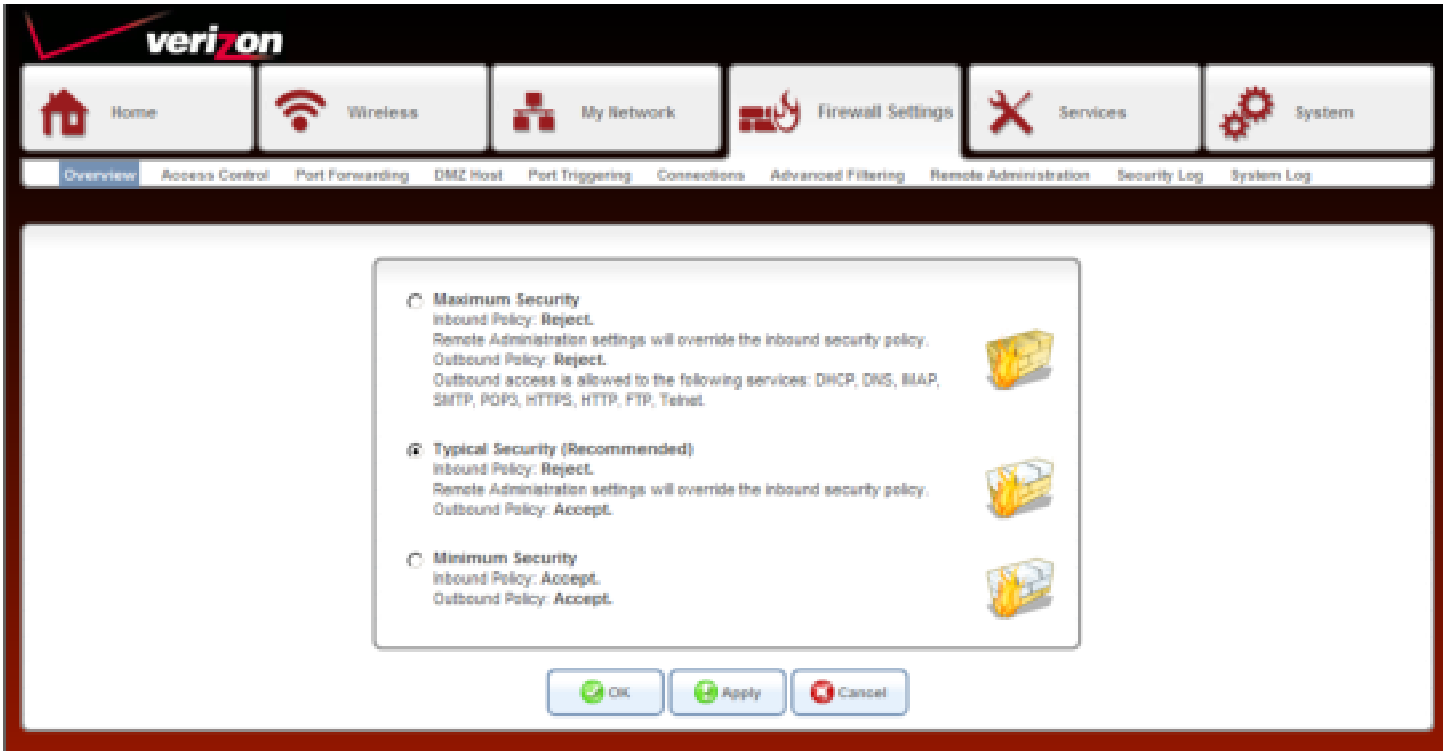
Action: Click the green + sign to add a computer or device, or click the red X to delete the computer or device.

Firewall Settings

Overview

This section explains how to configure your Router's firewall security features. The Router's firewall security settings allow you reduce the risk of unauthorized access to your network by prohibiting certain types of inbound and outbound network traffic and by allowing you to configure specific firewall rules.

To change your firewall security level, click the option next to the desired security setting. Next, click **Apply** to allow the changes to take effect.



○ **Maximum Security**
Inbound Policy: **Reject.**
Remote Administration settings will override the inbound security policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: DHCP, DNS, IMAP, SMTP, POP3, HTTPS, HTTP, FTP, Telnet.

● **Typical Security (Recommended)**
Inbound Policy: **Reject.**
Remote Administration settings will override the inbound security policy.
Outbound Policy: **Accept.**

○ **Minimum Security**
Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

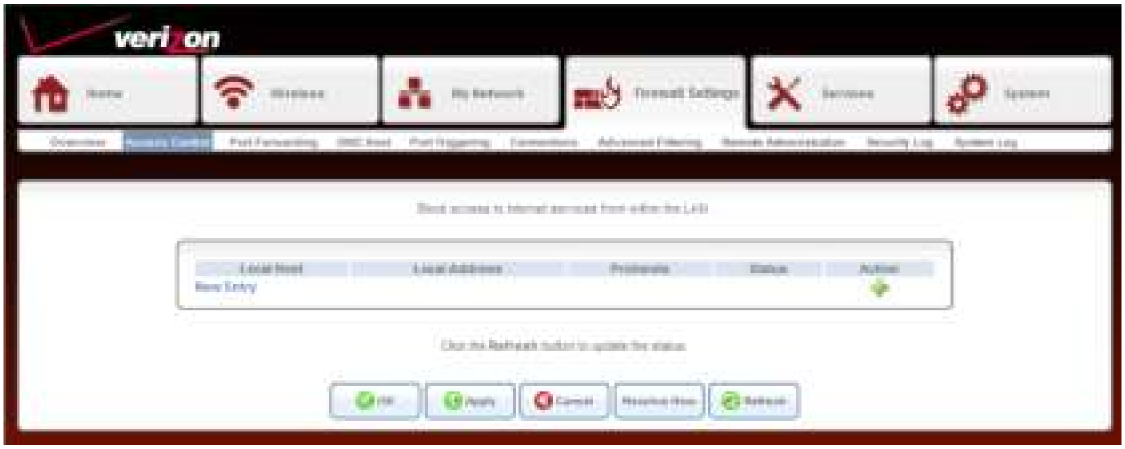
Maximum Security (High): High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited.

Typical Security (Medium): Like High security, Medium security only allows basic Internet functionality by default. However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass.

Minimum Security (Low): Low security setting will allow all traffic except for known attacks. With Low security, your Gateway is visible to other computers on the Internet.

Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

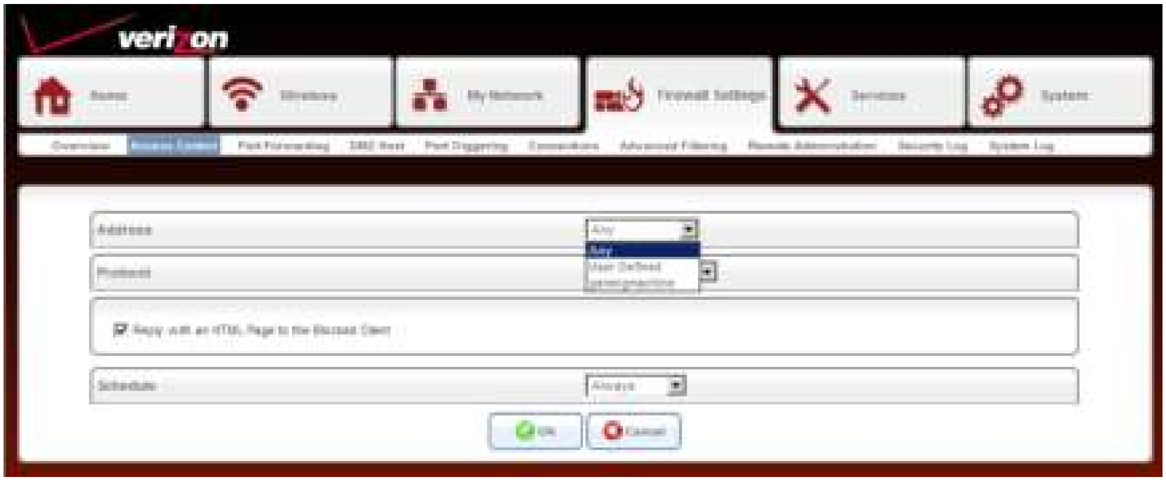


Block access to Internet services from within the LAN

Local Host	Local Address	Protocols	Status	Action
New Entry				✓

Click the Refresh button to update the status.

Click **New Entry** to add a rule.



Address: Any

Protocol:

☑ Reply with an HTML Page to the Blocked Client

Schedule: Always

Address: Select a device from the list or select **User Defined** to create a new object.

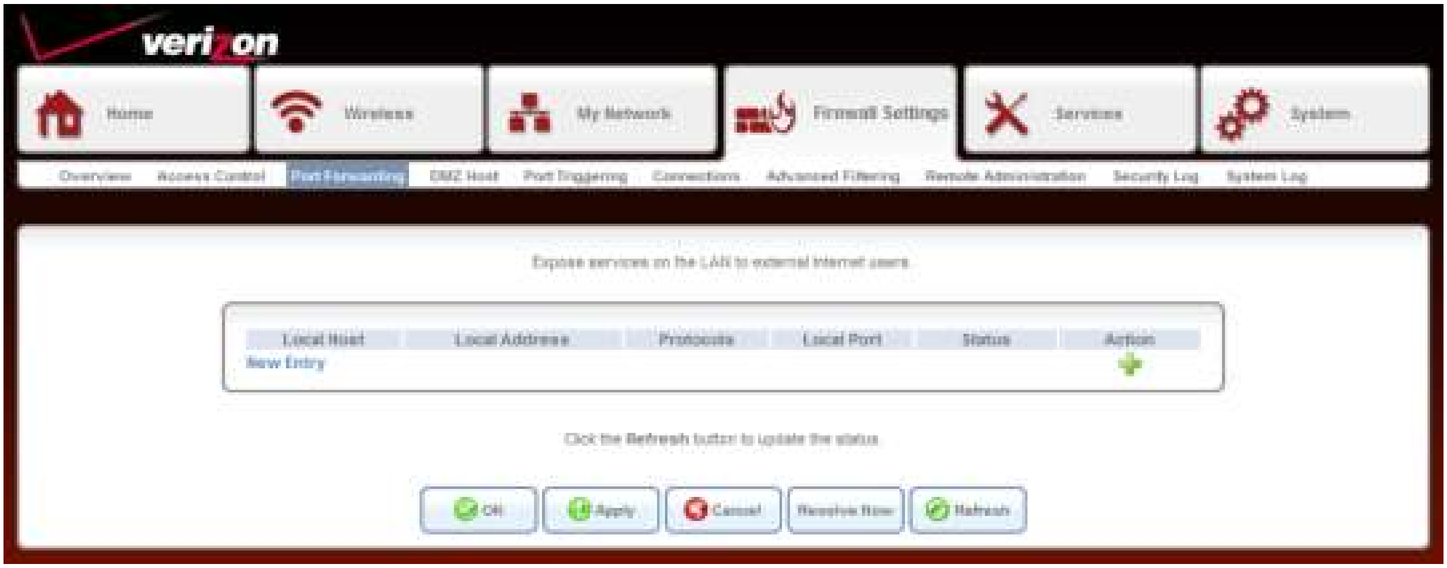
Protocol: Select the protocol or service you want to block. The default list will have basic services. You can select **Show All Services** for a large list. If you do not see the service you want, select **User Defined** to create your own. The complete list can be view and edited at **System** > **Objects and Rules** > **Protocols**.

Reply with an HTML Page: Check this box if you want to redirect the user who tries to access a blocked service to a website of your choice. To change the web site, go to **Services** > **Parental Control** > **Advanced Options**.

Schedule: Select **Any** or a user defined schedule. Select **User Defined** to create a schedule rule. You can create/view/edit schedules at **Services** > **Objects and Rules** > **Scheduler Rules**.

Port Forwarding

Port Forwarding allows you to open a single port or a range of ports. Certain applications and games may require ports to be opened or forwarded to your computer to work. Click **New Entry** to create a rule.



Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Local Port	Status	Action
New Entry					+

Click the **Refresh** button to update the status

Local Host: Displays the name of the host name.

Local Address: Displays the IP address of the host.

Protocols: Displays the protocol(s) used in the port forwarding rule.

Local Port: Displays the port(s) used in the port forwarding rule.

Status: Displays the current status of the rule (Active or Disabled).

Action: Click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

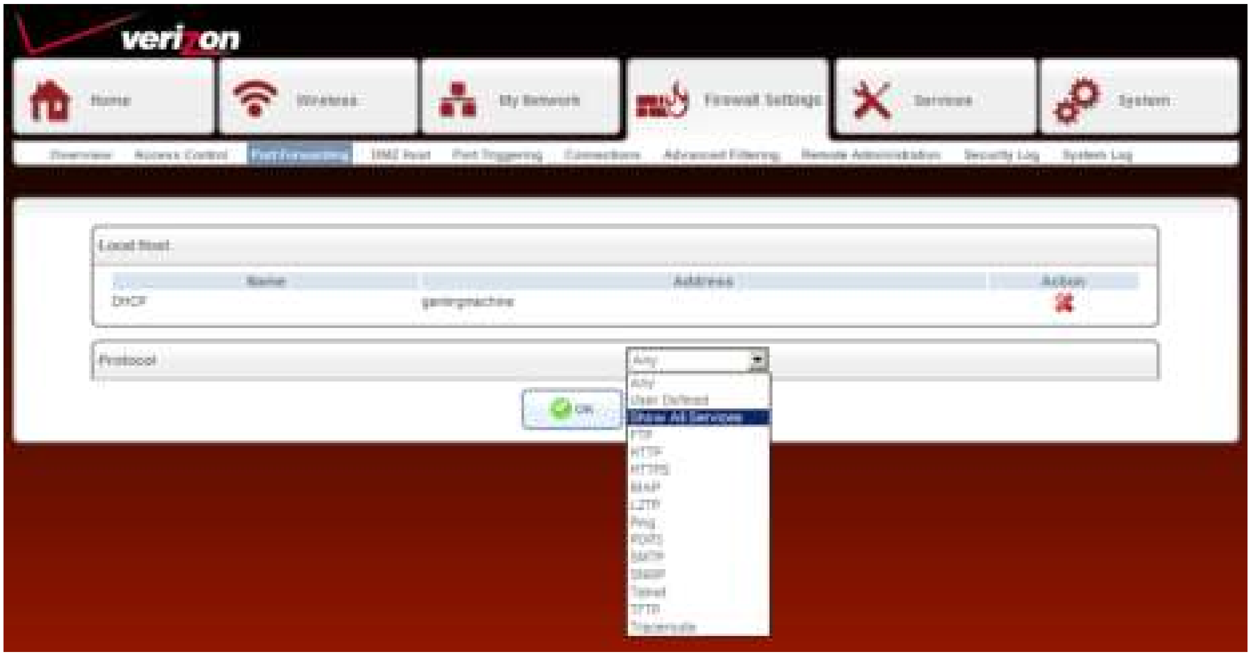
New Entry: Click to add a new port forwarding rule (refer to the next page).

Create a Rule

Step 1: Click New Entry.

Step 2: Next to Local Host, select a computer or device from the drop-down menu.

Step 3: Next to Protocols, select a pre-defined service from the drop-down menu. The default list will have basic services. Select **Show All Services** for a much larger list of specific games and applications. If you do not see the service you want, select **User Defined** to create your own. The complete list can be view and edited at **System** > **Objects and Rules** > **Protocols**.



Local Host

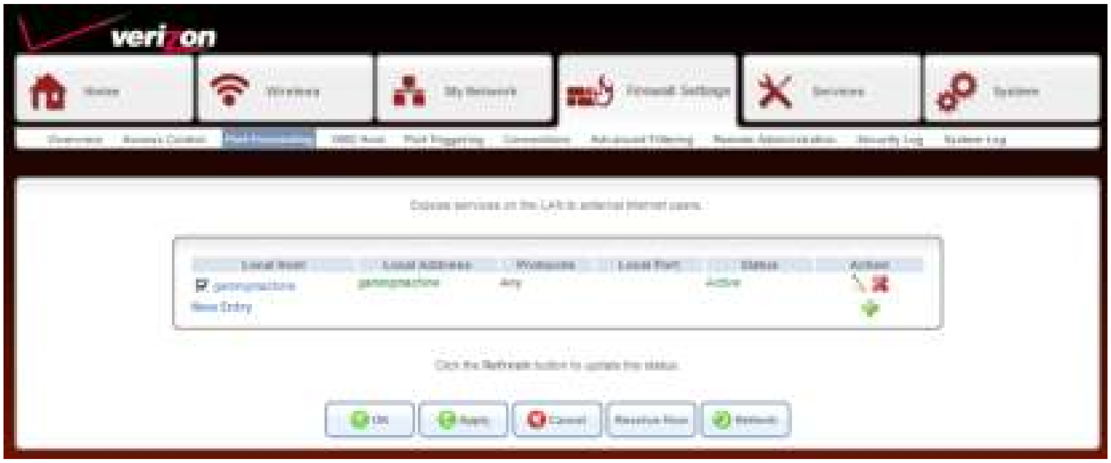
Name	Address	Action
DHCP	gamingmachine	✖

Protocol: Any

- Any
- User Defined
- Show All Services
- FTP
- HTTP
- HTTPS
- IMAP
- L2TP
- Ping
- POP3
- SMTP
- SNMP
- Telnet
- TFTP
- Traceroute

Step 4: Click **OK** to save the rule.

Step 5: The new rule will appear in the list. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.



Expose services on the LAN to external Internet users.

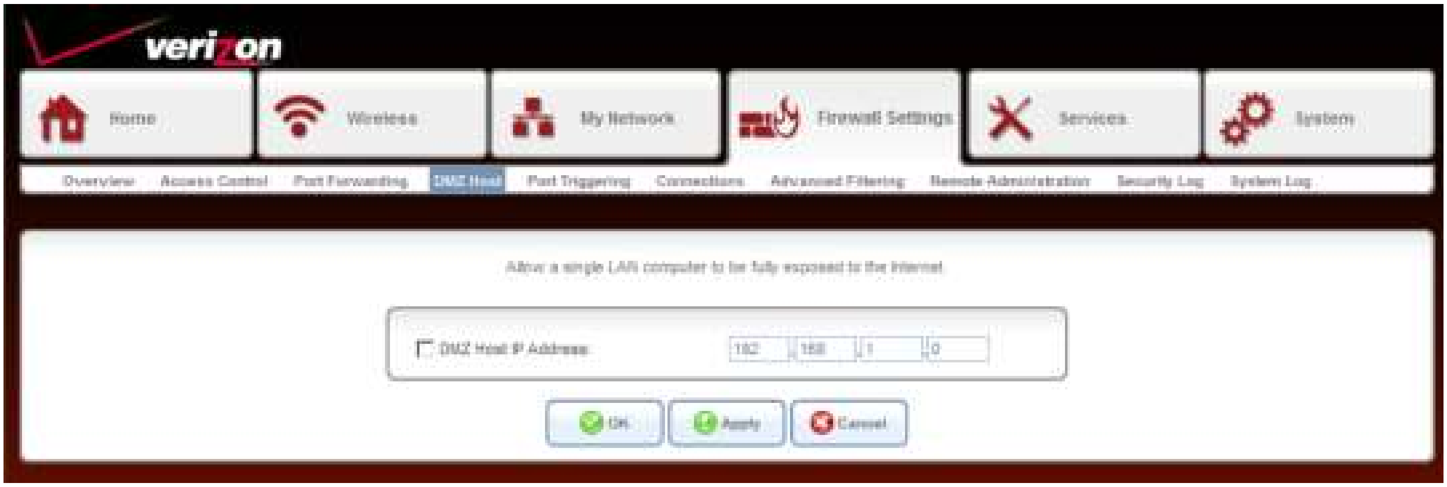
Local Host	Local Address	Protocols	Local Port	Status	Action
☑ gamingmachine	gamingmachine	Any		Active	✎ ✖
New Entry					✚

Click the Refresh button to update the status.

DMZ Host

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

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



Allow a single LAN computer to be fully exposed to the Internet

□ DMZ Host IP Address 192 . 168 . 1 . 0

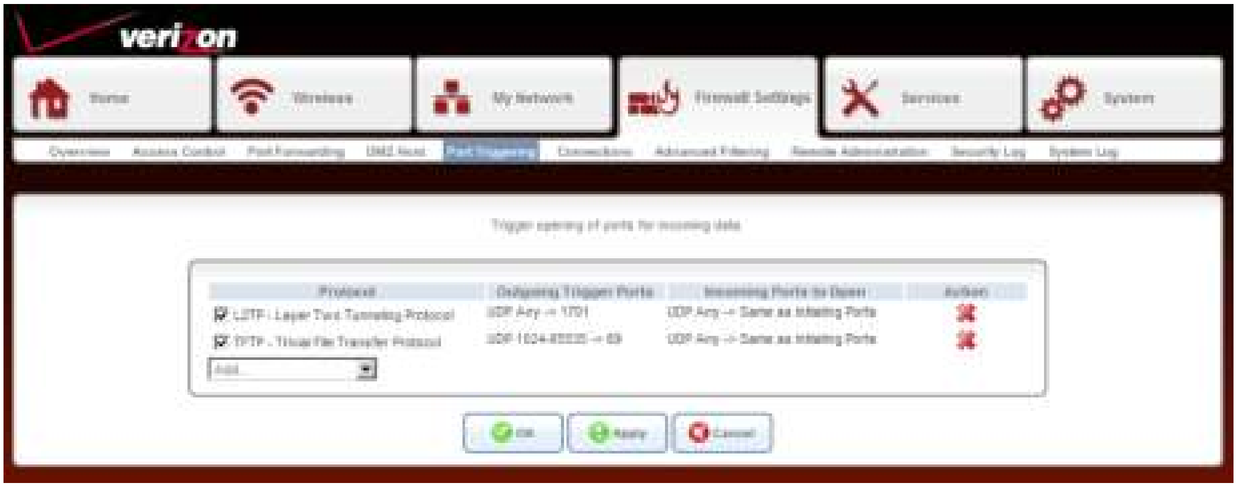
DMZ Host IP Address: Check the box to DMZ. This will de-activate any port-forwarding rules.

Enter the IP address of the computer you want to open to the Internet.

Port Triggering

The Port Triggering feature allows you to forward a range of ports to an IP address on your local network (LAN) only after specific outbound traffic is detected. You can set up a port triggering entry based on your specific ports.

IMPORTANT: Using various Internet applications depends on the Router's firewall settings. Make sure that the Router's firewall is set to Medium Security or lower to take advantage of all the port forwarding features. Firewall settings take precedence over port forwarding services configured in the Router. For example, if the firewall is set to Medium Security, this will block ICMP packets even if the ICMP service is enabled. If a port forwarding service is not working, try setting the firewall to a lower setting.



Trigger opening of ports for incoming data

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
☑ L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✗
☑ TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✗
Add...			

Protocol: Displays the protocol/service. Check the box to activate the rule.

Outgoing Trigger Ports: Displays the outgoing port(s) and protocol(s) used by the application.

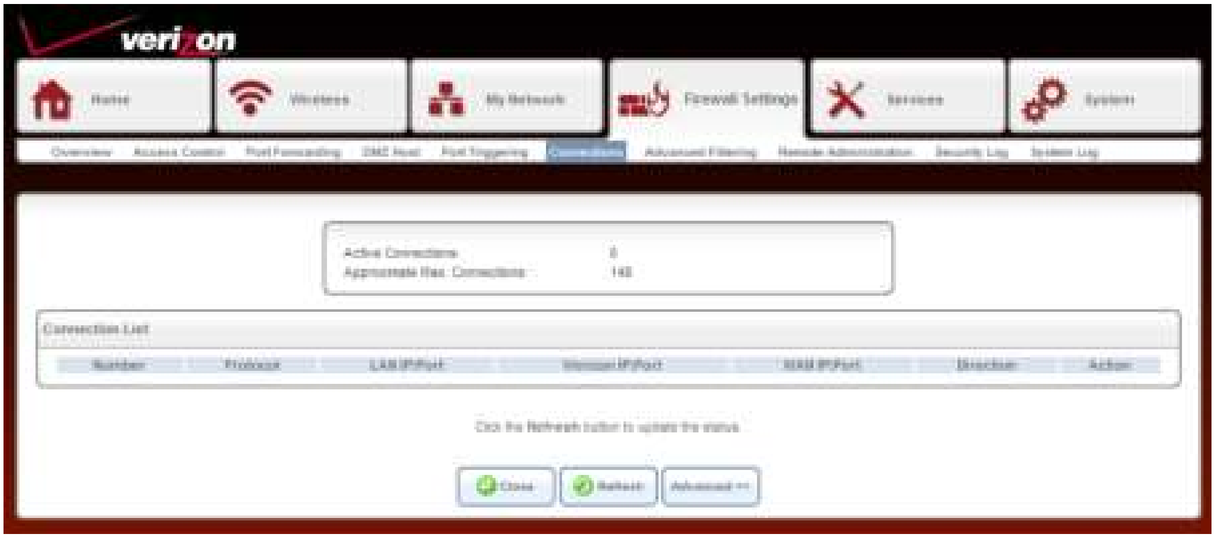
Incoming Ports to Open: Displays the incoming port(s) and protocol(s) opened by the application.

Action: Click the red X to delete the rule.

Add: Select a service/application from the drop-down menu to add.

Connections

This page will display connection from your local network (LAN) to the Internet.



Active Connections 0
Approximate Max. Connections 148

Connection List

Number	Protocol	LAN IP/Port	Internet IP/Port	WAN IP/Port	Direction	Action

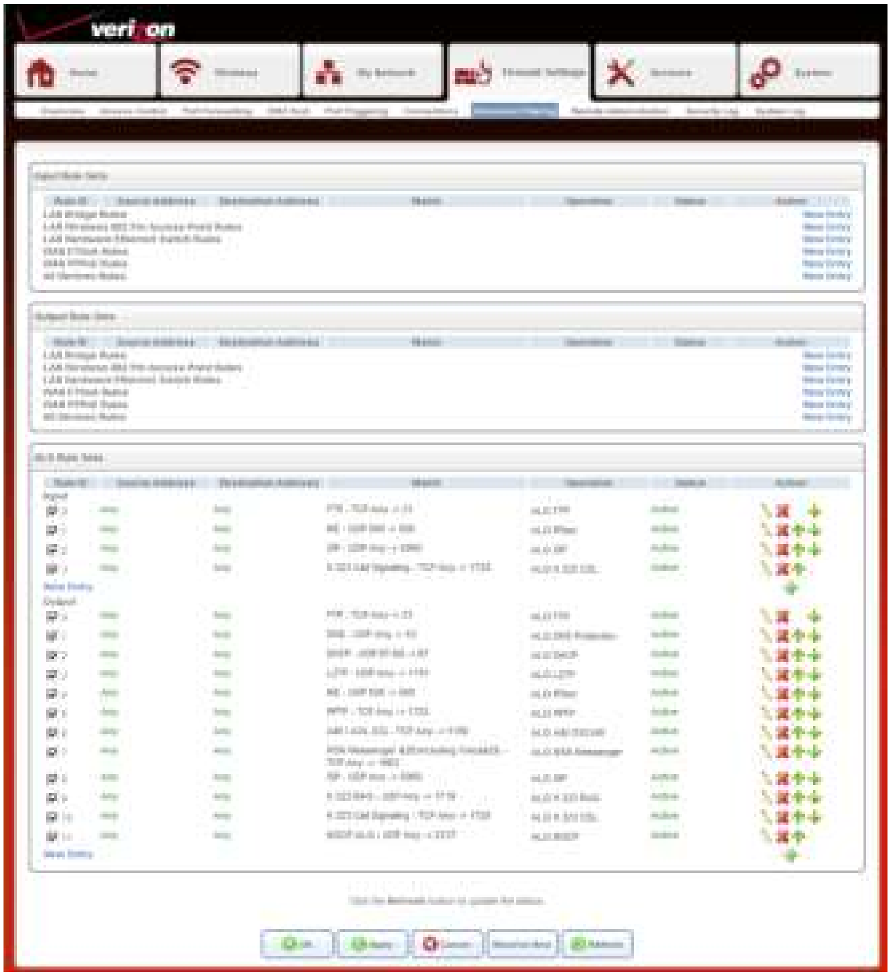
Click the Refresh button to update the status.

Action: Click the red X to delete the listing.

Close: Click to go to the Overview page.

Advanced Filtering

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Port Triggering makes some of these applications work with the Gateway.



Protocol: Displays the protocol/service. Check the box to activate the rule.

Outgoing Trigger Ports: Displays the outgoing port(s) and protocol(s) used by the application.

Incoming Ports to Open: Displays the incoming port(s) and protocol(s) opened by the application.

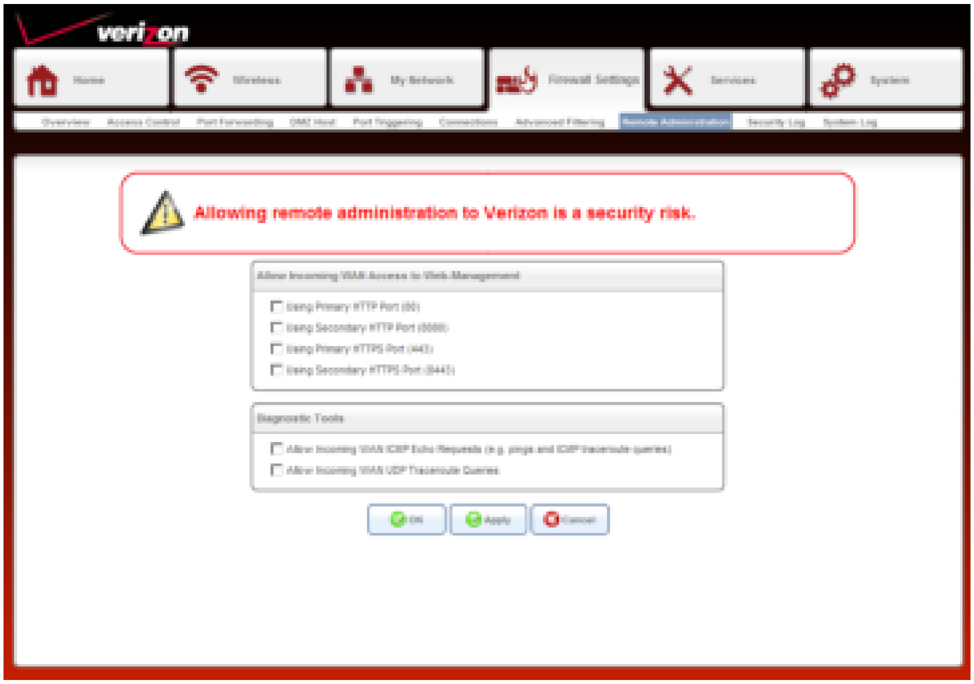
Action: Click the red X to delete the rule.

Add: Select a service/application from the drop-down menu to add.

Remote Administration

Remote management allows the Gateway to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface.

Example: http://x.x.x.x:8080 whereas x.x.x.x is the WAN IP address of the Gateway and 8080 is the port used for the Web Management interface.



Allowing remote administration to Verizon is a security risk.

Allow Incoming WAN Access to Web Management

☐ Using Primary HTTP Port (80)
☐ Using Secondary HTTP Port (8080)
☐ Using Primary HTTPS Port (443)
☐ Using Secondary HTTPS Port (8443)

Diagnostic Tools

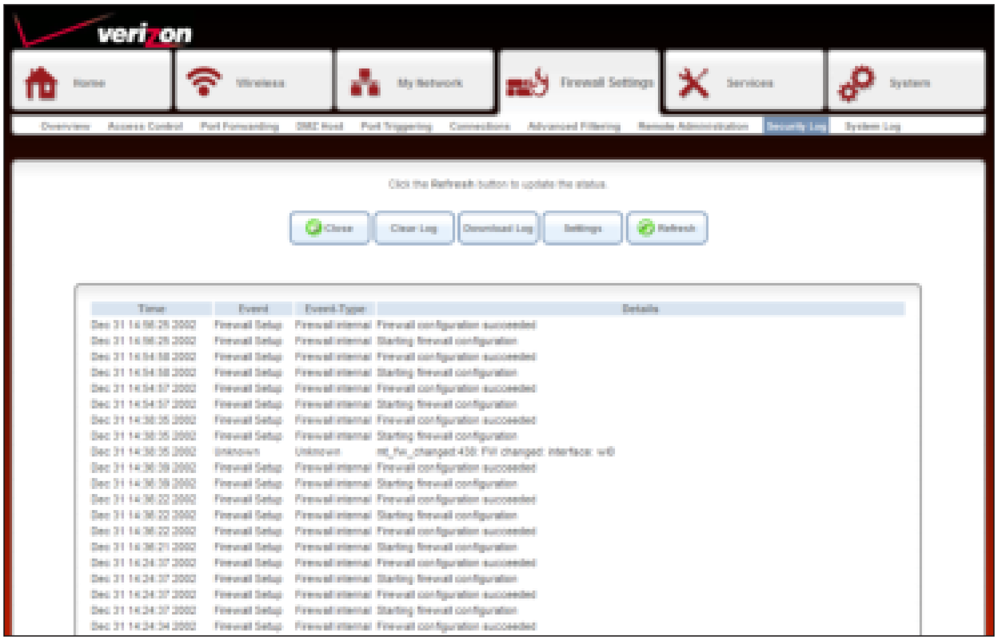
☐ Allow Incoming WAN ICMP Echo Requests (e.g. pings and ICMP traceroute queries)
☐ Allow Incoming WAN UDP Traceroute Queries

Allow Incoming WAN Access to Web Management: Check the box of the port you want to use. The default port is 80.

Diagnostic Tools: Check the box to activate the diagnostic tools rule.

Security Log

The Gateway automatically logs (records) security events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.



Click the Refresh button to update the status.

Time	Event	Event-Type	Details
Dec 31 14:56:25 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:56:25 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:54:58 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:54:58 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:54:57 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:54:57 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:38:35 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:38:35 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:38:35 2002	Unknown	Unknown	mt_fw_changed:438: FW changed: interface: wl0
Dec 31 14:36:39 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:36:39 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:36:22 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:36:22 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:36:22 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:36:21 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:24:37 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:24:37 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:24:37 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded
Dec 31 14:24:37 2002	Firewall Setup	Firewall internal	Starting firewall configuration
Dec 31 14:24:34 2002	Firewall Setup	Firewall internal	Firewall configuration succeeded

Close: Click to close the log page.

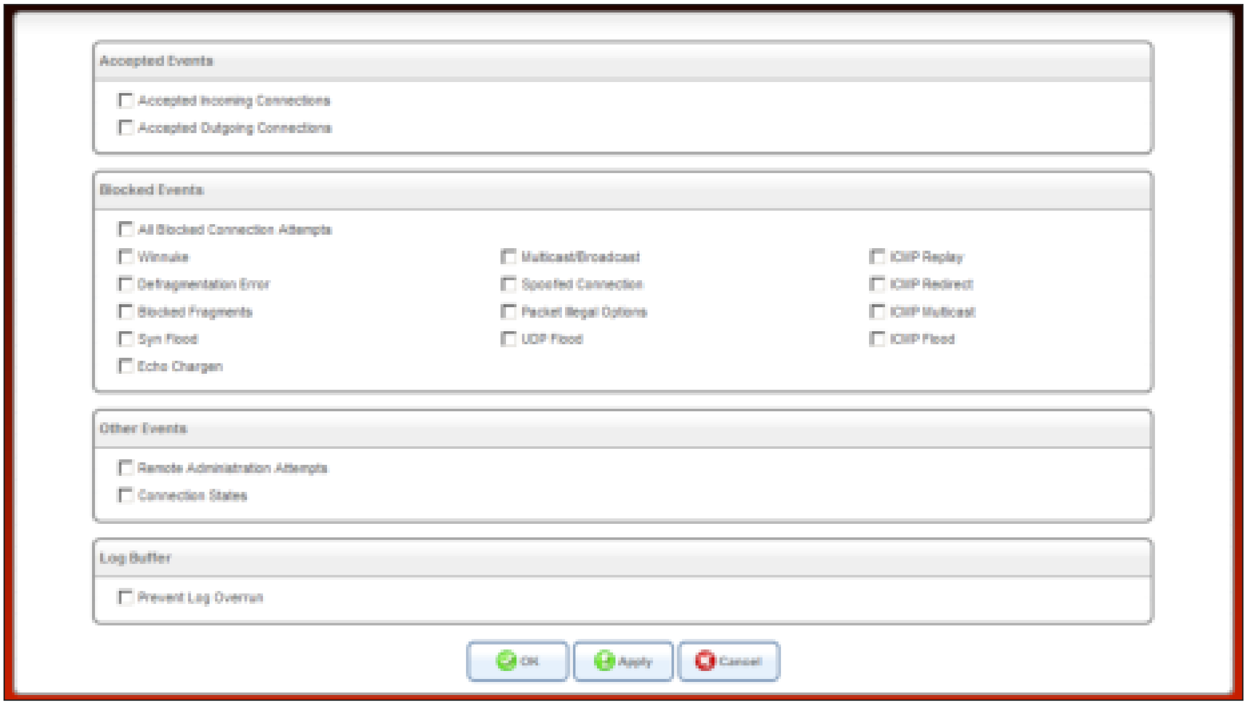
Clear Log: Click to delete all the log entries.

Download Log: Click to save the log to your computer.

Settings: Click to select filters for the information displayed in the log (refer to the next page).

Refresh: Click to update the log details on the screen so it displays any recent activity.

Check the box(es) below to include in the security log.



Accepted Events

□ Accepted Incoming Connections
□ Accepted Outgoing Connections

Blocked Events

□ All Blocked Connection Attempts
□ Winnuke
□ Defragmentation Error
□ Blocked Fragments
□ Syn Flood
□ Echo Chargen
□ Multicast/Broadcast
□ Spoofed Connection
□ Packet Illegal Options
□ UDP Flood
□ ICMP Replay
□ ICMP Redirect
□ ICMP Multicast
□ ICMP Flood

Other Events

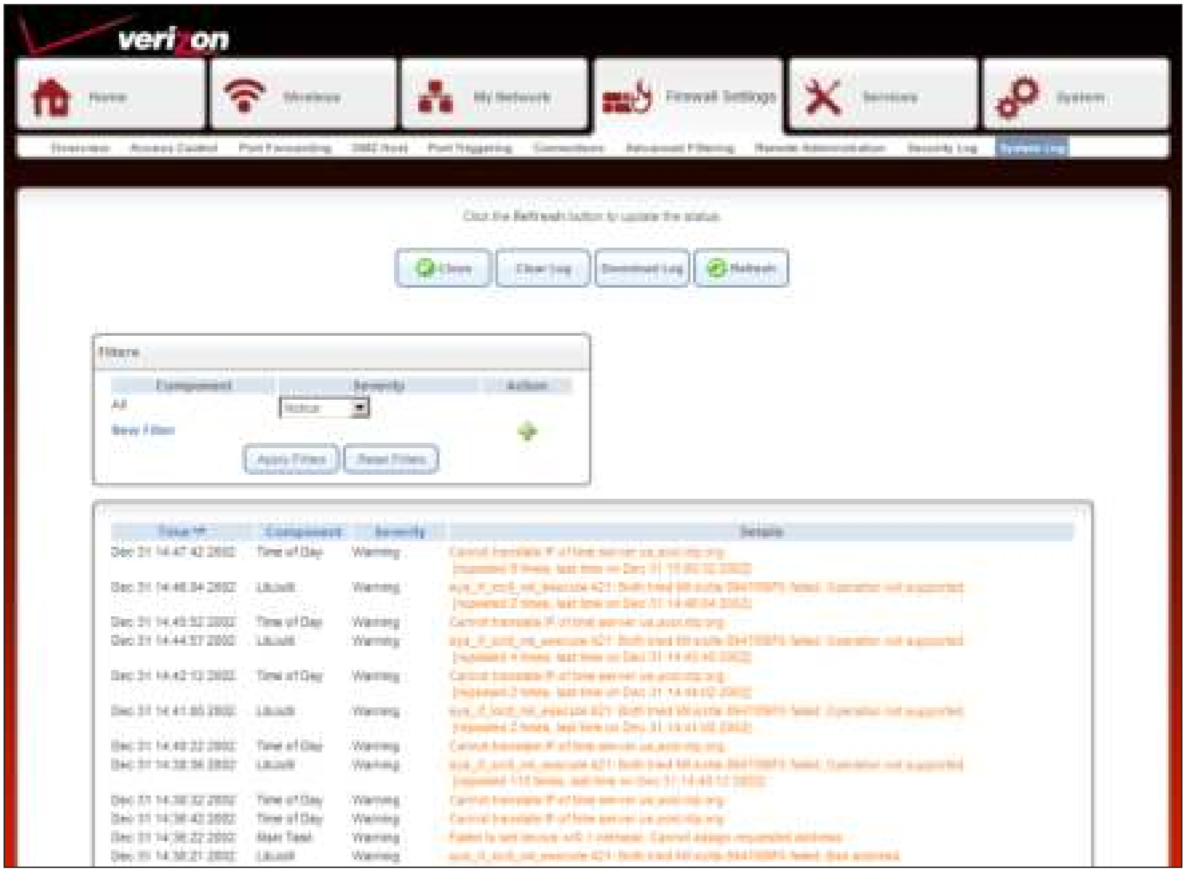
□ Remote Administration Attempts
□ Connection States

Log Buffer

□ Prevent Log Overrun

System Log

The Gateway automatically logs (records) system events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.



Click the Refresh button to update the status.

Component	Severity	Action
All	Notice	

Time	Component	Severity	Details
Dec 31 14:47:42 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org (repeated [illegible] times, last time on Dec 31 [illegible] 2002)
Dec 31 14:46:34 2002	Libuxdi	Warning	sys_if_ioctl_net_execute 421: Both tried [illegible] failed: Operation not supported (repeated 2 times, last time on Dec 31 14:46:04 2002)
Dec 31 14:45:52 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org
Dec 31 14:44:37 2002	Libuxdi	Warning	sys_if_ioctl_net_execute 421: Both tried [illegible] failed: Operation not supported (repeated 4 times, last time on Dec 31 14:45:40 2002)
Dec 31 14:42:12 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org (repeated 2 times, last time on Dec 31 14:44:02 2002)
Dec 31 14:41:55 2002	Libuxdi	Warning	sys_if_ioctl_net_execute 421: Both tried [illegible] failed: Operation not supported (repeated 2 times, last time on Dec 31 14:41:58 2002)
Dec 31 14:40:22 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org
Dec 31 14:38:56 2002	Libuxdi	Warning	sys_if_ioctl_net_execute 421: Both tried [illegible] failed: Operation not supported (repeated 115 times, last time on Dec 31 14:40:12 2002)
Dec 31 14:38:32 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org
Dec 31 14:38:42 2002	Time of Day	Warning	Cannot translate IP of time server us.pool.ntp.org
Dec 31 14:38:22 2002	Main Task	Warning	Failed to set device [illegible] netmask: Cannot assign requested address
Dec 31 14:38:21 2002	Libuxdi	Warning	sys_if_ioctl_net_execute 421: Both tried [illegible] failed: Bad address

Close: Click to close the log page and go back to the Overview page.

Clear Log: Click to delete all the log entries.

Download Log: Click to save the log to your computer.

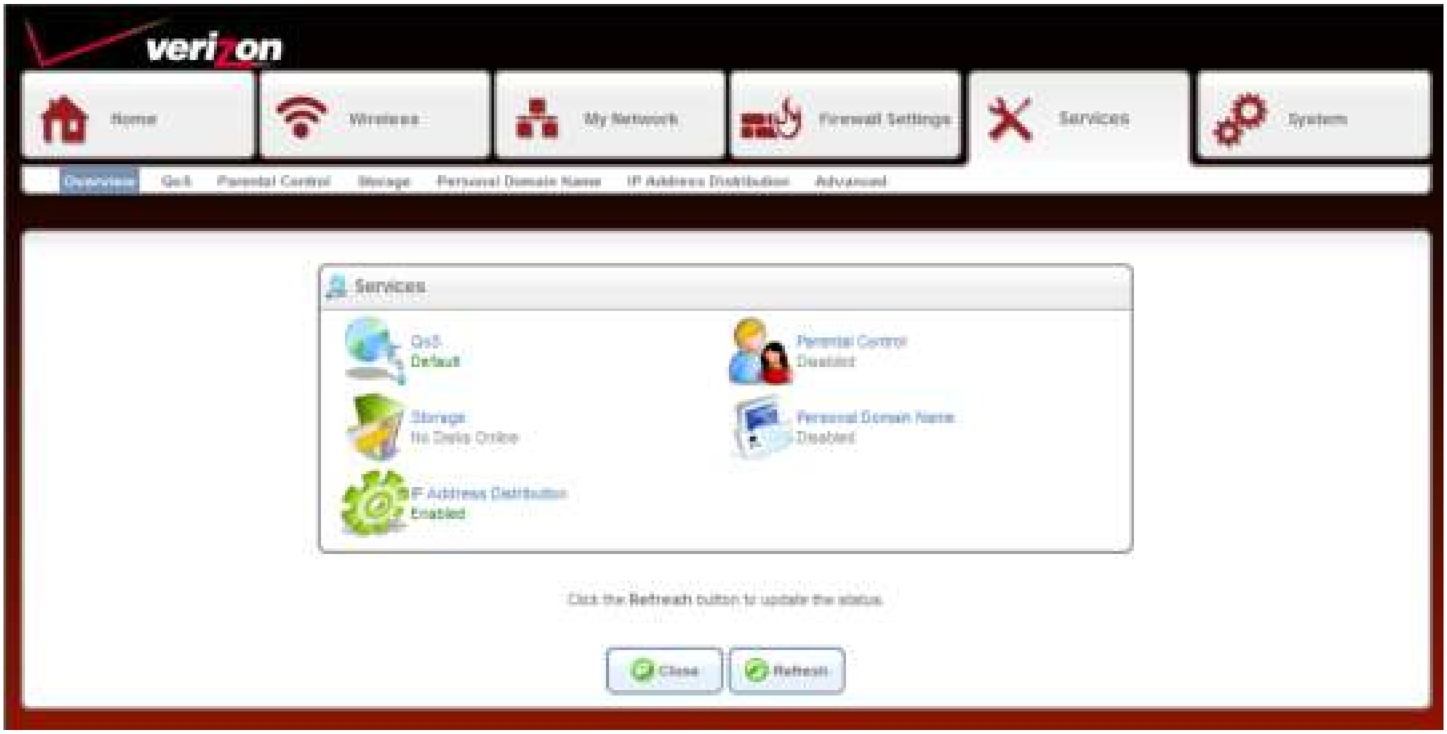
Refresh: Click to update the log details on the screen so it displays any recent activity.

Filters: Select specific items to record in the log or click **New Filter** to add an item. Click **Apply Filters** to add it to the list.

Services

Overview

This page displays the status of each service. Click on the service to configure.



Services

QoS
Default

Parental Control
Disabled

Storage
No Disks Online

Personal Domain Name
Disabled

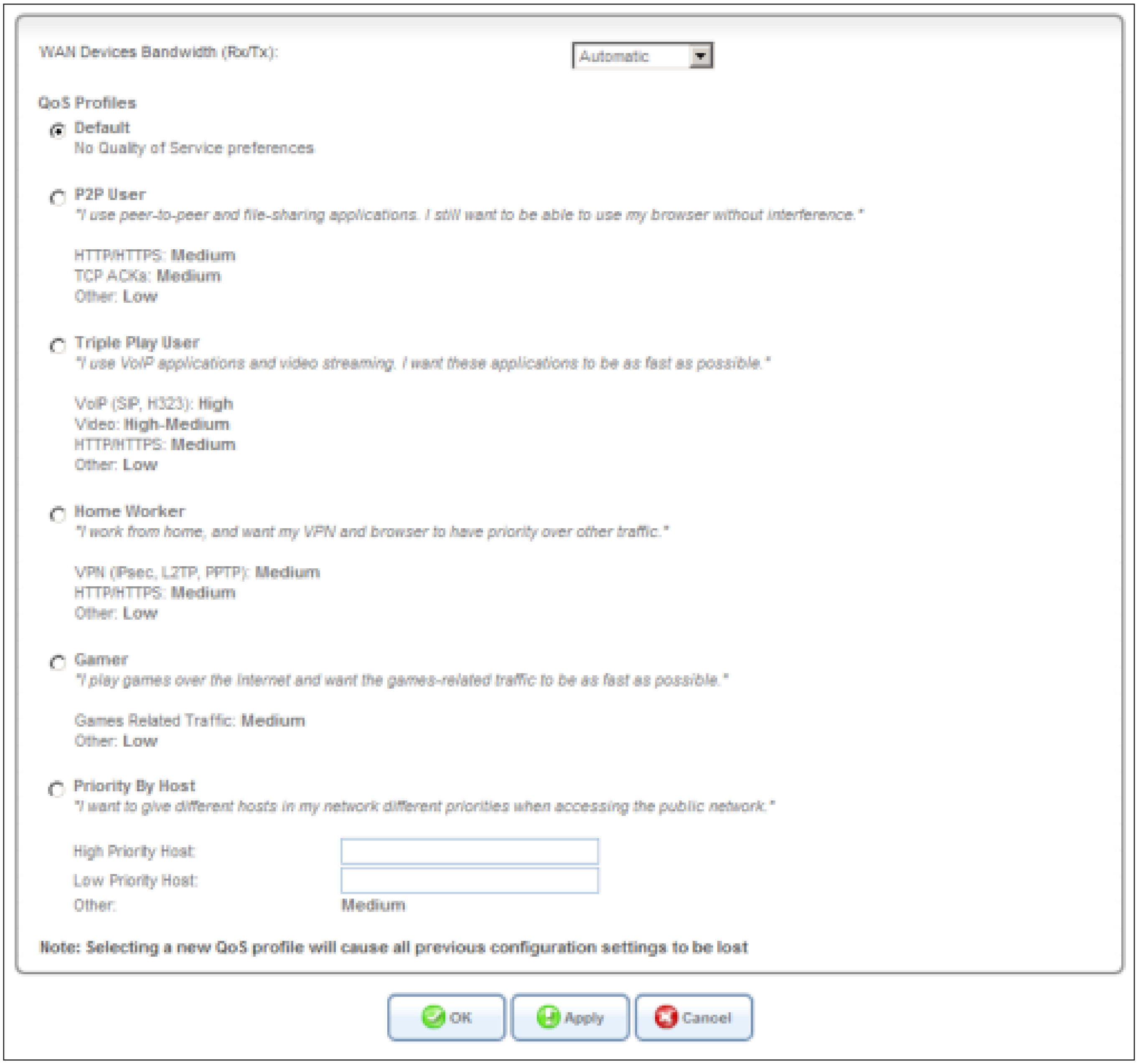
IP Address Distribution
Enabled

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

QoS

Overview

This screen allows you to configure Quality of Service parameters in the Gateway. Select the profile that fits you the best and click **OK**.



WAN Devices Bandwidth (Rx/Tx): Automatic

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**
TCP ACKs: **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**

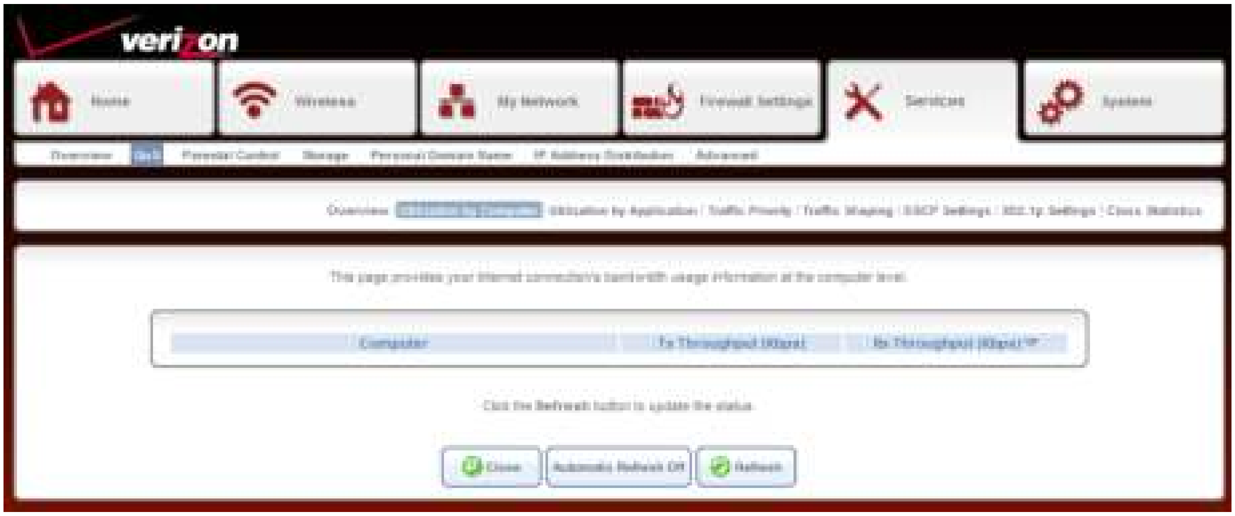
○ **Priority By Host**
"I want to give different hosts in my network different priorities when accessing the public network."

High Priority Host:	
Low Priority Host:	
Other:	**Medium**

Note: Selecting a new QoS profile will cause all previous configuration settings to be lost

Utilization by Computer

This screen displays bandwidth usage from computers on your local network.



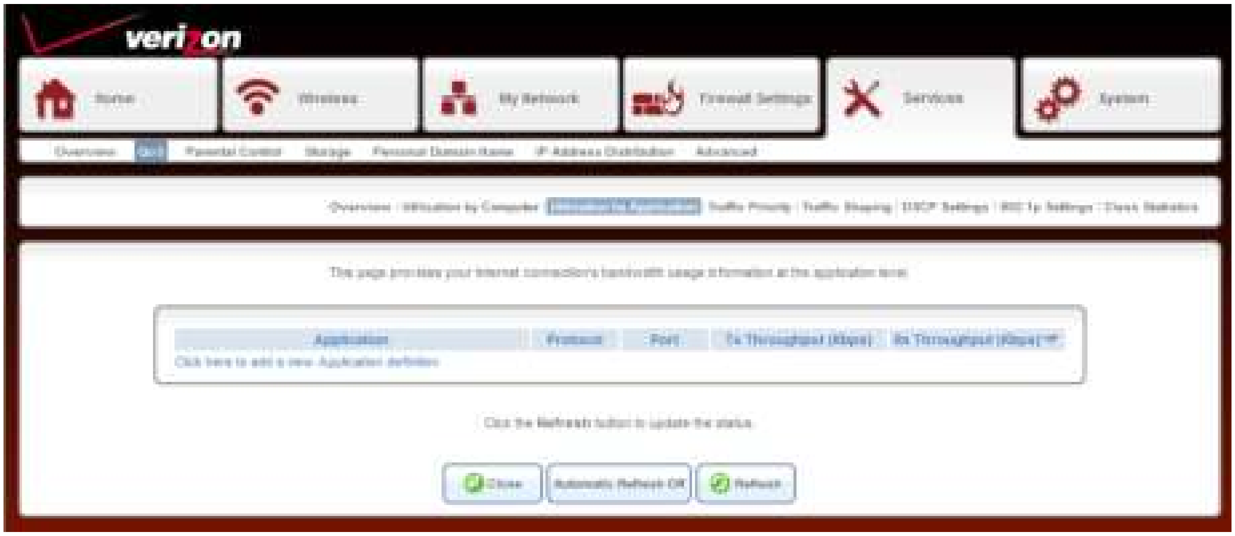
This page provides your Internet connection's bandwidth usage information at the computer level.

Computer	Tx Throughput (Kbps)	Rx Throughput (Kbps)

Click the Refresh button to update the status.

Utilization by Application

This screen displays bandwidth usage from applications on your local network.



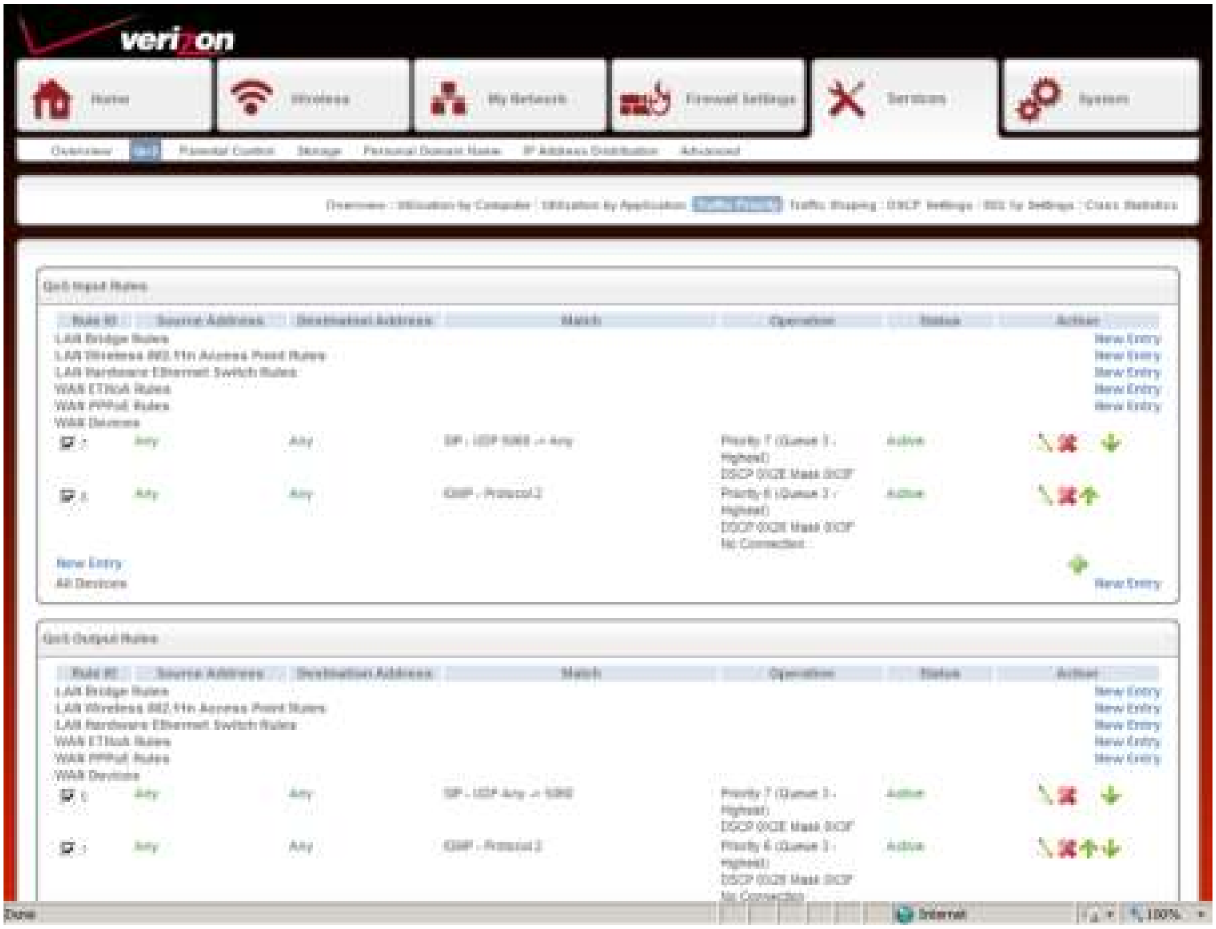
This page provides your Internet connection's bandwidth usage information at the application level.

Application	Protocol	Port	Tx Throughput (Kbps)	Rx Throughput (Kbps)
Click here to add a new Application definition				

Click the Refresh button to update the status.

Traffic Priority

This screen displays the QoS input and output rules. These will change depending on the selection you selected on the **Services** > **QoS** > **Overview** page.



QoS Input Rules

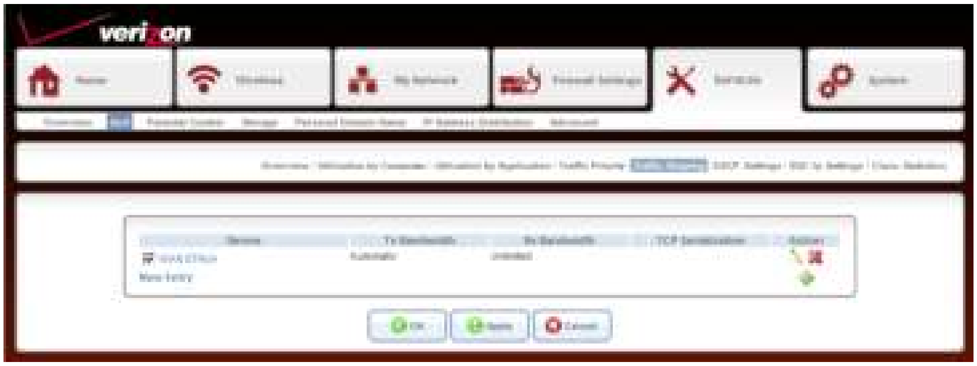
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
LAN Bridge Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
WAN Devices						
☑ [illegible]	Any	Any	SIP - UDP 5060 -> Any	Priority 7 (Queue 3 - Highest) DSCP 0x2E Mask 0x3F	Active	
☑ [illegible]	Any	Any	IGMP - Protocol 2	Priority 6 (Queue 3 - Highest) DSCP 0x28 Mask 0x3F No Connection	Active	
New Entry						
All Devices						New Entry

QoS Output Rules

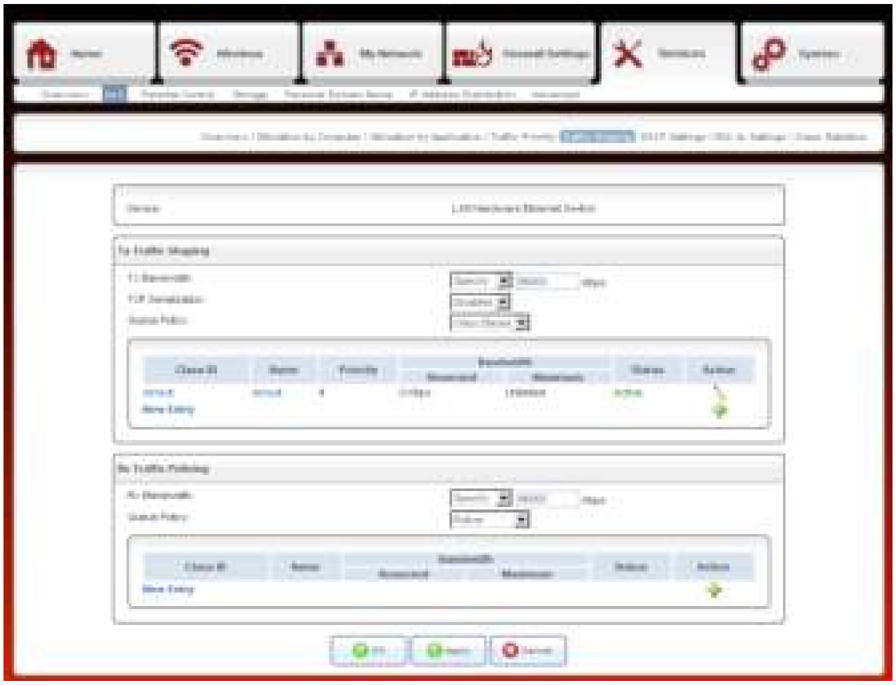
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
LAN Bridge Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
WAN Devices						
☑ [illegible]	Any	Any	SIP - UDP Any -> 5060	Priority 7 (Queue 3 - Highest) DSCP 0x2E Mask 0x3F	Active	
☑ [illegible]	Any	Any	IGMP - Protocol 2	Priority 6 (Queue 3 - Highest) DSCP 0x28 Mask 0x3F No Connection	Active	

Traffic Shaping

This page allows you to add traffic shaping rules. Click **New Entry** to add a rule.



Once you click New Entry, select the device/Gateway segment you want to configure from the drop-down menu.



Tx Bandwidth: Select the Tx traffic bandwidth from the drop-down. Select **Specify** to enter your own value, **Automatic**, or **Unlimited**.

TCP Serialization: Select **Enabled** or **Disabled**.

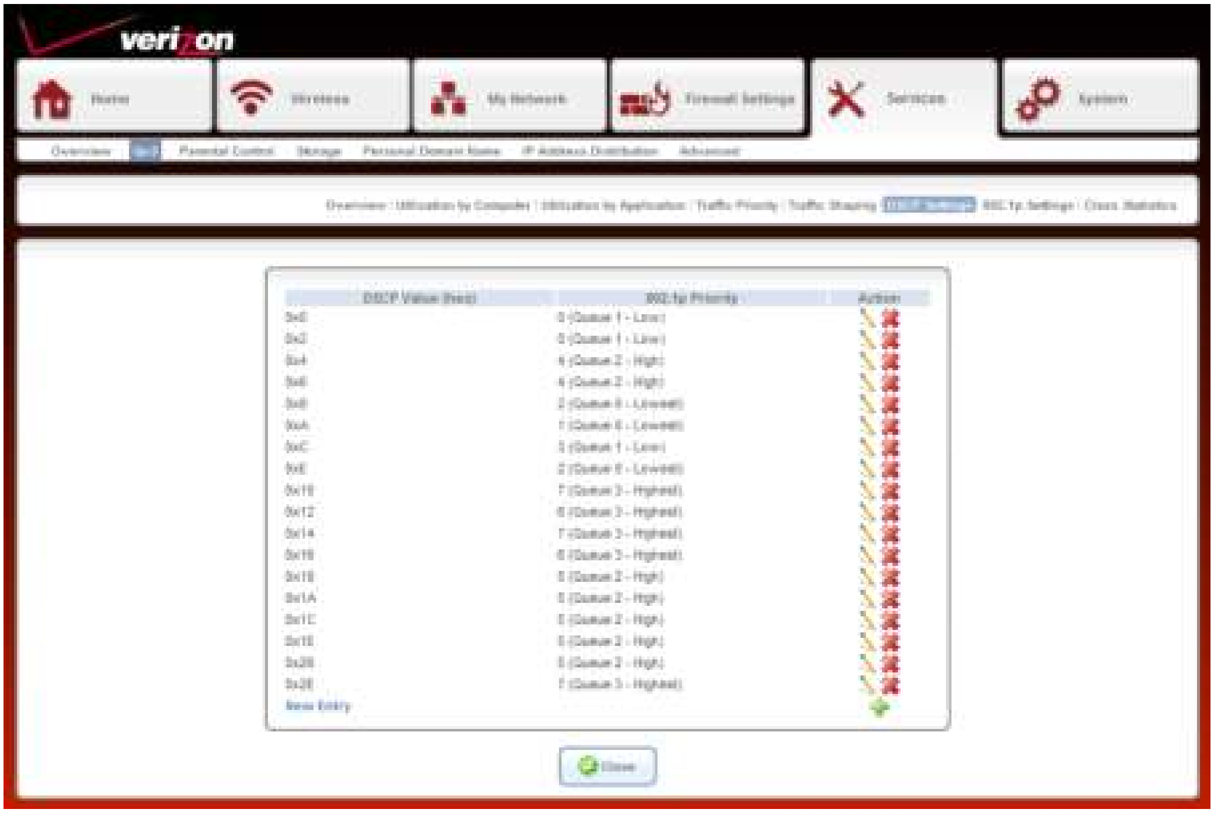
Queue Policy: Select **Class Based** or **Strict Priority**.

Rx Bandwidth: Select the Rx traffic bandwidth from the drop-down. Select **Specify** to enter your own value, **Automatic**, or **Unlimited**.

Queue Policy: Select **Policer**, **Class Based** or **Strict Priority**.

DSCP Settings

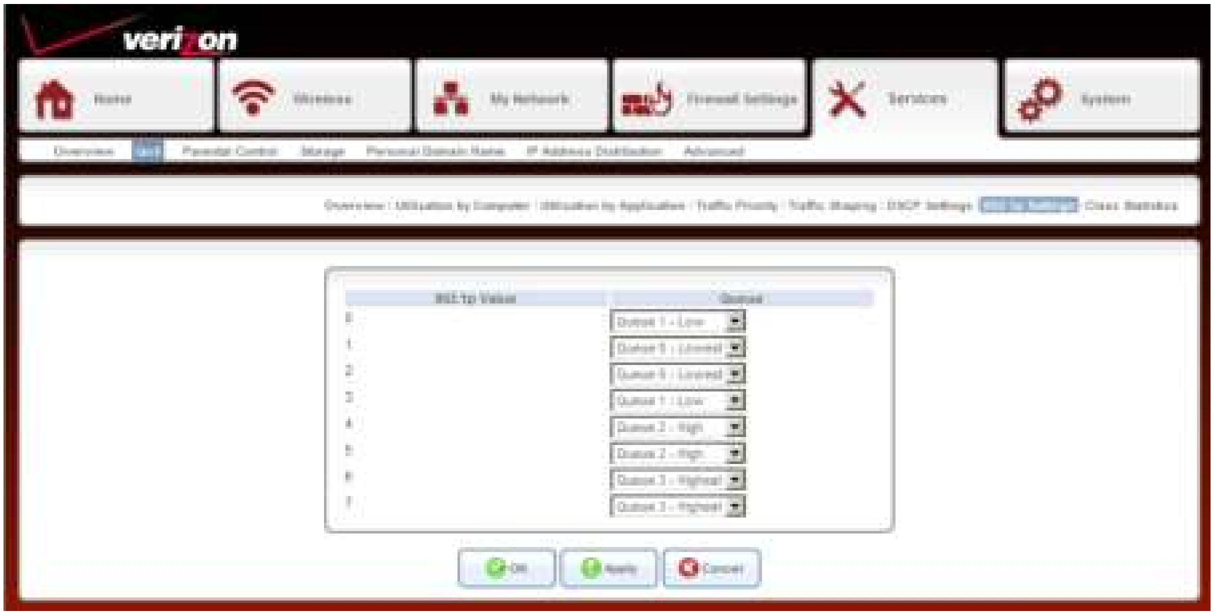
This page allows you to configure DSCP (Differentiated Services Code Point) settings. Click the pencil icon to edit the priority and settings for each DSCP value.



DSCP Value (hex)	802.1p Priority	Action
0x0	0 (Queue 1 - Low)	✎ ✖
0x2	0 (Queue 1 - Low)	✎ ✖
0x4	4 (Queue 2 - High)	✎ ✖
0x6	4 (Queue 2 - High)	✎ ✖
0x8	2 (Queue 0 - Lowest)	✎ ✖
0xA	1 (Queue 0 - Lowest)	✎ ✖
0xC	3 (Queue 1 - Low)	✎ ✖
0xE	2 (Queue 0 - Lowest)	✎ ✖
0x10	7 (Queue 3 - Highest)	✎ ✖
0x12	6 (Queue 3 - Highest)	✎ ✖
0x14	7 (Queue 3 - Highest)	✎ ✖
0x16	6 (Queue 3 - Highest)	✎ ✖
0x18	5 (Queue 2 - High)	✎ ✖
0x1A	5 (Queue 2 - High)	✎ ✖
0x1C	5 (Queue 2 - High)	✎ ✖
0x1E	5 (Queue 2 - High)	✎ ✖
0x20	5 (Queue 2 - High)	✎ ✖
0x28	7 (Queue 3 - Highest)	✎ ✖
New Entry		✚

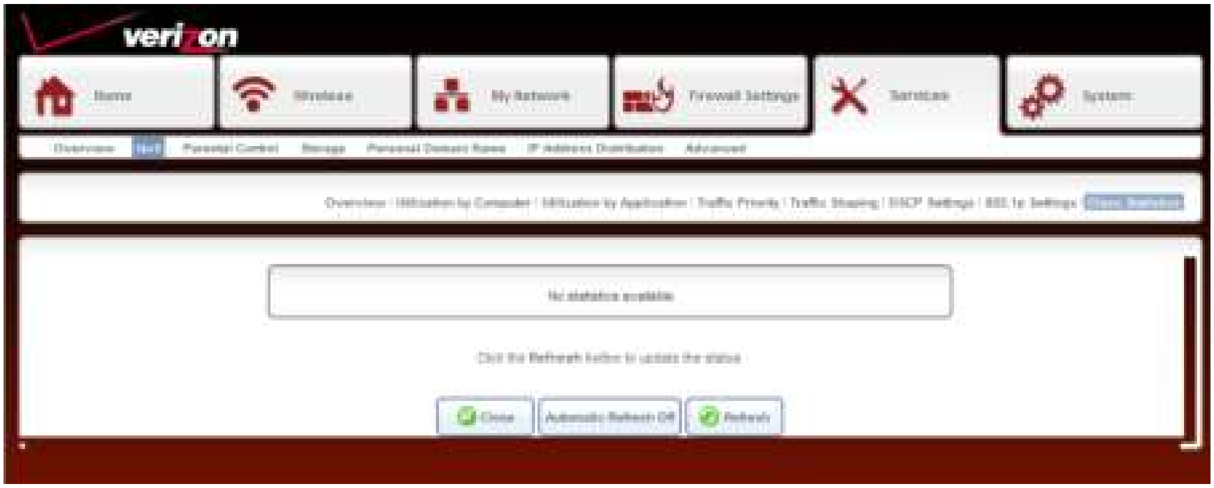
802.1p Settings

This page allows you to configure 802.1p settings. Select the queue for each 802.1p value.



802.1p Value	Queue
0	Queue 1 - Low
1	Queue 5 - Lowest
2	Queue 5 - Lowest
3	Queue 1 - Low
4	Queue 2 - High
5	Queue 2 - High
6	Queue 3 - Highest
7	Queue 3 - Highest

Class Statistics



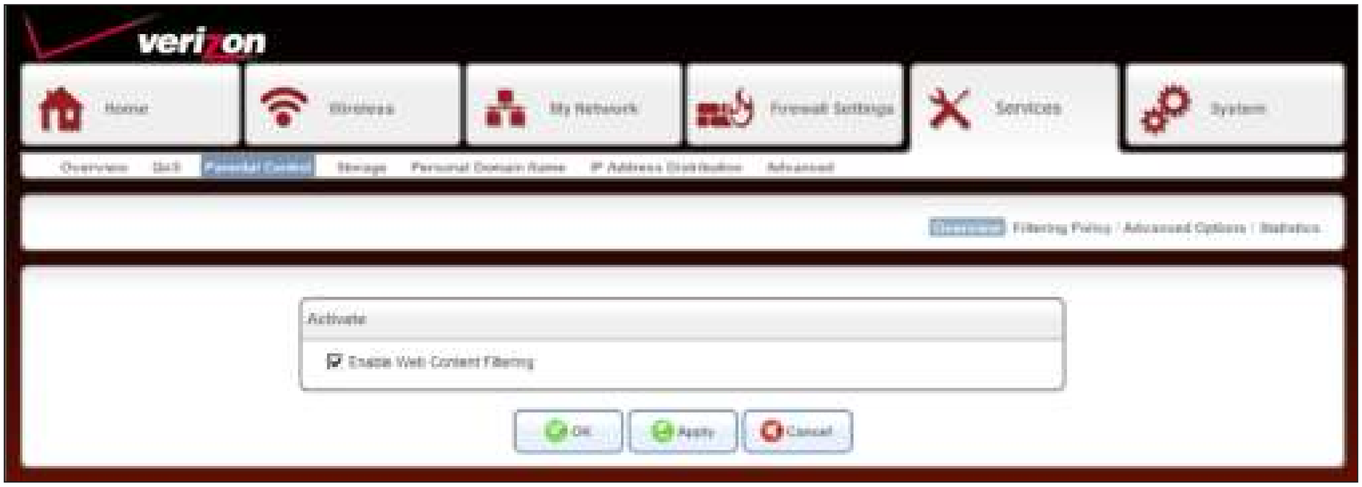
No statistics available

Click the Refresh button to update the status

Parental Controls

Overview

To activate parental control, check the **Enable Web Content Filtering** box and then click **OK**. You will be directed to the Filtering Policy page (refer to the next page).

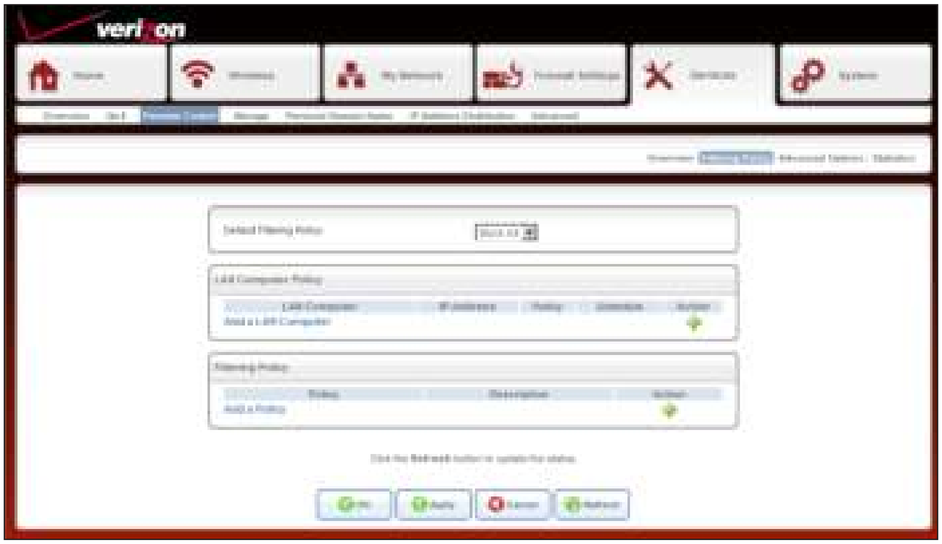


Activate

☑ Enable Web Content Filtering

Filtering Policy

Once you enable Parental Controls, you can create filtering rules here.



Default Filtering Policy: This is a global setting. If you select **Block All**, it will over-ride LAN Computer Policies and Filtering Policies created and block all computers/devices from connecting to the Internet. To use created policies, select **Allow All**.

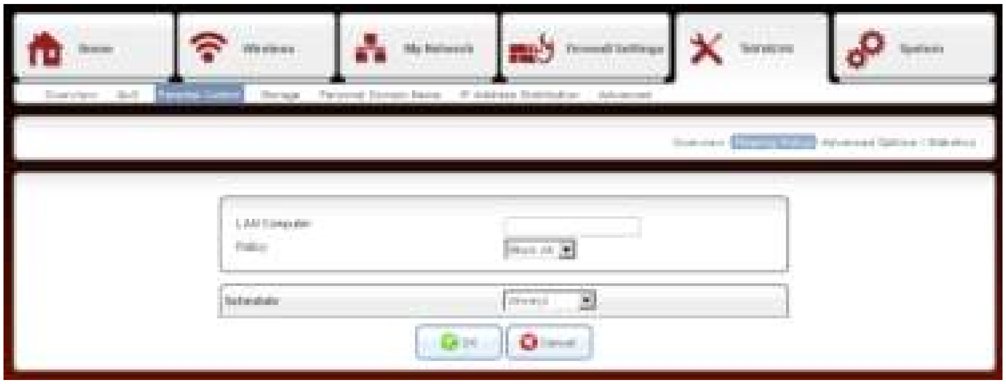
LAN Computer Policy: This list will display any LAN computer policies. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

Click **Add a LAN Computer** to create a new entry (see below).

Filtering Policy: This list will display any filter policies that were created. You can click the green + icon to add a new entry, click the pencil icon to edit, or click the red X to delete the entry.

Click **Add a Policy** to create a new entry (refer to the next page).

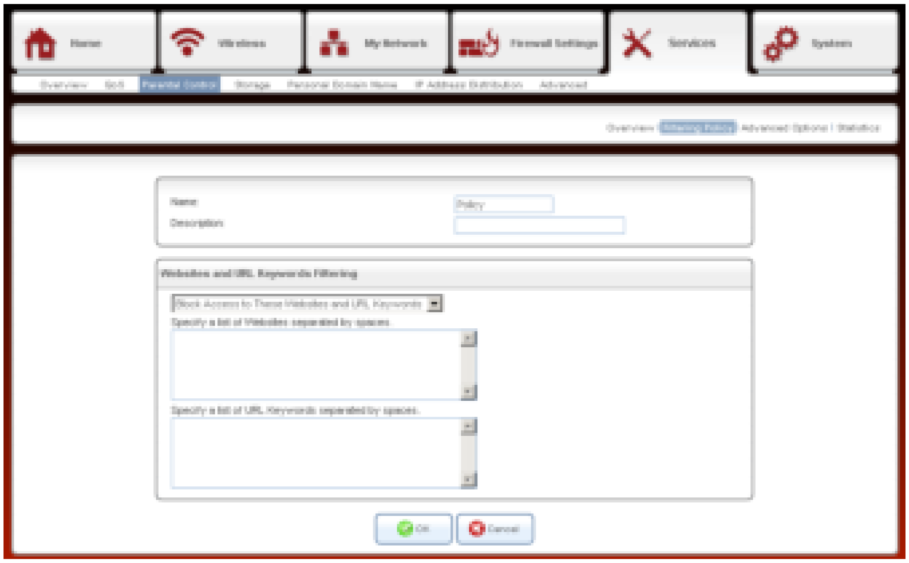
Add a LAN Computer



Enter the name or IP address (x.x.x.x) of your computer or device and then select **Allow All**, **Block All**, or any created policy (see next page). You can then select a schedule from the drop-down. Click **OK** to continue.

WARNING: If you enter the computer you are working on and select Block All, you will disconnect from the Gateway and will not be able to log back in (since you are blocked). You will have to connect to the Gateway from another computer or reset the Gateway back to factory default settings.

Add a Policy



Name: Policy

Description:

Websites and URL Keywords Filtering

Block Access to These Websites and URL Keywords

Specify a list of Websites separated by spaces.

Specify a list of URL Keywords separated by spaces.

Name: Enter a name for your policy.

Description: Enter a description.

Websites and URL Keywords Filtering: Select either **Block Access to These Websites and URL Keywords** or **Allow Access to These Websites and URL Keywords** from the drop-down menu.

List of Websites: Enter specific websites you want to block or allow.

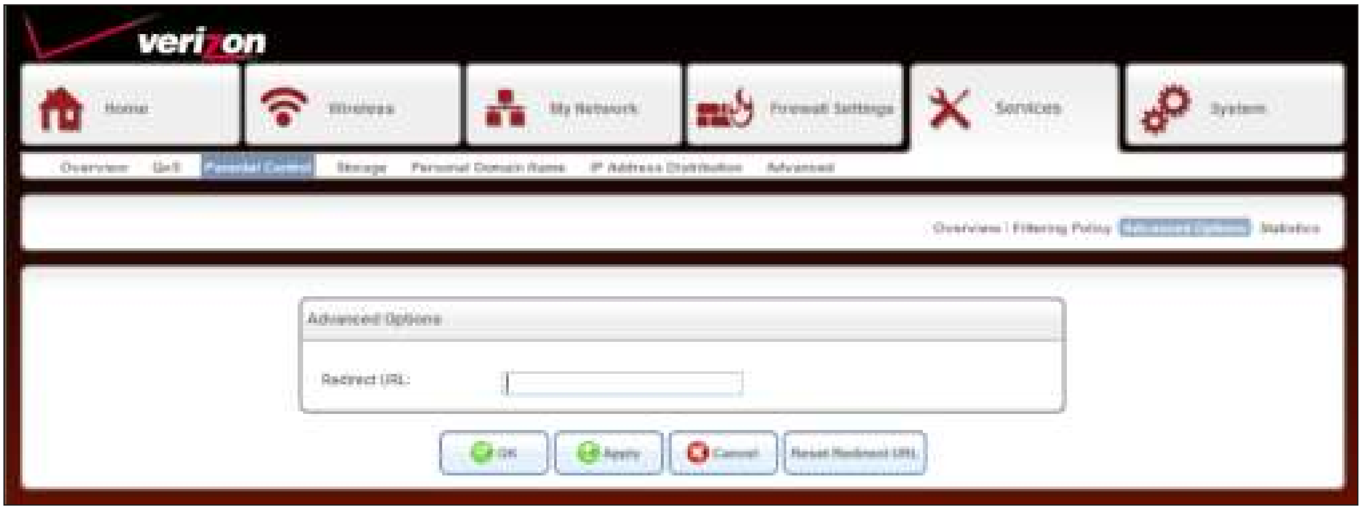
List of Keywords: Enter keywords that are on websites that you want to block or allow.

OK: Click to save your policies.

Created policies will then appear in the drop-down list when adding LAN computers.

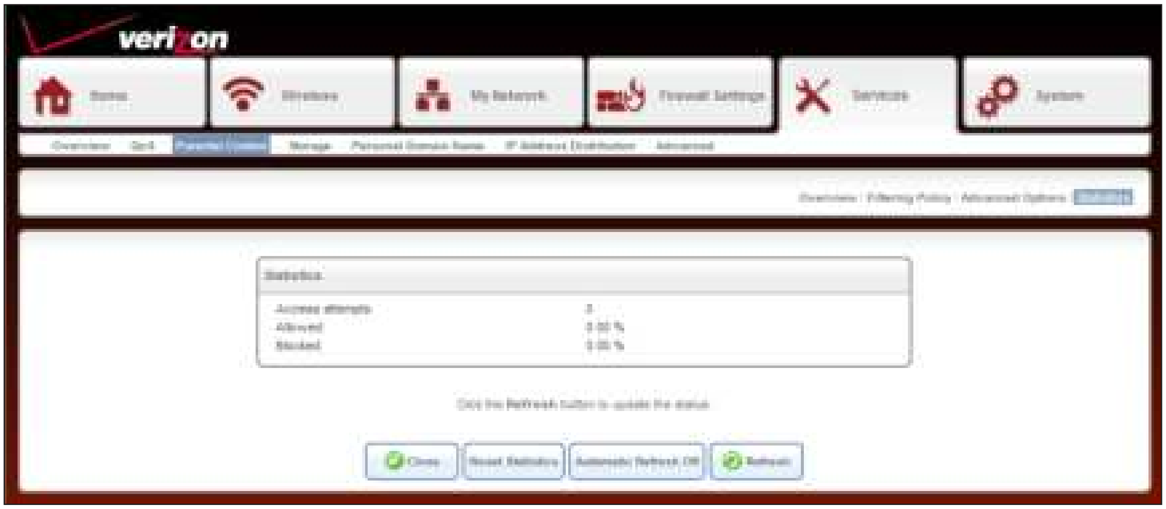
Advanced Options

If a user from your local network attempts to visit a site that you blocked, they will get redirected to the URL you want. Enter the URL below and click **OK**. Click **Reset Redirect URL** to clear out the URL.



Statistics

This page displays the number of allowed and blocked sites that were attempted to be view from your local network.



Statistics

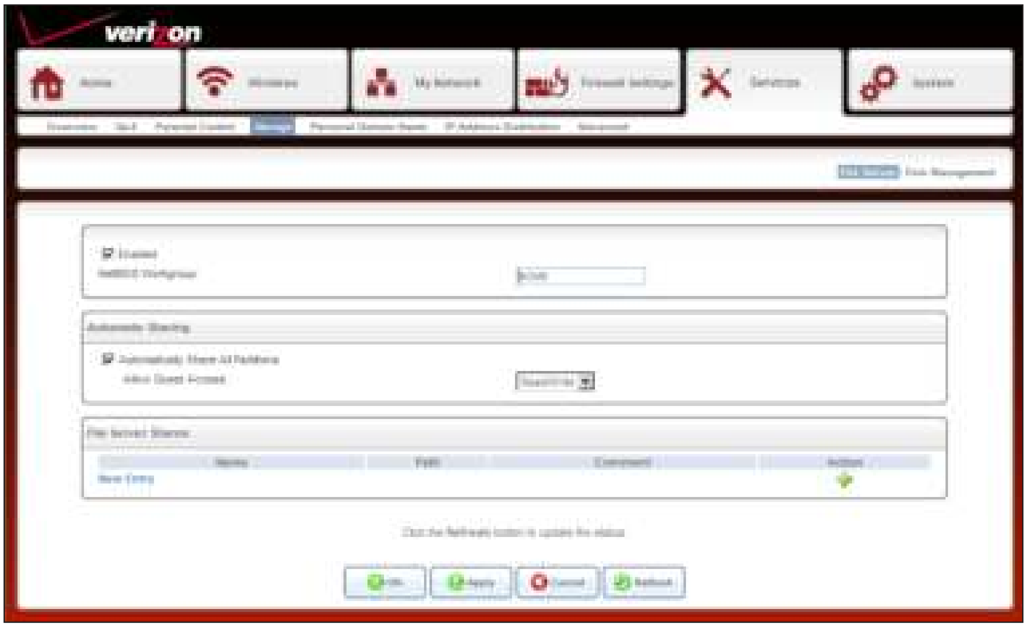
Access attempts	0
Allowed	0.00 %
Blocked	0.00 %

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

Storage

File Server

You can connect a USB thumb drive or external hard drive to the router and share it with users on your local network.



Enabled: Check to enable access to your USB drive.

NetBIOS Workgroup: Enter the name of your workgroup.

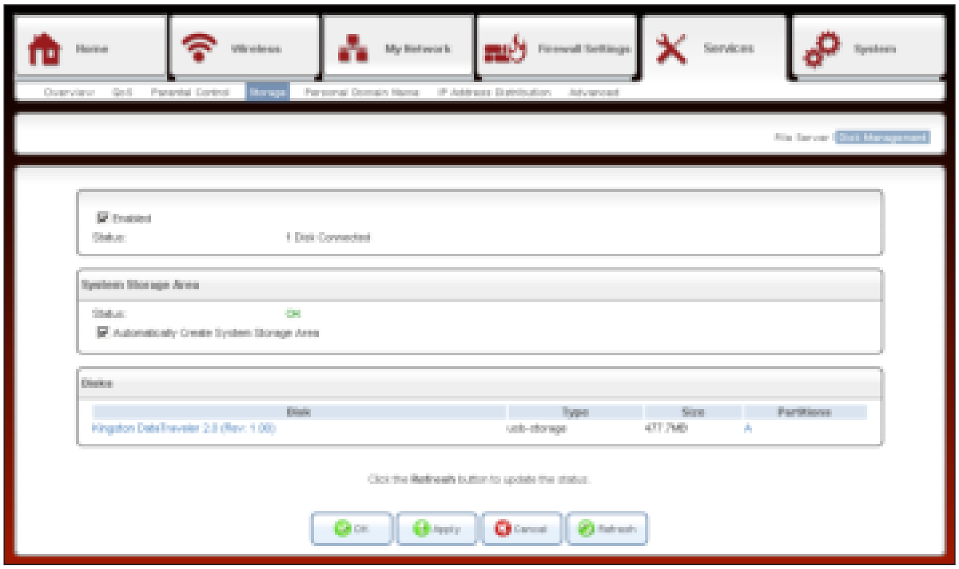
Automatically Share All Partitions: Check to automatically allow all partitions on your drive shared.

Allow Guest Access: Select the user rights for Guests - **Disabled**, **Read only**, or **Read/Write**.

File Server Shares: Your drive will appear here. Click the name of the drive to access the folders and files. Advanced users can click **New Entry** to assign specific users, groups to specific folders on your USB drive.

OK: Click **OK** to save your settings.

Disk Management



☑ Enabled

Status: 1 Disk Connected

System Storage Area

Status: OK

☑ Automatically Create System Storage Area

Disks

Disk	Type	Size	Partitions
Kingston DataTraveler 2.0 (Rev: 1.00)	usb-storage	477.7MB	A

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

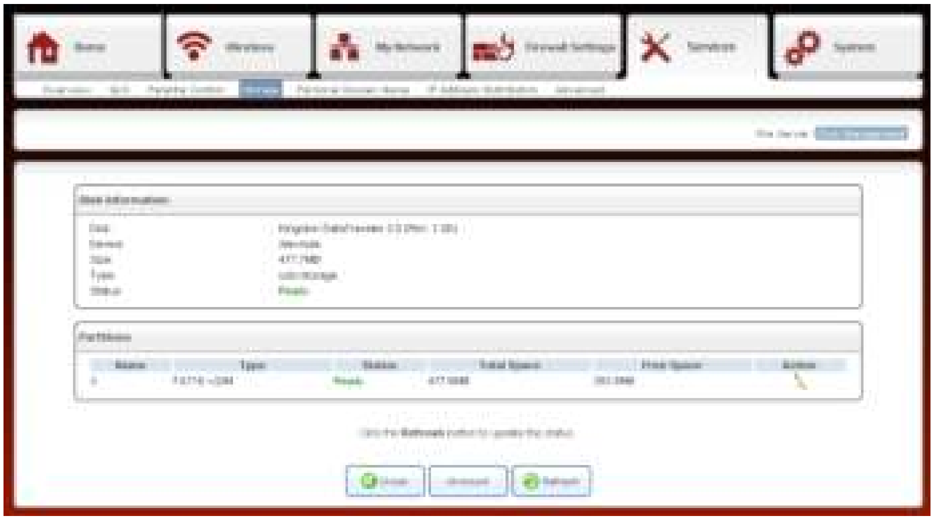
Enabled: Check to enable the disk management.

Status: Displays the status of your USB drive.

System Storage Area Status: Displays the status of the

Automatically Create System Storage Area: Check to automatically create a system storage area for your USB drive. The default partition name will be **A**. If you uncheck this box, you can rename the partition (storage area).

Disks: Displays information about your USB drive. Click on the Name of the drive to access more information about the drive (see below). Also, click the name under Partitions to view the files on your drive.



Disk Information

Disk: Kingston DataTraveler 2.0 (Rev: 1.00)

[illegible]

Size: 477.7MB

Type: usb-storage

Status: Ready

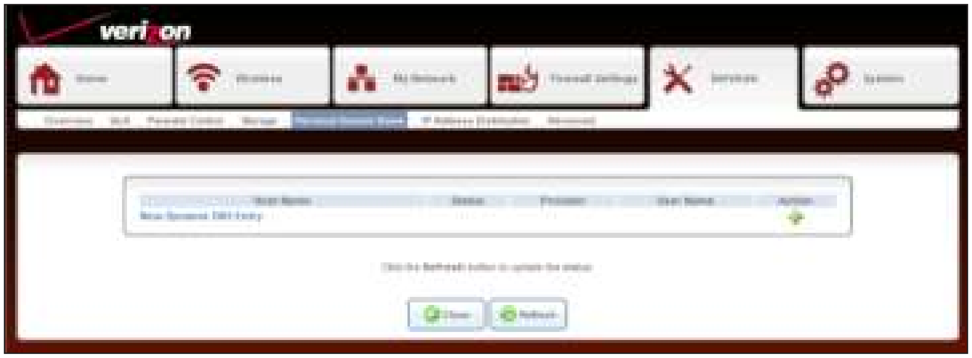
Partitions

Name	Type	Status	Total Space	Free Space	Action
A	[illegible]	Ready	[illegible]	[illegible]	

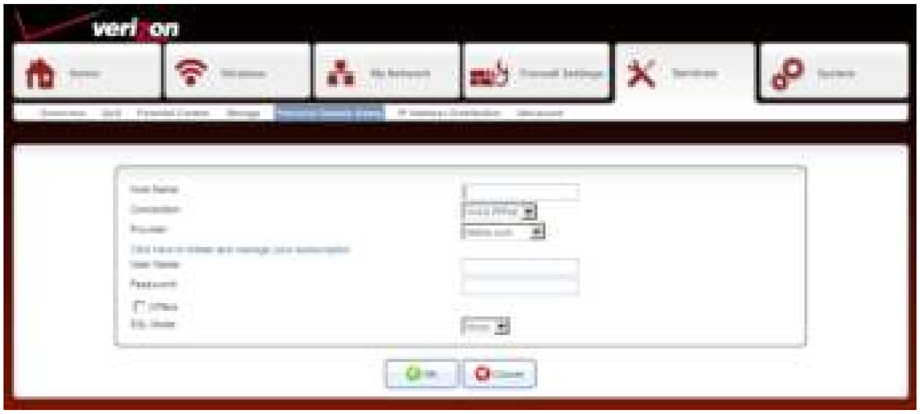
Click the **Refresh** button to update the status.

Personal Domain Name (DDNS)

Dynamic DNS is a dynamic IP address that can aliased to a static host name, allowing a computer on the network to be more easily accessible from the Internet.



To add your DDNS information, click **New Dynamic DNS Entry**.



Host Name: Enter your full DDNS domain name (e.g. myrouter.dyndns.org).

Connection: Select the connection to which you would like to couple the DDNS service. The DDNS service will only use the chosen device, unless failover is enabled. In this case, the failed-to device will be used instead (assuming its route rules consent), until the chosen device is up again.

Provider: Select your DDNS service provider. The screen will refresh, displaying the parameters required by each provider. The provider depicted herein is dyndns, which includes all available parameters.

User Name: Enter your DDNS user name.

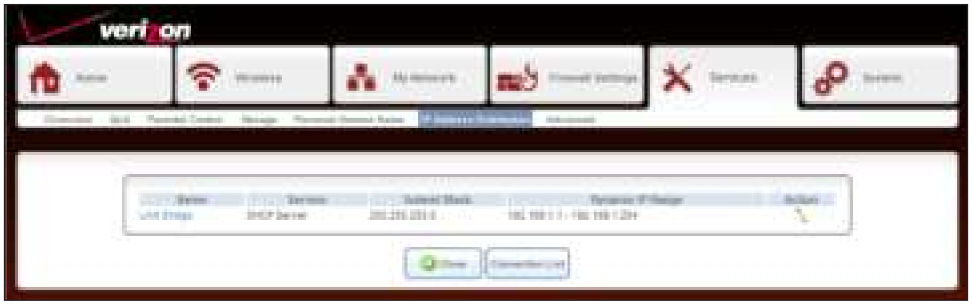
Password: Enter your DDNS password.

Offline: If you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), check this box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.

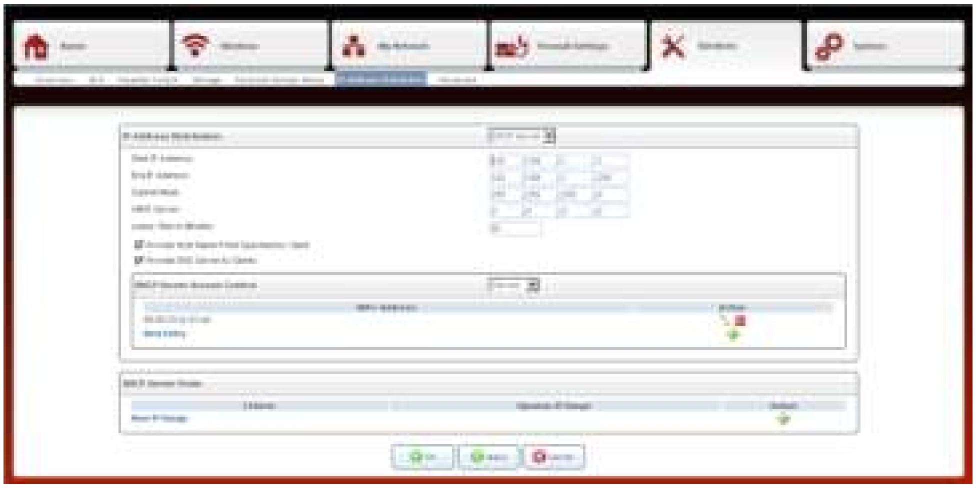
SSL Mode: With the gateway versions that support Secure Socket Layer (SSL), secured DDNS services are accessed using HTTPS. Upon connection, the gateway validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.

IP Address Distribution (DHCP)

Dynamic DNS is a dynamic IP address that can aliased to a static host name, allowing a computer on the network to be more easily accessible from the Internet.



Click **LAN Bridge** to configure.



IP Address Distribution: Select DHCP Server to have your Gateway assign IP settings to your Ethernet devices connected to the LAN ports.

Start IP Address: Enter the starting IP address in your DHCP range.

End IP Address: Enter the end IP address in your DHCP range.

Subnet Mask: Enter the subnet mask of your network.

WINS Server: Enter the IP address of your WINS server (optional).

Lease Time in Minutes: Enter the lease time (in minutes).

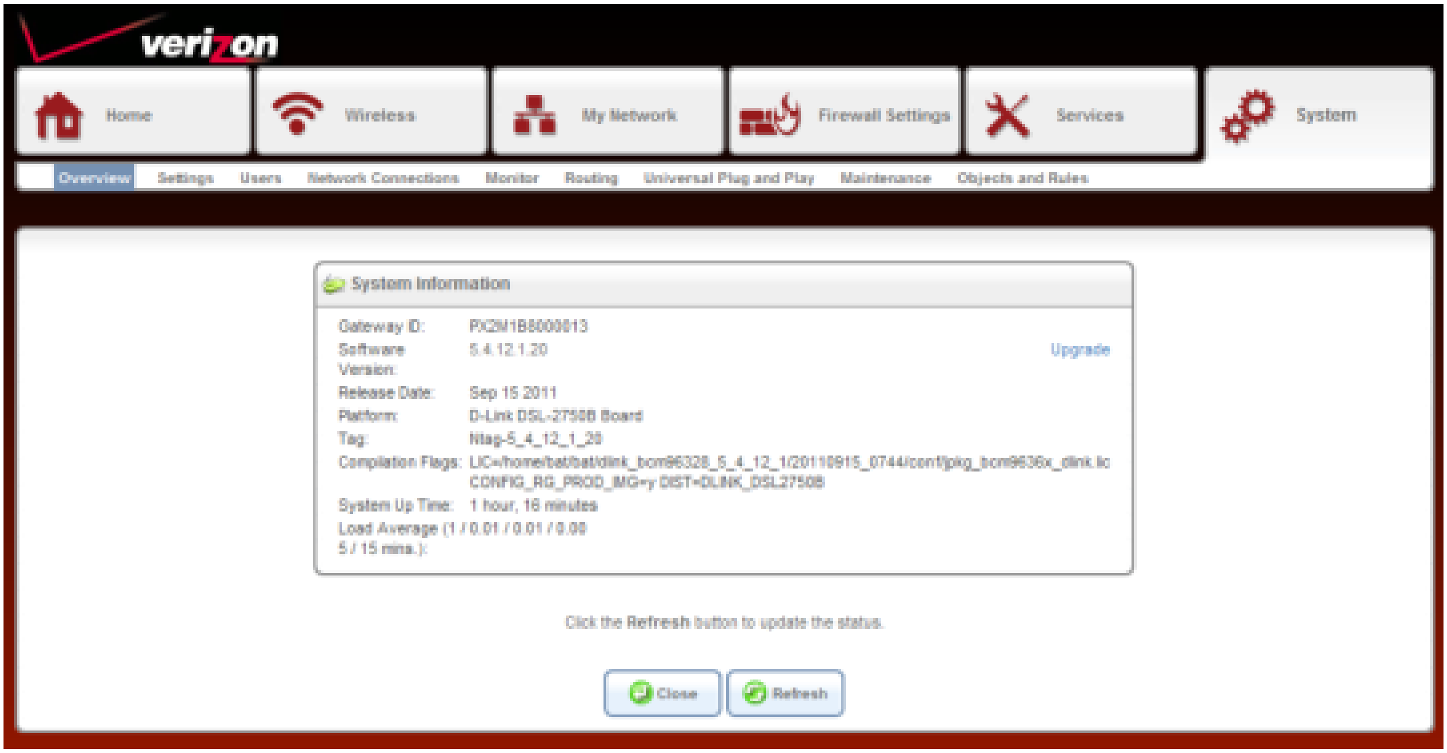
Provide Host Name: Check this box if you want the Gateway to assign a host name to your device if one is not supplied.

Provide DNS Server: Check this box to assign the DNS server to your devices.

DHCP Server Access Control: Select **Disable** (turn off option), **Served** (to have the Gateway assign IP settings to only the devices in the list), or **Denied** (to have the Gateway assign IP settings to all devices except for the ones in the list). Click **New Entry** to add devices to the list.

Overview

This section displays system information about the Gateway.



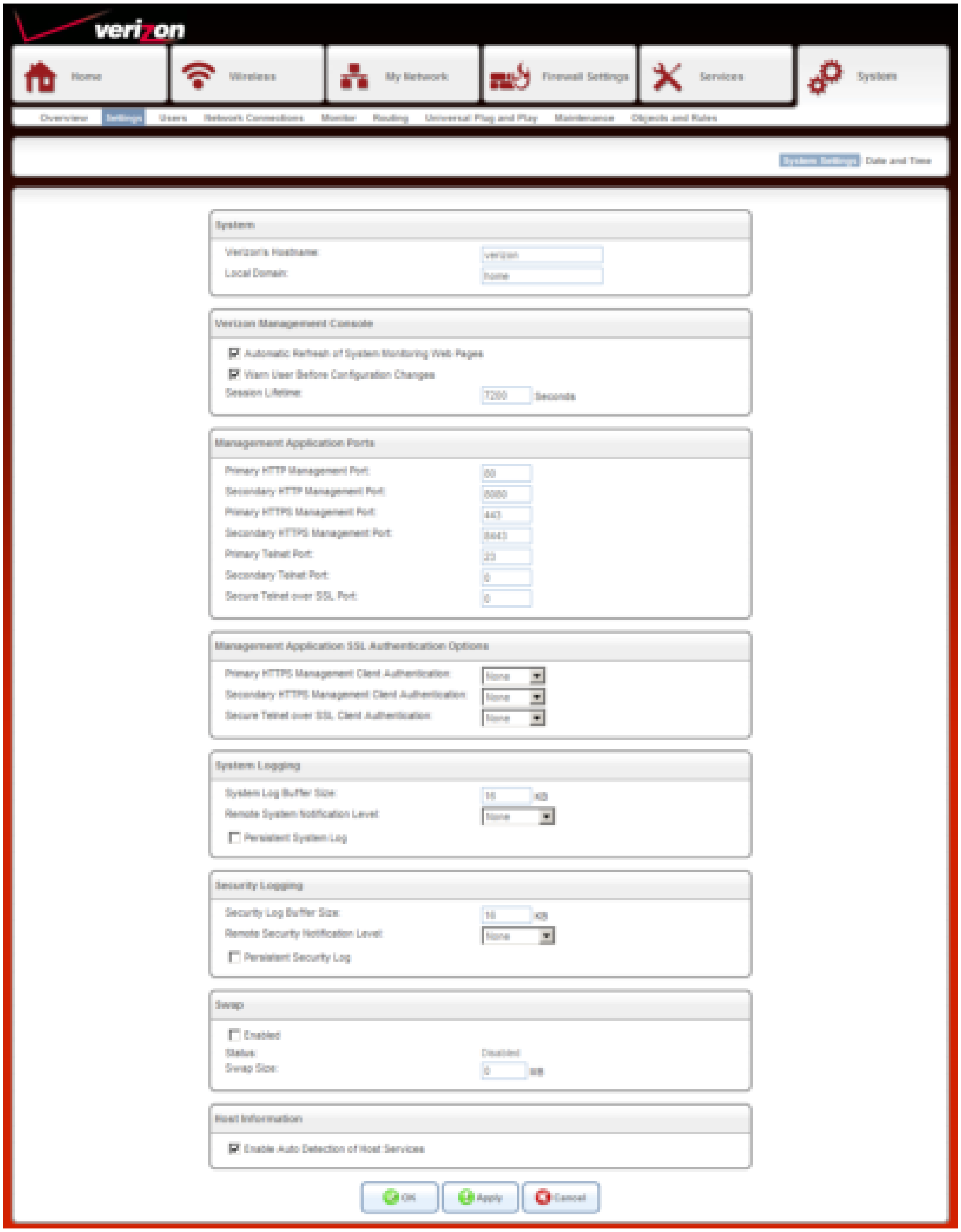
System Information

Gateway ID:	PX2M1B8000013	
Software Version:	5.4.12.1.20	Upgrade
Release Date:	Sep 15 2011	
Platform:	D-Link DSL-2750B Board	
Tag:	Ntag-5_4_12_1_20	
Compilation Flags:	LIC=/home/bat/bat/dlink_bcm96328_5_4_12_1/20110915_0744/conf/jpkg_bcm9636x_dlink.lic CONFIG_RG_PROD_IMG=y DIST=DLINK_DSL2750B	
System Up Time:	1 hour, 16 minutes	
Load Average (1 / 5 / 15 mins.):	0.01 / 0.01 / 0.00	

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

Settings

This section allows you to change system settings on the Gateway. It is strongly recommended not to change any of these settings. Click **Date and Time** on the right side to change the time and date on the Gateway (refer to the next page).



System

Verizon's Hostname: verizon
Local Domain: home

Verizon Management Console

☑ Automatic Refresh of System Monitoring Web Pages
☑ Warn User Before Configuration Changes
Session Lifetime: 7200 Seconds

Management Application Ports

Primary HTTP Management Port: 80
Secondary HTTP Management Port: 8080
Primary HTTPS Management Port: 443
Secondary HTTPS Management Port: 8443
Primary Telnet Port: 23
Secondary Telnet Port: 0
Secure Telnet over SSL Port: 0

Management Application SSL Authentication Options

Primary HTTPS Management Client Authentication: None
Secondary HTTPS Management Client Authentication: None
Secure Telnet over SSL Client Authentication: None

System Logging

System Log Buffer Size: 16 KB
Remote System Notification Level: None
☐ Persistent System Log

Security Logging

Security Log Buffer Size: 16 KB
Remote Security Notification Level: None
☐ Persistent Security Log

Swap

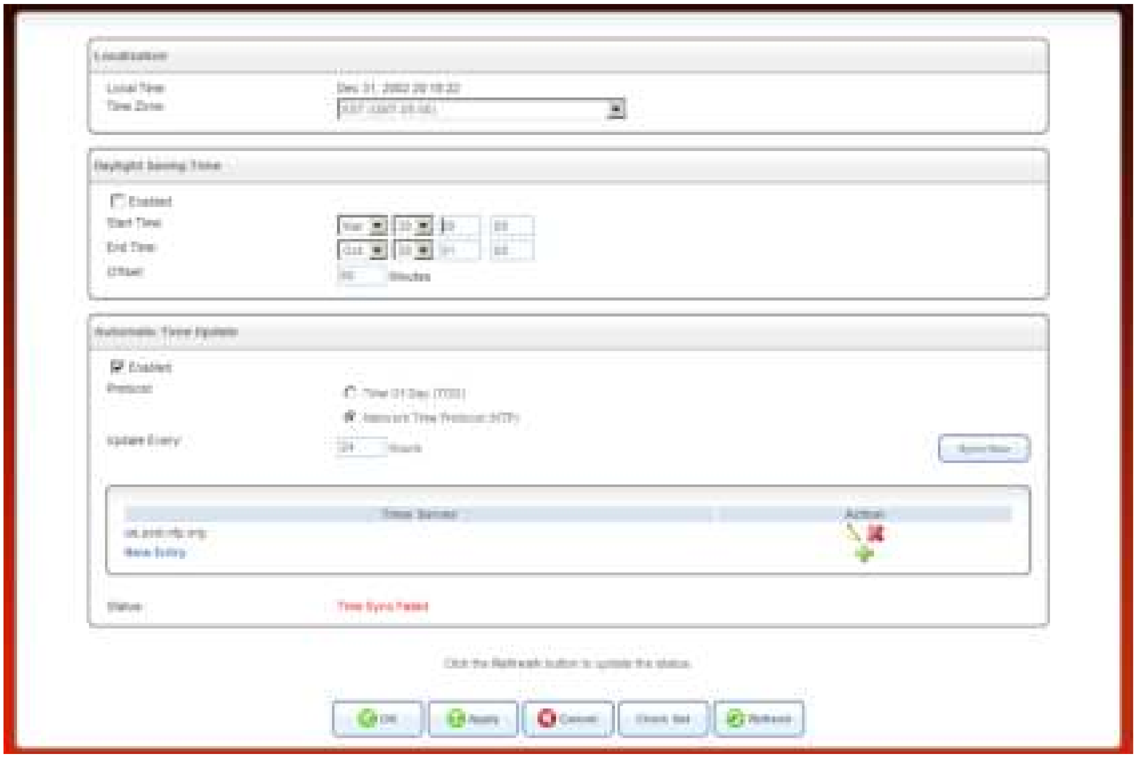
☐ Enabled
Status: Disabled
Swap Size: 0 KB

Host Information

☑ Enable Auto Detection of Host Services

Date and Time

This feature allows you to set the date and time values on your Gateway.



Localization

Local Time Dec 31, 2002 20:18:22

Time Zone EST (GMT-05:00)

Daylight Saving Time

□ Enabled

Start Time Mar [illegible] [illegible] [illegible]

End Time Oct [illegible] [illegible] [illegible]

Offset 60 Minutes

Automatic Time Update

☑ Enabled

Protocol ○ Time Of Day (TOD)

● Network Time Protocol (NTP)

Update Every 24 Hours

Time Server	Action
us.pool.ntp.org	
New Entry	

Status Time Sync Failed

Click the Refresh button to update the status.

Local Time: Displays the current Gateway date and time.

Time Zone: Select your time zone from the drop-down menu.

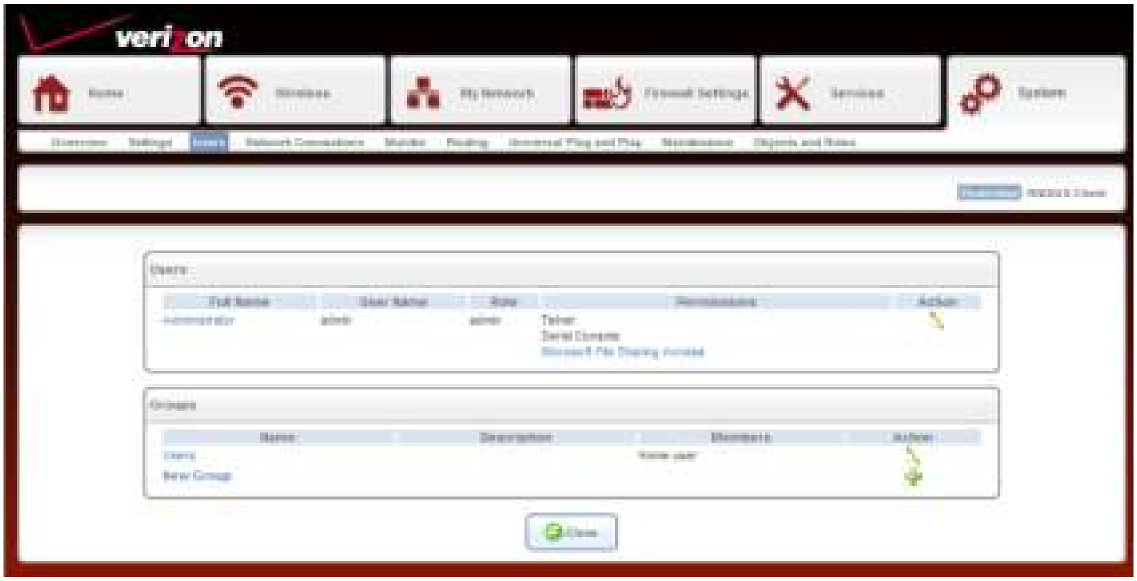
Daylight Saving Time: Check to enable daylight saving time and then enter the desired Start and End values in the fields provided. Click **Apply** to save the settings.

Automatic Time Update: Check the Enable box to use a time server. Check either TOD or NTP protocol and then enter the *Update Every* box with a value (in hours). Click **Sync Now** to connect to the server.

You may use the default server or add your own server information by clicking **New Entry**.

Overview

The **System** > **Users** page allows you to create users and groups, and assign permissions. Administrator is the default user.



Users

Full Name	User Name	Role	Permissions	Action
Administrator	admin	admin	Telnet Serial Console Microsoft File Sharing Access	

Groups

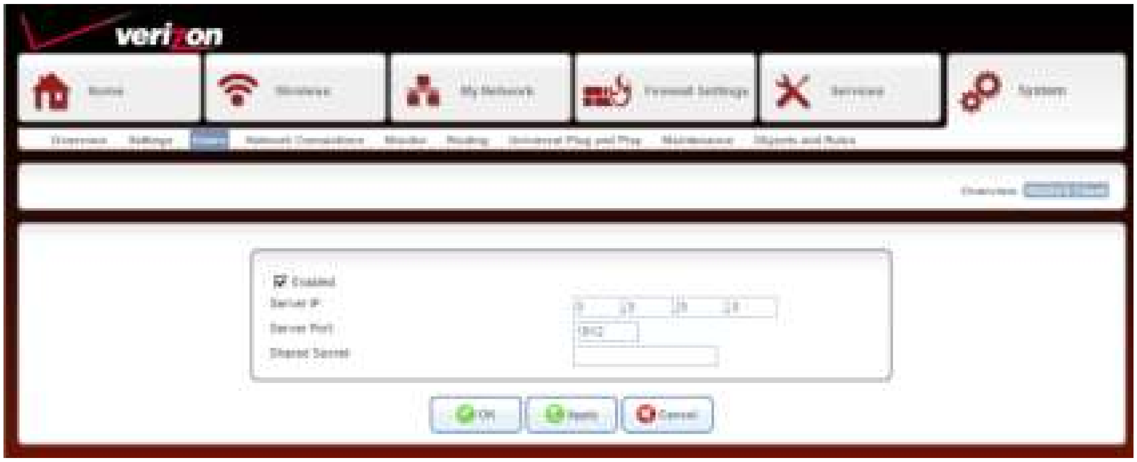
Name	Description	Members	Action
Users		Home user	
New Group			

Users: Displays active users, roles, and permissions. Under Action, you can click the pencil icon to edit the user's settings, the green + to add a user, or the red X to delete the user.

Groups: Displays active group, description, and members (users assign to that group). Under Action, you can click the pencil icon to edit the group's settings, the green + to add a group, or the red X to delete the group.

RADIUS Client

This page allows you to use a RADIUS server to authenticate users to log into the router.



☑ Enabled

Server IP 0 . 0 . 0 . 0

Server Port 1812

Shared Secret

Enabled: Check this box to enable RADIUS server authentication.

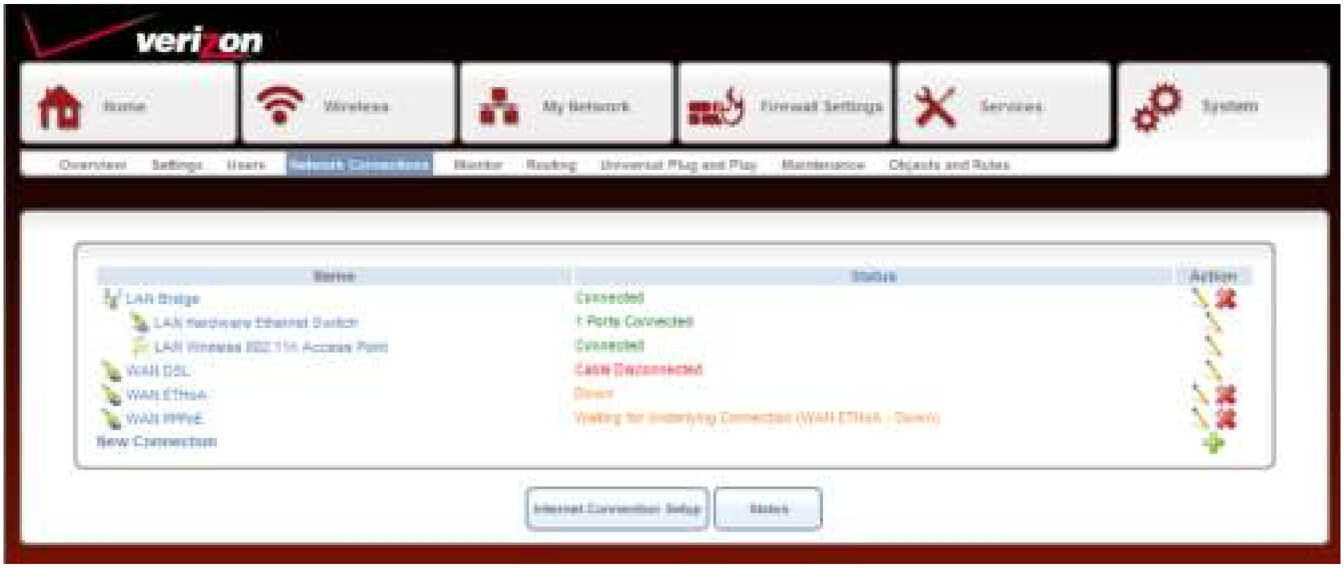
Server IP: Enter the IP address of the RADIUS server.

Server Port: Enter the port used.

Shared Secret: Enter the shared secret (passphrase).

Network Connections

This page will display the status of your network connections. You may add, edit, and delete these connections.



Name	Status	Action
LAN Bridge	Connected	✎ ✖
LAN Hardware Ethernet Switch	1 Ports Connected	✎
LAN Wireless 802.11n Access Point	Connected	✎
WAN DSL	Cable Disconnected	✎
WAN ETHoA	Down	✎ ✖
WAN PPPoE	Waiting for Underlying Connection (WAN ETHoA - Down)	✎ ✖
New Connection		+

Name: Displays the name of the connection. Click on the name to edit.

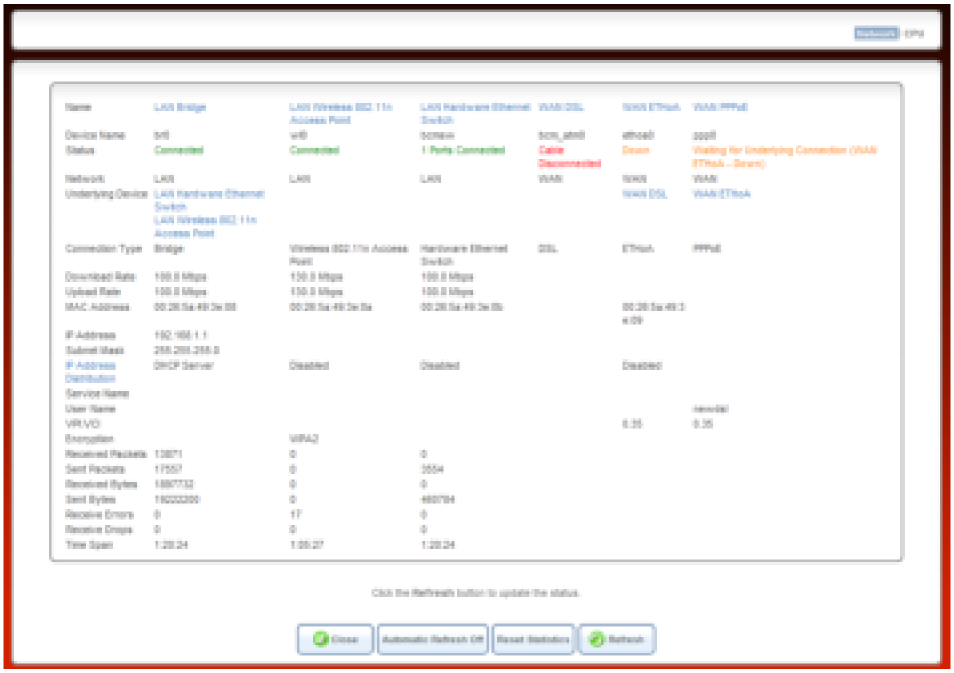
Status: Displays the status of the connection.

Action: Click the pencil icon to edit the connection, the green + icon to add a new connection, or the red X to delete the connection.

New Connection: Click to add a new connection.

Network

This page will display network statistics on the Gateway.

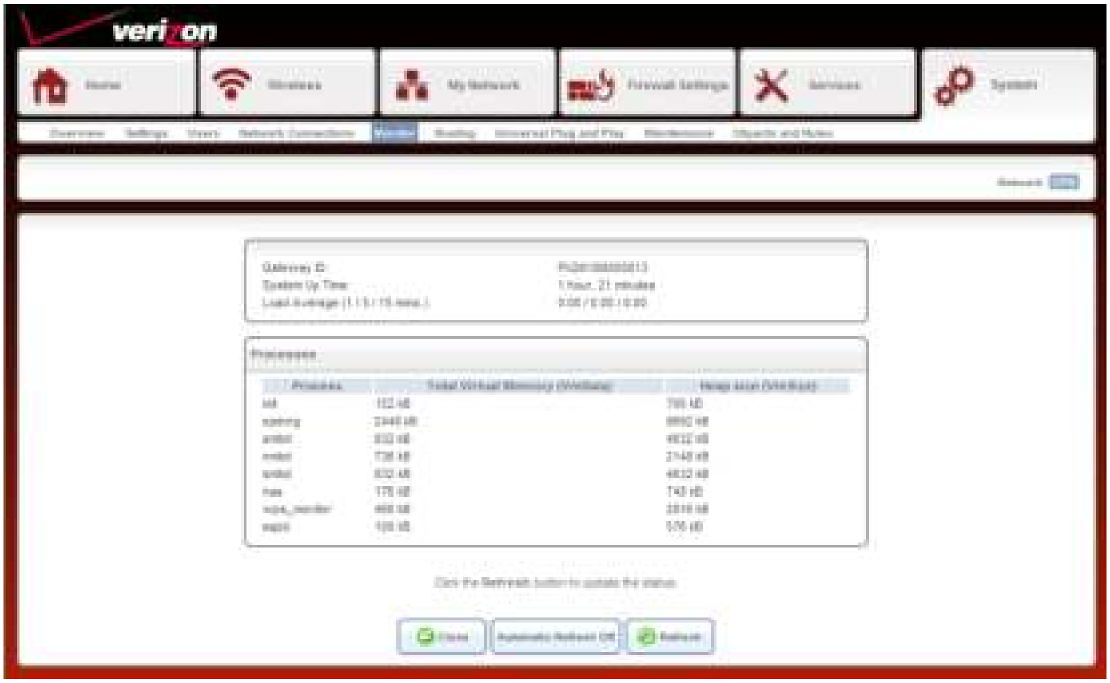


Name	LAN Bridge	LAN Wireless 802.11n Access Point	LAN Hardware Ethernet Switch	WAN DSL	WAN ETHoA	WAN PPPoE
Device Name	br0	wl0	bcmsw	bcm_atm0	atm0	ppp0
Status	Connected	Connected	1 Ports Connected	Cable Disconnected	Down	Waiting for Underlying Connection (WAN ETHoA - Down)
Network	LAN	LAN	LAN	WAN	WAN	WAN
Underlying Device	LAN Hardware Ethernet Switch LAN Wireless 802.11n Access Point				WAN DSL	WAN ETHoA
Connection Type	Bridge	Wireless 802.11n Access Point	Hardware Ethernet Switch	DSL	ETHoA	PPPoE
Download Rate	100.0 Mbps	150.0 Mbps	100.0 Mbps			
Upload Rate	100.0 Mbps	150.0 Mbps	100.0 Mbps			
MAC Address	00:26:5a:49:3e:08	00:26:5a:49:3e:0a	00:26:5a:49:3e:0b		00:26:5a:49:3e:09	
IP Address	192.168.1.1					
Subnet Mask	255.255.255.0					
IP Address Distribution	DHCP Server	Disabled	Disabled		Disabled	
Service Name						
User Name						[illegible]
VPI/VCI					0.35	0.35
Encryption		WPA2				
Received Packets	13871	0	0			
Sent Packets	17557	0	3554			
Received Bytes	1887732	0	0			
Sent Bytes	19222200	0	460794			
Receive Errors	0	17	0			
Receive Drops	0	0	0			
Time Span	1:20:24	1:05:27	1:20:24			

Click the Refresh button to update the status.

CPU

This page will display the Gateway's CPU statistics.



Gateway ID:	PLD01000000013
System Up Time:	1 hour, 21 minutes
Load Average (1 / 5 / 15 mins.):	0.00 / 0.00 / 0.00

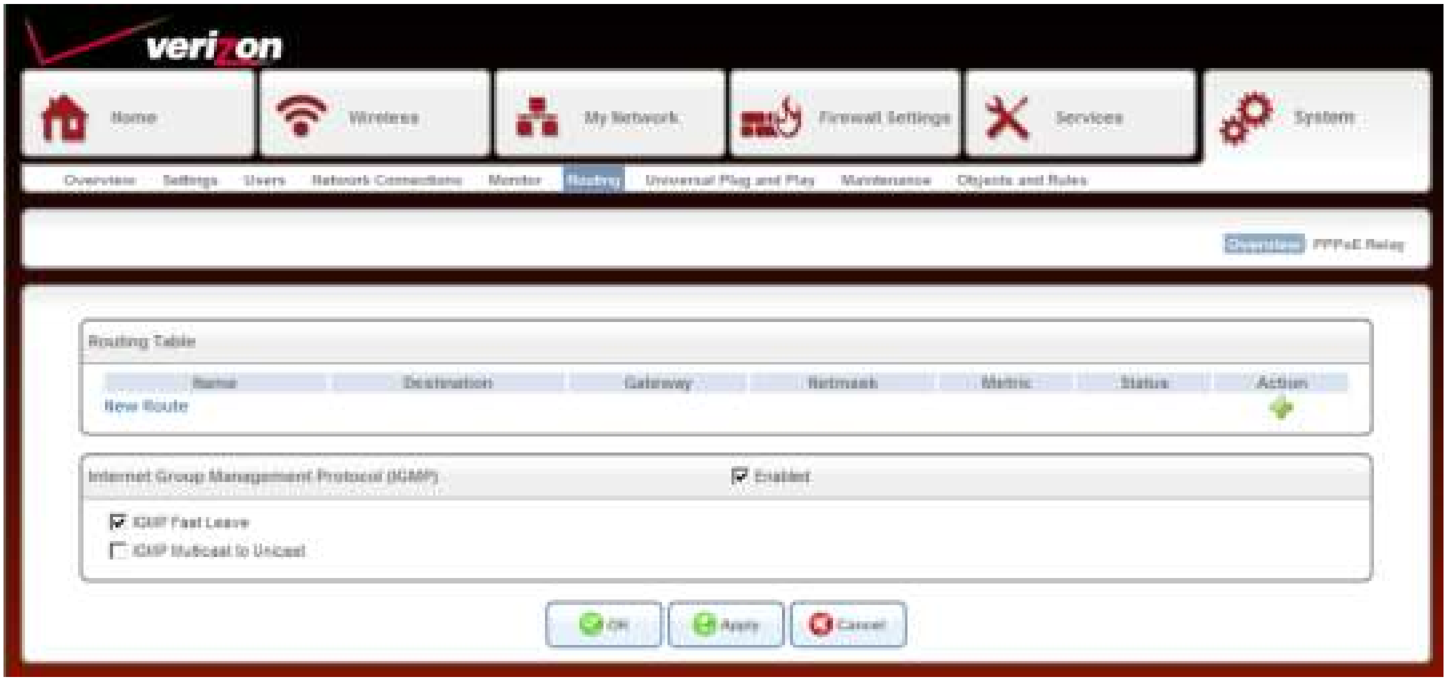
Processes

Process	Total Virtual Memory (VmData)	Heap size (VmRSS)
init	152 kB	700 kB
[illegible]	2348 kB	8892 kB
smbd	832 kB	4832 kB
nmbd	736 kB	2148 kB
smbd	832 kB	4832 kB
[illegible]	176 kB	740 kB
wps_monitor	468 kB	2316 kB
[illegible]	108 kB	576 kB

Click the Refresh button to update the status.

Routing

Overview



Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						✚

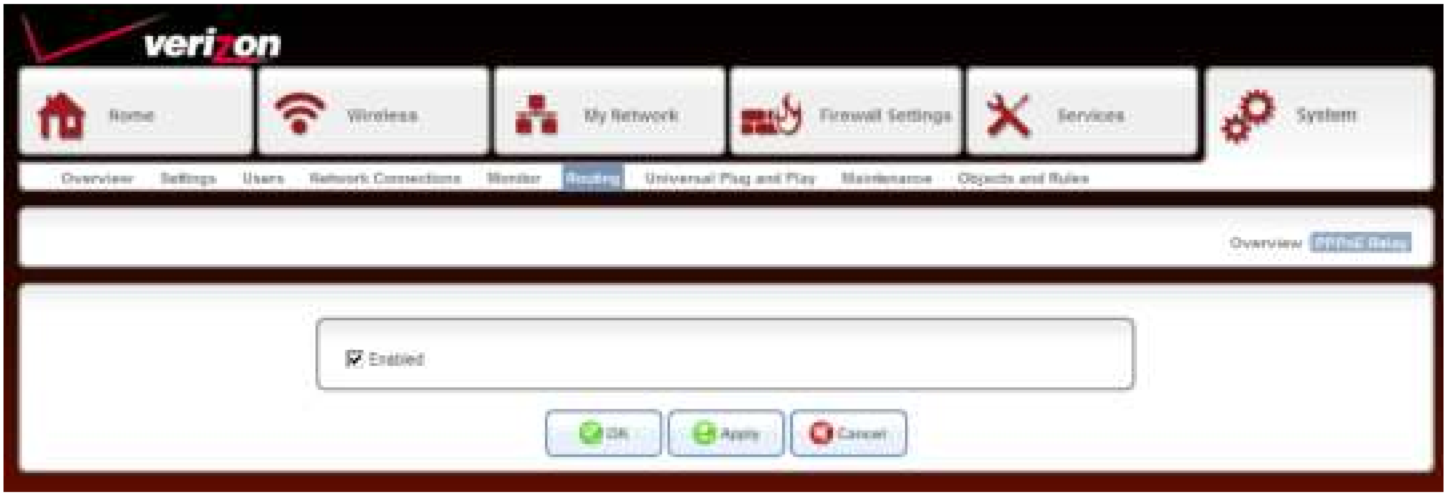
Internet Group Management Protocol (IGMP) ☑ Enabled

☑ IGMP Fast Leave

□ IGMP Multicast to Unicast

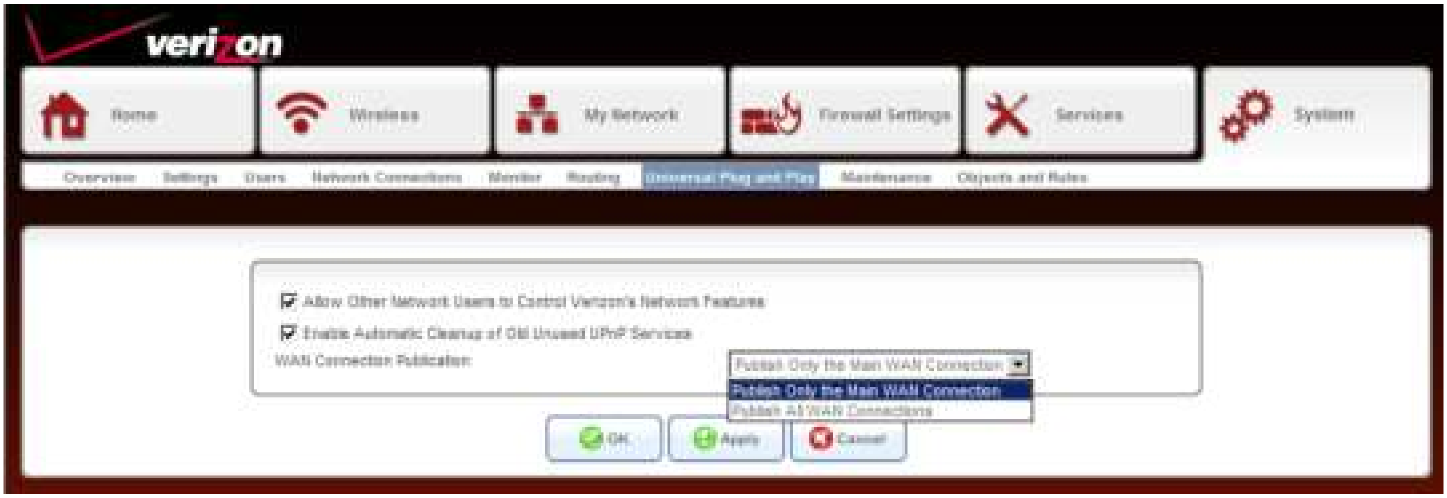
The routing table will display any routes. Check the IGMP Enabled box and check to enable IGMP Fast Leave and/or IGMP Multicast to Unicast. Click **OK** to save your settings.

PPPoE Relay



☑ Enabled

Check the Enabled box to activate PPPoE relay. Click **OK** to save your settings.



☑ Allow Other Network Users to Control Verizon's Network Features

☑ Enable Automatic Cleanup of Old Unused UPnP Services

WAN Connection Publication: Publish Only the Main WAN Connection

Publish Only the Main WAN Connection
Publish All WAN Connections

Allow Other Network Users to Control Verizon's Network Features: Check this box to broadcast the router to all computers on your local network. You computer (if UPnP is enabled on your computer) will detect the router as a UPnP device.

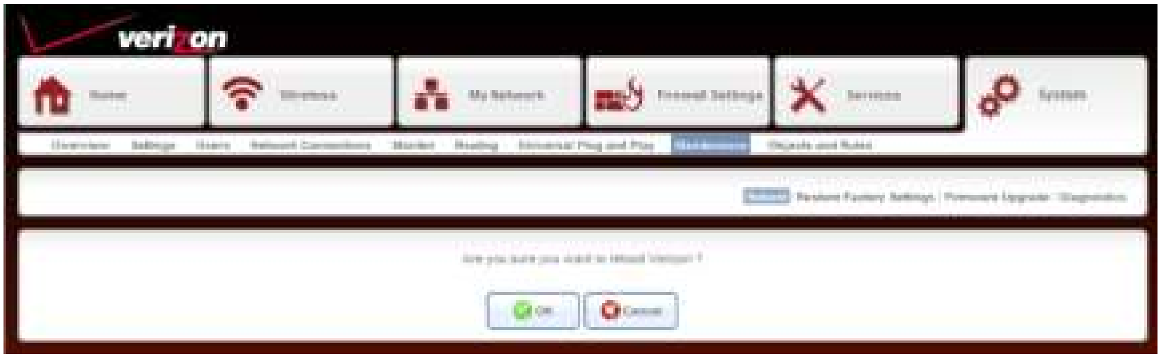
Enable Automatic Cleanup of Old Unused UPnP Services: Check this box to have the Gateway automatically remove unused UPnP services.

WAN Connection Publication: Select **Publish Only the Main WAN Connection**.

OK: Click **OK** to save your settings.

Maintenance

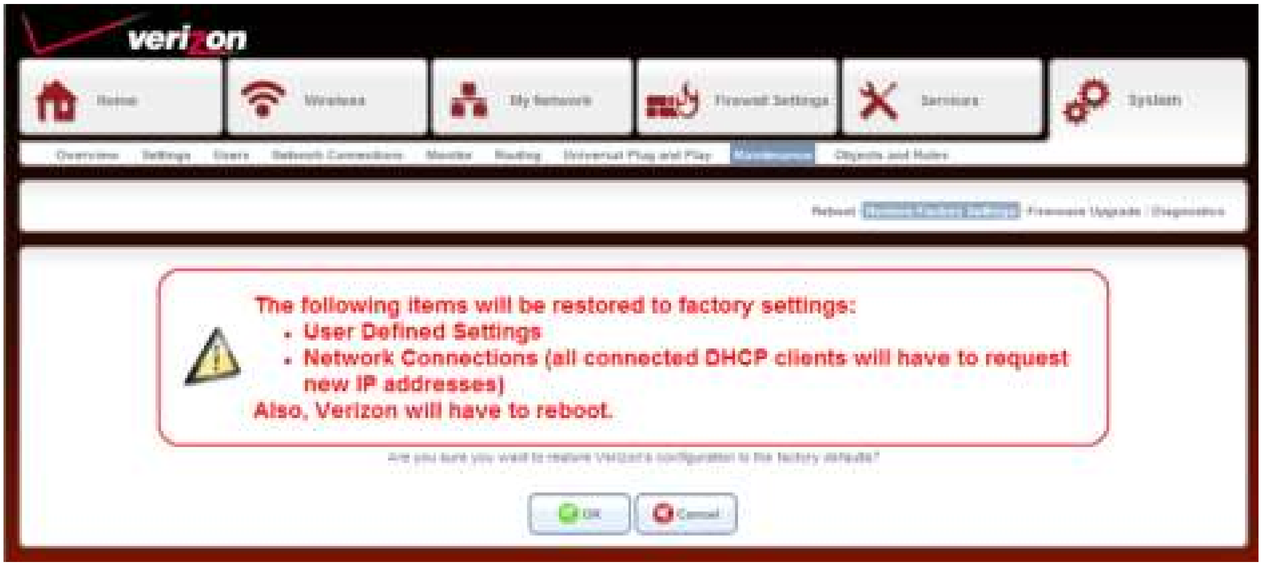
Reboot



Are you sure you want to reboot Verizon ?

Click **OK** to reboot the Gateway.

Restore Factory Settings

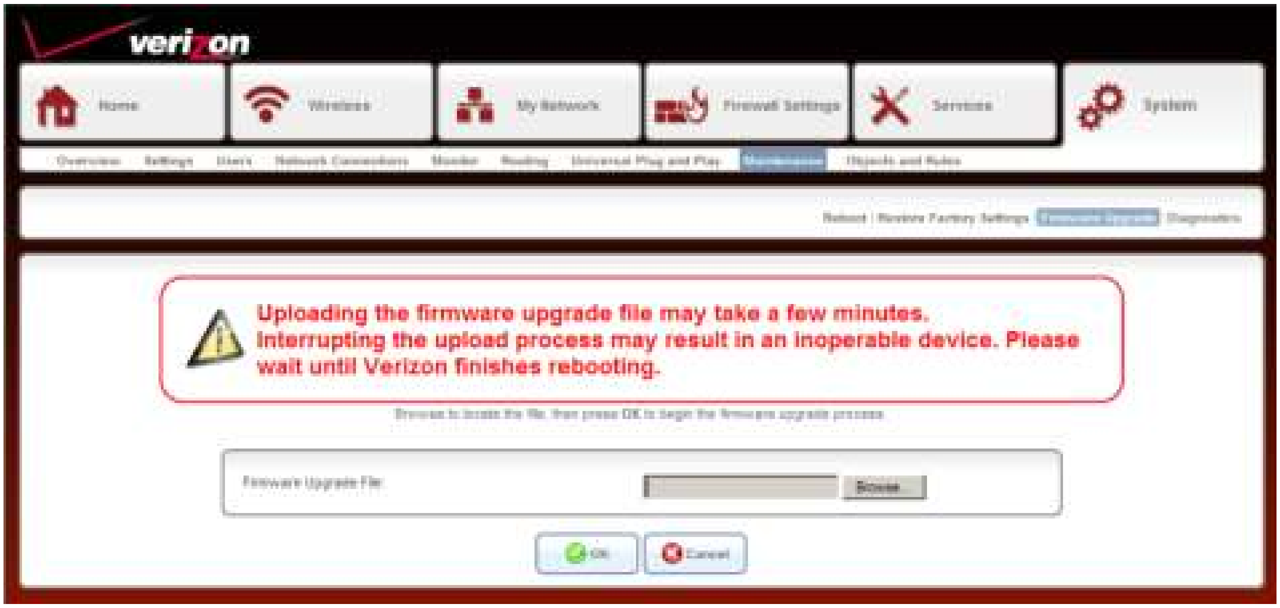


The following items will be restored to factory settings:
- User Defined Settings
- Network Connections (all connected DHCP clients will have to request new IP addresses)

Also, Verizon will have to reboot.

Are you sure you want to restore Verizon's configuration to the factory defaults?

Click **OK** to reset the Gateway to the default factory settings. All rules, users, groups, etc you configured will be lost.



Uploading the firmware upgrade file may take a few minutes. Interrupting the upload process may result in an inoperable device. Please wait until Verizon finishes rebooting.

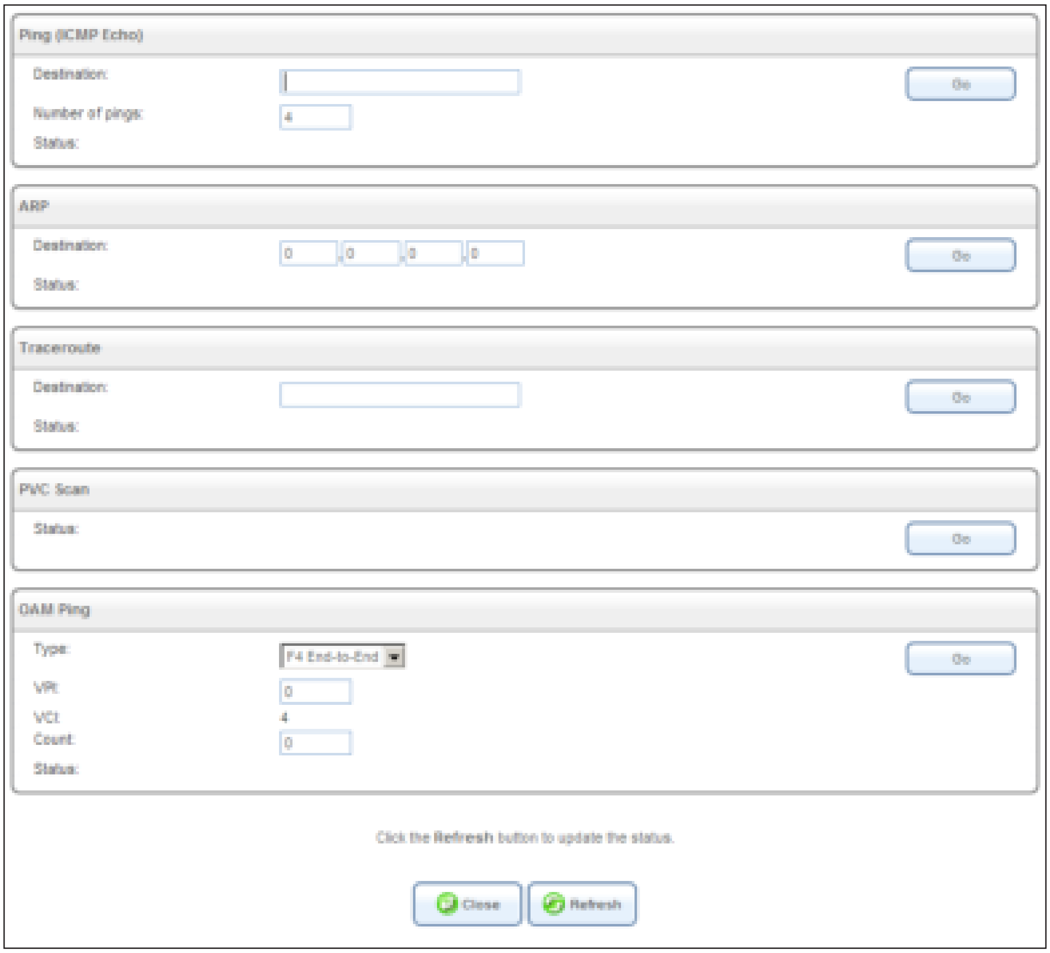
Browse to locate the file, then press OK to begin the firmware upgrade process.

Firmware Upgrade File: [Browse]

Visit the Verizon website to download a firmware upgrade file to your computer if available. Click **Browse** and then navigate to the location of the upgrade file; the path will appear in the window. Next, click **OK** to begin the upload to your Gateway.

Diagnostics

This page will allow you to test different connection using Ping, ARP, Traceroute, PVC Scan, and OAM Ping. Enter the IP address of your target (destination) and adjust settings if needed, then click **Go**. The results will appear next to *Status*.



Ping (ICMP Echo)

Destination:

Number of pings: 4

Status:

ARP

Destination: 0 . 0 . 0 . 0

Status:

Traceroute

Destination:

Status:

PVC Scan

Status:

OAM Ping

Type: F4 End-to-End

VPI: 0

VCI: 4

Count: 0

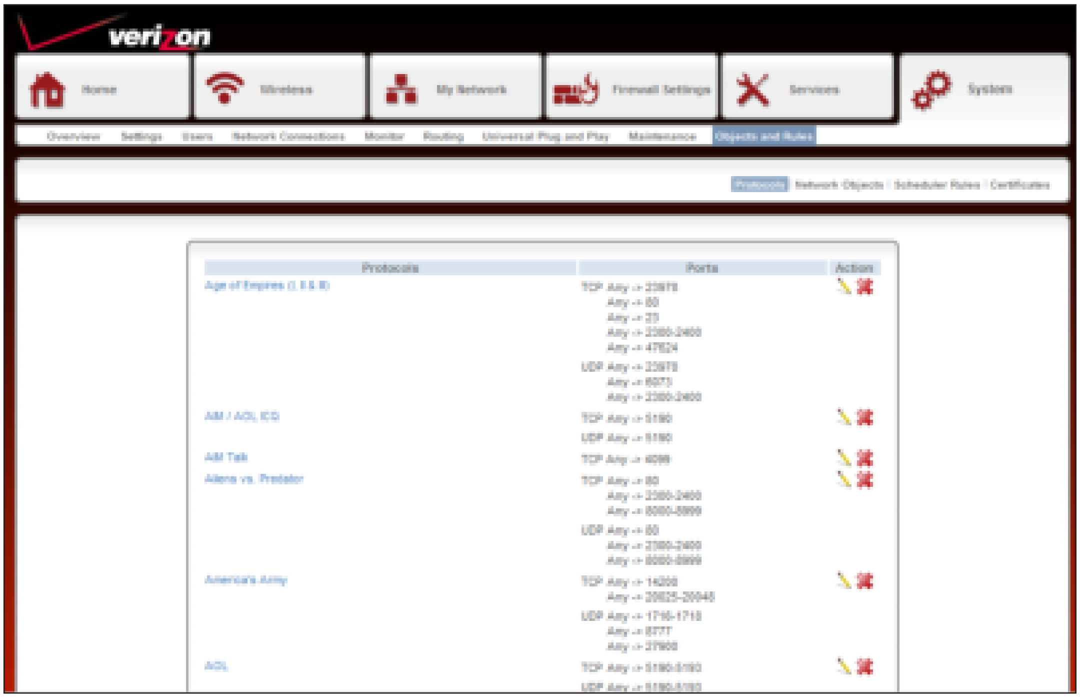
Status:

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

Objects and Rules

Protocols

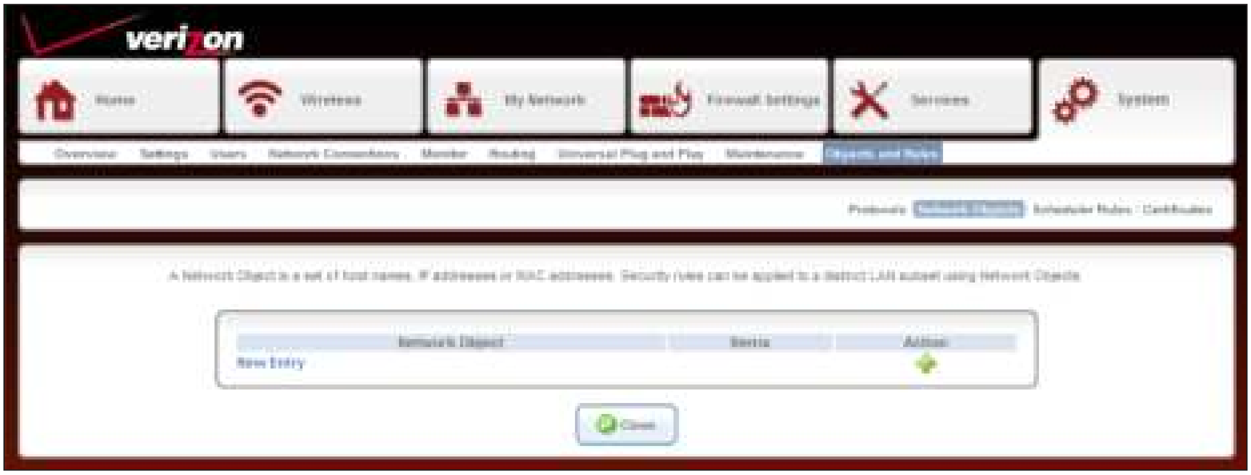
The Protocols page will display all the default and user-created services and their port information. This is used for the Port Forwarding and Port Triggering features. You may click the pencil icon to edit the item, click the red X to remove the item, or scroll all the way to the bottom and click **New Entry** on the left side to create a new protocol.



Protocols	Ports	Action
Age of Empires (I, II & III)	TCP Any -> 23978 Any -> 80 Any -> 23 Any -> 2300-2400 Any -> 47624 UDP Any -> 23978 Any -> 6073 Any -> 2300-2400	✎ ✖
AIM / AOL ICQ	TCP Any -> 5190 UDP Any -> 5190	✎ ✖
AIM Talk	TCP Any -> 4099	✎ ✖
Aliens vs. Predator	TCP Any -> 80 Any -> 2300-2400 Any -> 8000-8999 UDP Any -> 80 Any -> 2300-2400 Any -> 8000-8999	✎ ✖
America's Army	TCP Any -> 14200 Any -> 20025-20045 UDP Any -> 1716-1718 Any -> 8777 Any -> 27900	✎ ✖
AOL	TCP Any -> 5190-5193 UDP Any -> 5190-5193	✎ ✖

Network Objects

Network objects are devices on your local network such as computers, game consoles, media players, Internet TVs, and network storage (NAS) devices, or a specific IP address or a range of IP address. You can add a network object by clicking **New Entry**.

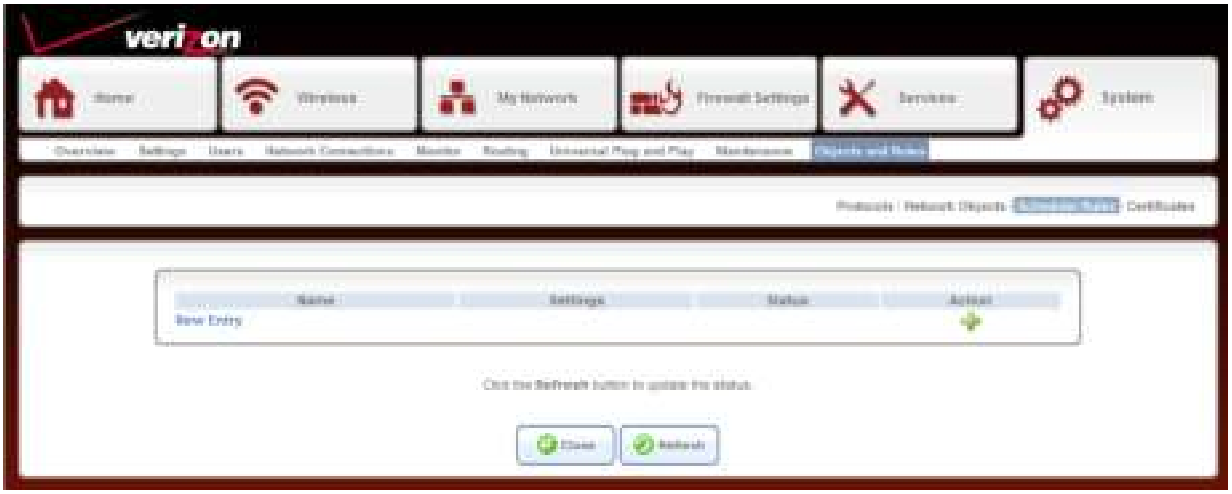


A Network Object is a set of host names, IP addresses or MAC addresses. Security rules can be applied to a distinct LAN subnet using Network Objects.

Network Object	Items	Action
New Entry		✚

Scheduler Rules

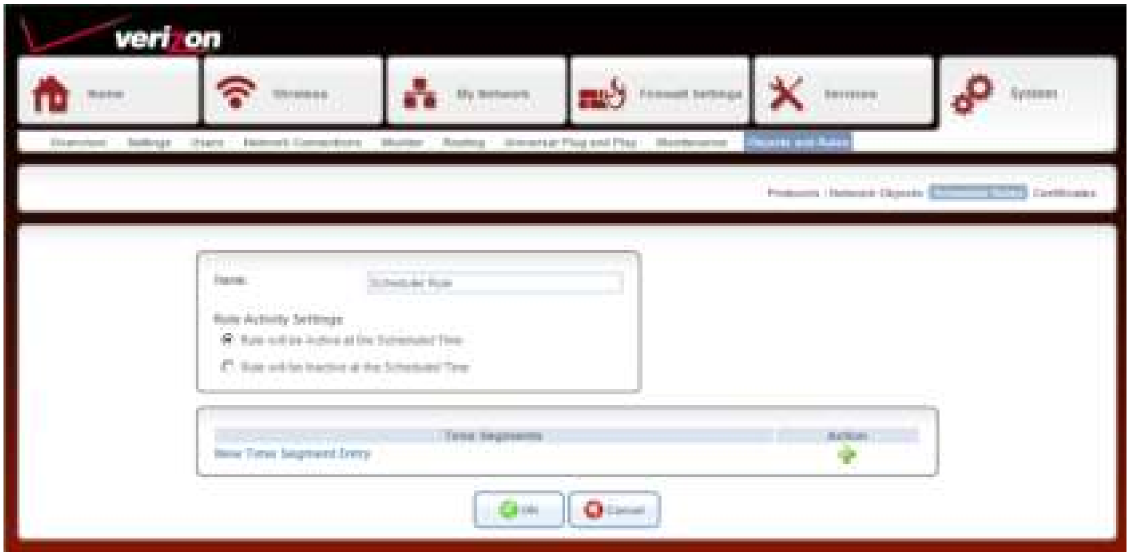
Scheduler Rules will allow you to set up a specific schedule that you can apply to parental control and firewall features. For example if you want to block your kids' computers from the Internet at certain times, you can create a schedule that specifies the day and time you want blocked, and then apply that schedule to a firewall rule. Click **New Entry** or the green + icon.



Name	Settings	Status	Action
New Entry			✚

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

Click **New Entry** or the green + icon under *Action* and the following screen will appear.



Name: Scheduler Rule

Rule Activity Settings:

- ● Rule will be Active at the Scheduled Time
- ○ Rule will be Inactive at the Scheduled Time

Time Segments	Action
New Time Segment Entry	✚

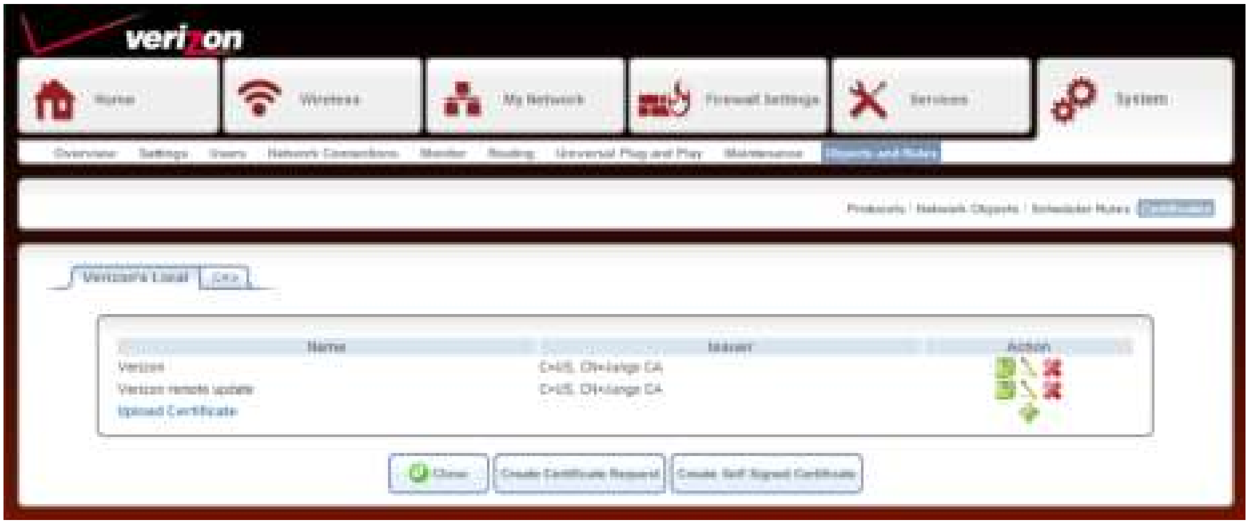
Name: Enter a name for your rule.

Rule Activity Settings: Select either the time frame is going to be active or inactive.

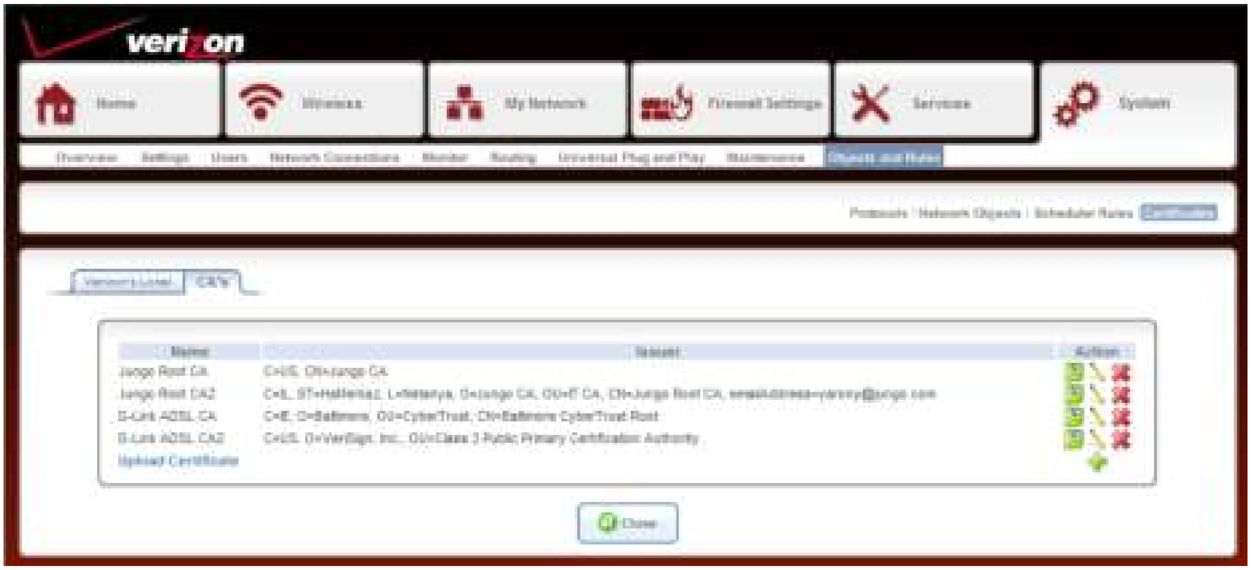
New Time Segment Entry: Click to enter the time frame you want for the rule.

OK: Click to save your rule.

Certificates



Name	Issuer	Action
Verizon	C=US, CN=Jungo CA	
Verizon remote update	C=US, CN=Jungo CA	
Upload Certificate		

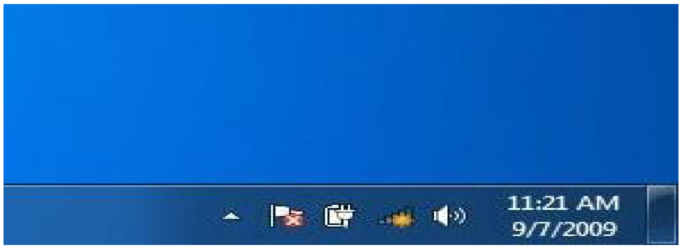


Name	Issuer	Action
Jungo Root CA	C=US, CN=Jungo CA	
Jungo Root CA2	C=IL, ST=HaMerkaz, L=Netanya, O=Jungo CA, OU=IT CA, CN=Jungo Root CA, emailAddress=yaronv@jungo.com	
D-Link ADSL CA	C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	
D-Link ADSL CA2	C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority	
Upload Certificate		

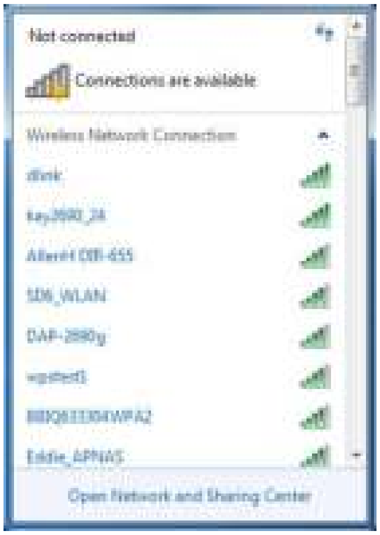
Connect to your Wireless Network
Windows® 7

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



2. The utility will display any available wireless networks in your area.



Not connected

Connections are available

Wireless Network Connection

dlink

kay2690_24

Allen## DIR-655

SDN_WLAN

DAP-2590g

wpstest3

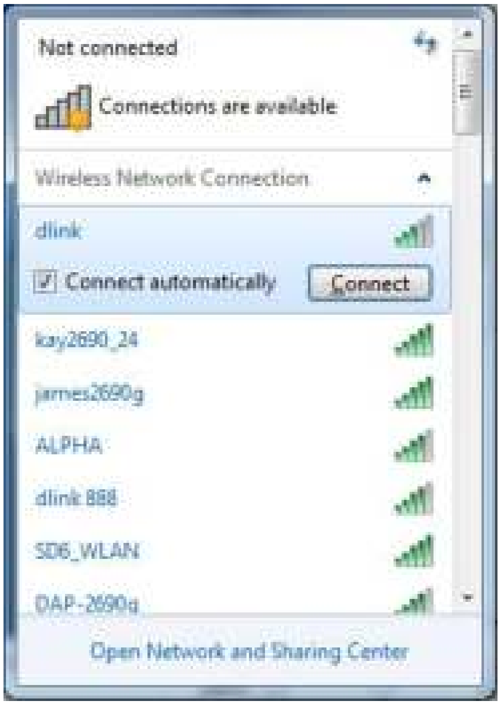
BBQ633304WPA2

Eddie_APNAS

Open Network and Sharing Center

3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



Not connected

Connections are available

Wireless Network Connection

dlink

☑ Connect automatically

kay2690_24

james2690g

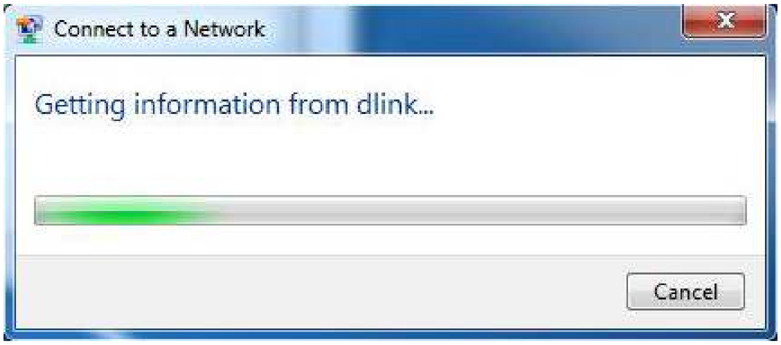
ALPHA

dlink 888

SD6_WLAN

DAP-2690g

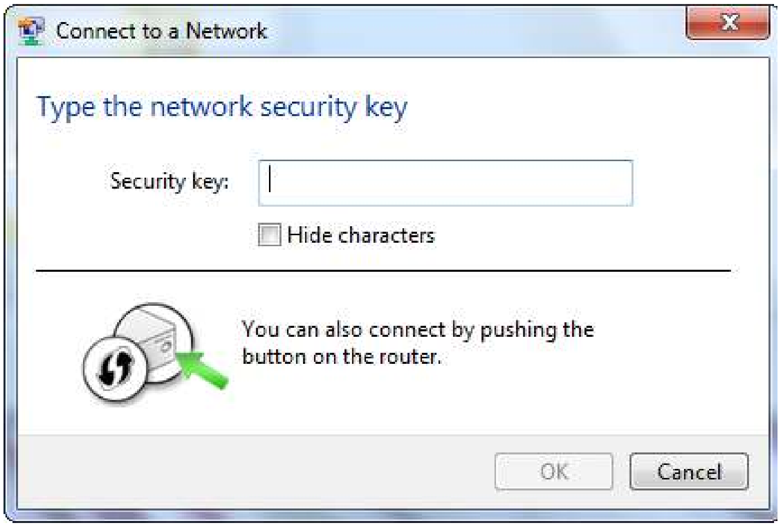
4. The following window appears while your computer tries to connect to the Gateway.



Connect to a Network

Getting information from dlink...

5. Enter the same passphrase that is on your Gateway and click **Ok**.



Connect to a Network

Type the network security key

Security key:

□ Hide characters

You can also connect by pushing the button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The passphrase must be exactly the same as on the Gateway.

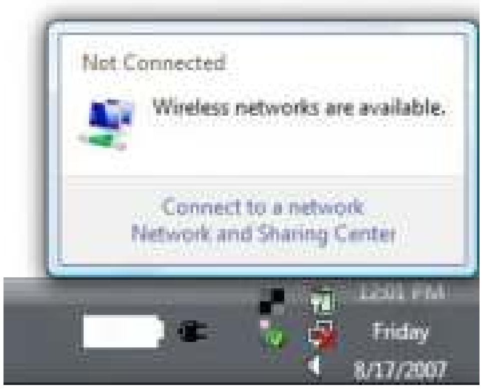
Using Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.

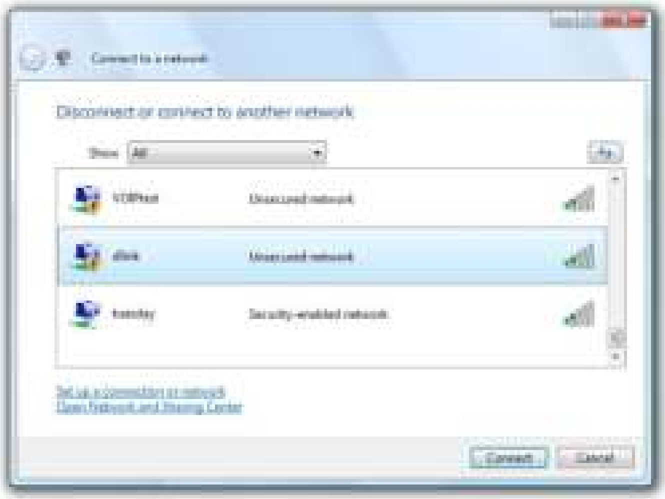


Not Connected

Wireless networks are available.

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



Connect to a network

Disconnect or connect to another network

Show: All

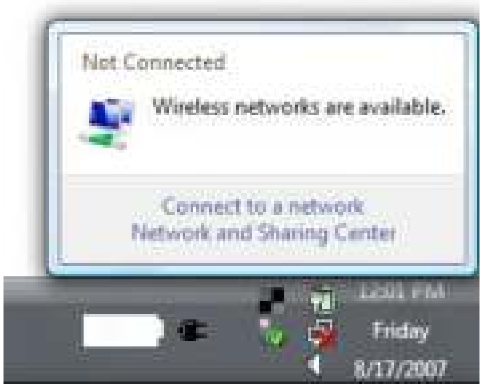
VOIPtest	Unsecured network
dlink	Unsecured network
[illegible]	Security-enabled network

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Wireless Security

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

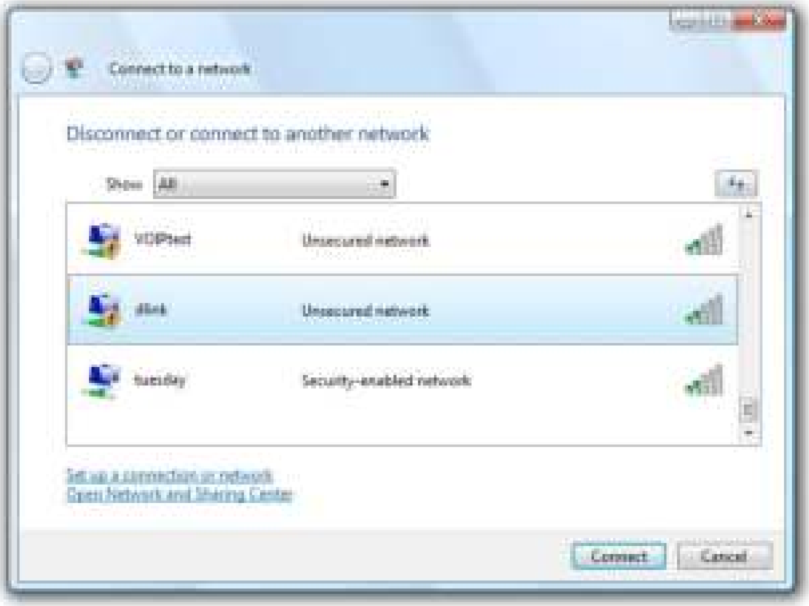
1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



Not Connected

Wireless networks are available.

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



Connect to a network

Disconnect or connect to another network

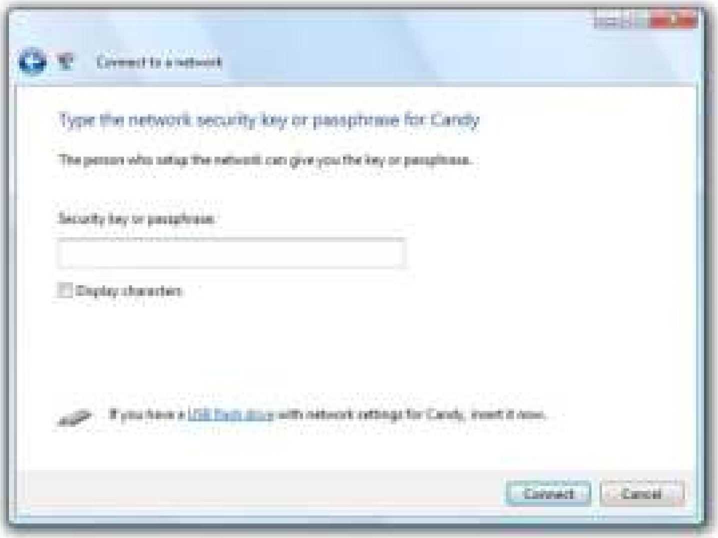
Show: All

VOIPtest	Unsecured network	
dlink	Unsecured network	
tuesday	Security-enabled network	

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

3. Enter the same security key or passphrase that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



Type the network security key or passphrase for Candy

The person who setup the network can give you the key or passphrase.

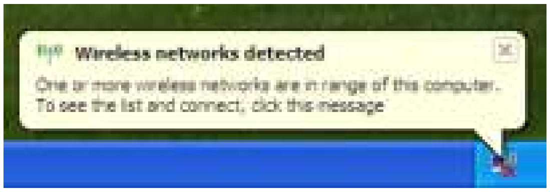
Security key or passphrase:

□ Display characters

If you have a USB flash drive with network settings for Candy, insert it now.

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

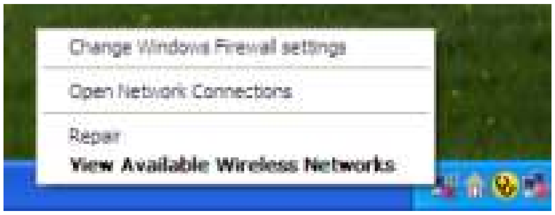
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.



One or more wireless networks are in range of this computer. To see the list and connect, click this message

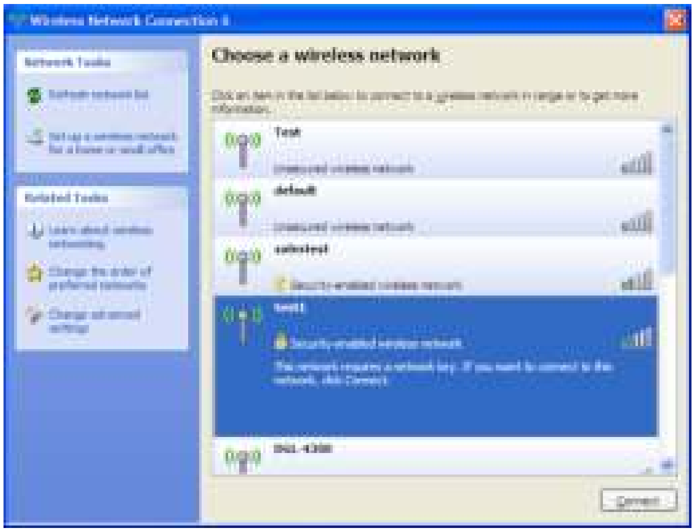
or

Right-click on the wireless computer icon in your system tray (lower right corner next to the time). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network
DSL-4300
Connect

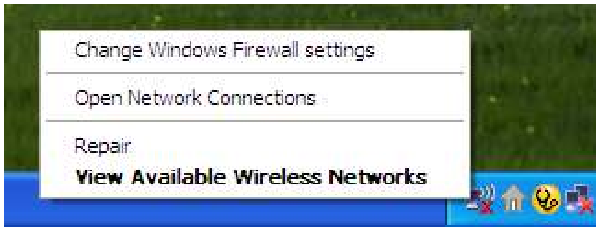
Click an item in the list below to connect to a wireless network in range or to get more information.

This network requires a network key. If you want to connect to this network, click Connect.

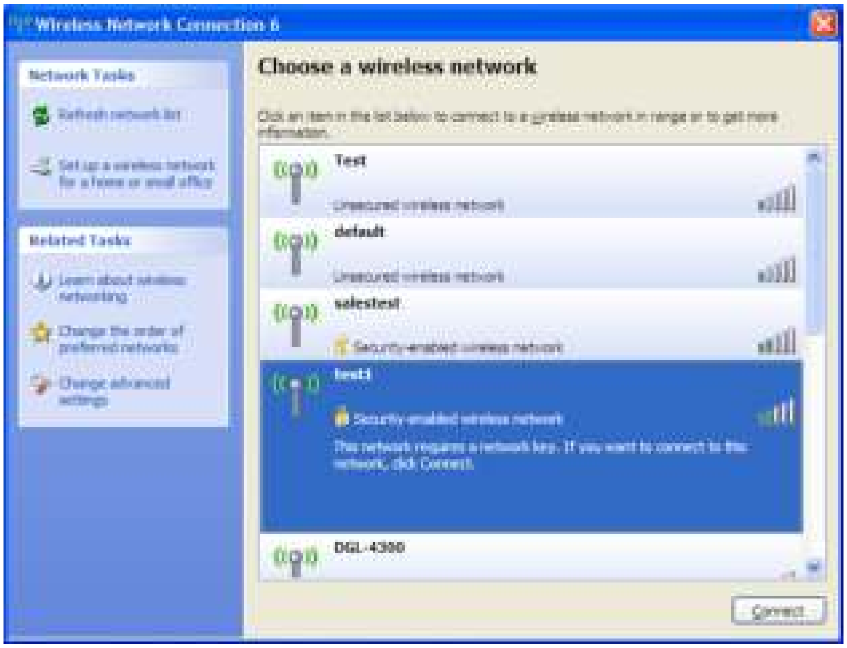
Wireless Security

It is recommended to enable encryption on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the passphrase being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network

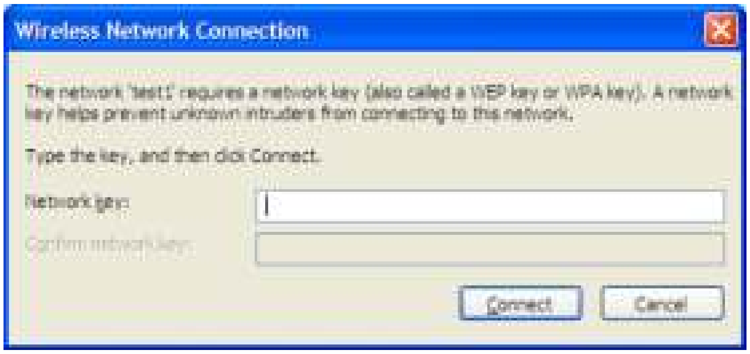
Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network
default
Unsecured wireless network
salestest
Security-enabled wireless network
test1
Security-enabled wireless network

This network requires a network key. If you want to connect to this network, click Connect.

3. The **Wireless Network Connection** box will appear. Enter the WPA/WPA2 passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA/WPA2 settings are correct. The WPA/WPA2 passphrase must be exactly the same as on the wireless router.



The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Networking Basics

Check your IP address

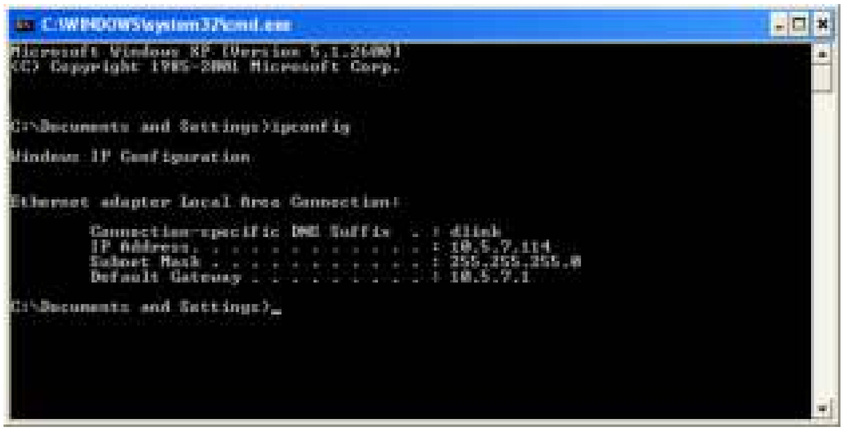
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from the DHCP server on your Gateway automatically. To verify your IP address, please follow the steps below.

Click on **Start** > **Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type **cmd** in the Start Search box.)

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dlink
        IP Address. . . . . . . . . . . . : 10.5.7.114
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.5.7.1

C:\Documents and Settings>_
```

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

Statically Assign an IP address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows® 7 -	Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
Windows Vista® -	Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections**.
Windows® XP -	Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 -	From the desktop, right-click **My Network Places** > **Properties**.

Step 2

Right-click on the Local Area Connection which represents your network adapter and select **Properties**.

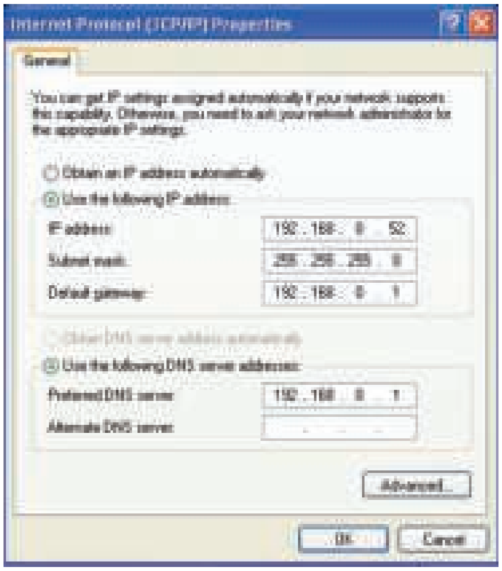
Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

Click Use the following IP address and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 0 . 52
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 0 . 1
Alternate DNS server:	. . .

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.