14.2.3.3 Editing the VC Protocol Settings for WAN Uplink Port

NOTE: The instructions in this section refer to the Router configured for **Ethernet WAN Uplink port** mode. Be sure that you have selected **WAN Uplink port** in the **VersaPort** screen.

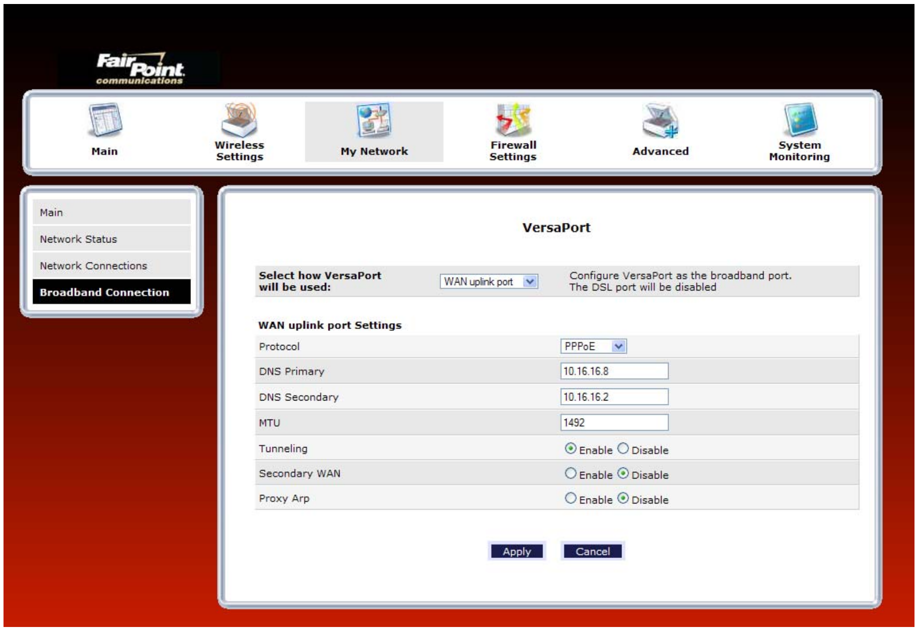
14.2.3.3.1 Configuring the WAN Uplink Protocol Settings for PPPoE

After you have selected **WAN Uplink port**, in the preceding steps, select the desired protocol from the **Protocol** drop-down menu. If you select PPPoE, the following screen will appear. Select the desired options, and then click **Apply** to save the settings.

NOTE:

1. If you experience any problems, reset the Router by pressing the reset button on the rear of the Router. Or follow the instructions in section 16.2, "Restore Defaults," to restore the Router to factory default settings. The actual information displayed in this screen may vary, depending on network connection established.

2. PPPoE is the factory default setting for WAN Uplink port.



VersaPort

Select how VersaPort will be used: WAN uplink port — Configure VersaPort as the broadband port. The DSL port will be disabled

WAN uplink port Settings

Protocol	PPPoE
DNS Primary	10.16.16.8
DNS Secondary	10.16.16.2
MTU	1492
Tunneling	● Enable ○ Disable
Secondary WAN	○ Enable ● Disable
Proxy Arp	○ Enable ● Disable

Uplink Settings for WAN Uplink Port (PPPoE protocol)	
Tunneling	Factory Default = Enable If Enabled, this option allows PPP traffic to be bridged to the WAN. This feature allows you to use a PPPoE shim on the host computer to connect to the Internet Service Provider, by bypassing the Router's capability to do this. Factory default is "Enable."
Secondary WAN	Factory Default = Disable The secondary WAN interface is used for multicast traffic. This feature applies only when you are using PPPoE as the Primary WAN protocol.
Proxy ARP	Factory Default = Disable When this feature is activated, the VersaLink will respond to ARP requests. To activate this feature, click Enable.

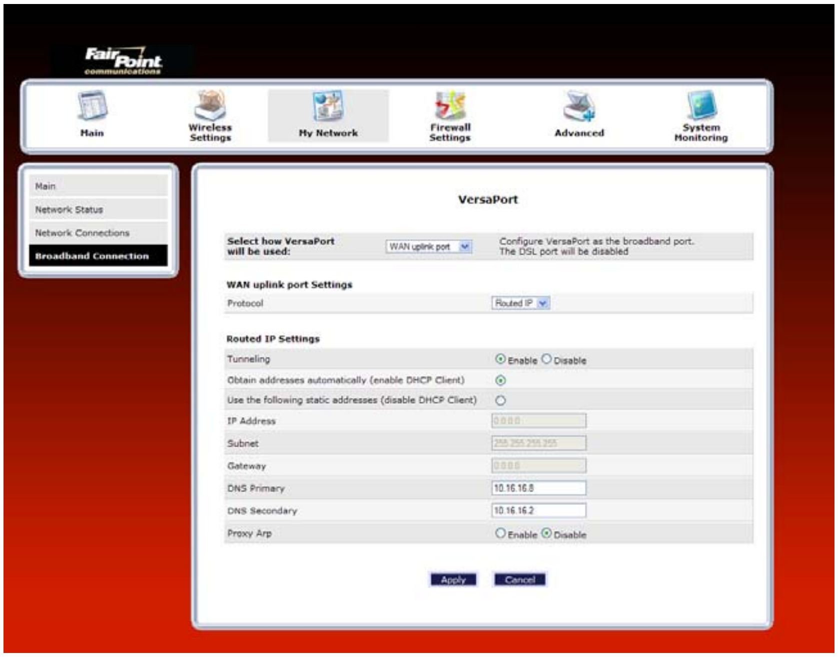
14.2.3.3.2 Configuring the WAN Uplink Protocol Settings for Routed IP

If you select **Routed IP** from the **Protocol** drop-down menu, the following screen will appear. Enter the desired options, and then click **Apply** to save the settings.

NOTE:

1. If you experience any problems, reset the Router by pressing the reset button on the rear of the Router. Or follow the instructions in section 16.2, “Restore Defaults,” to restore the Router to factory default settings. The actual information displayed in this screen may vary, depending on the network connection established.

2. PPPoE is the factory default setting for Ethernet WAN Uplink.



VersaPort

Select how VersaPort will be used: WAN uplink port — Configure VersaPort as the broadband port. The DSL port will be disabled

WAN uplink port Settings

Protocol: Routed IP

Routed IP Settings

Tunneling	● Enable ○ Disable
Obtain addresses automatically (enable DHCP Client)	●
Use the following static addresses (disable DHCP Client)	○
IP Address	0.0.0.0
Subnet	255.255.255.255
Gateway	0.0.0.0
DNS Primary	10.16.16.8
DNS Secondary	10.16.16.2
Proxy Arp	○ Enable ● Disable

Uplink Settings for WAN Uplink Port (Routed IP protocol)	
Tunneling	Factory Default = Enable If Enabled, this option allows PPP traffic to be bridged to the WAN. This feature allows you to use a PPPoE shim on the host computer to connect to the Internet Service Provider, by bypassing the Router’s capability to do this.
DHCP Client	Selecting a option allows you to either Enable or Disable the DHCP Client. Click the top option labeled (enable DHCP Client) to allow the Router to obtain an IP address automatically from your service provider. Click the bottom option labeled (disable DHCP Client) to allow the Router to accept static IP address information. Then, manually enter the IP values into the fields. Obtain these values from your ISP.
IP Address	The IP network address that your Router is on.
Subnet	The IP subnet address that your Router is on.
Gateway	The Router’s IP gateway address.
DNS Primary	Provided by your Internet service provider.
DNS Secondary	Provided by your Internet service provider.
Note: The values for the IP Address, Gateway, DNS Primary, and DNS Secondary are all “Override of the value obtained from the PPP connection,” They default to “0.0.0.0,” in which case the override is ignored. It is recommended that you do not change the values unless your Internet service provider instructs you to do so.	

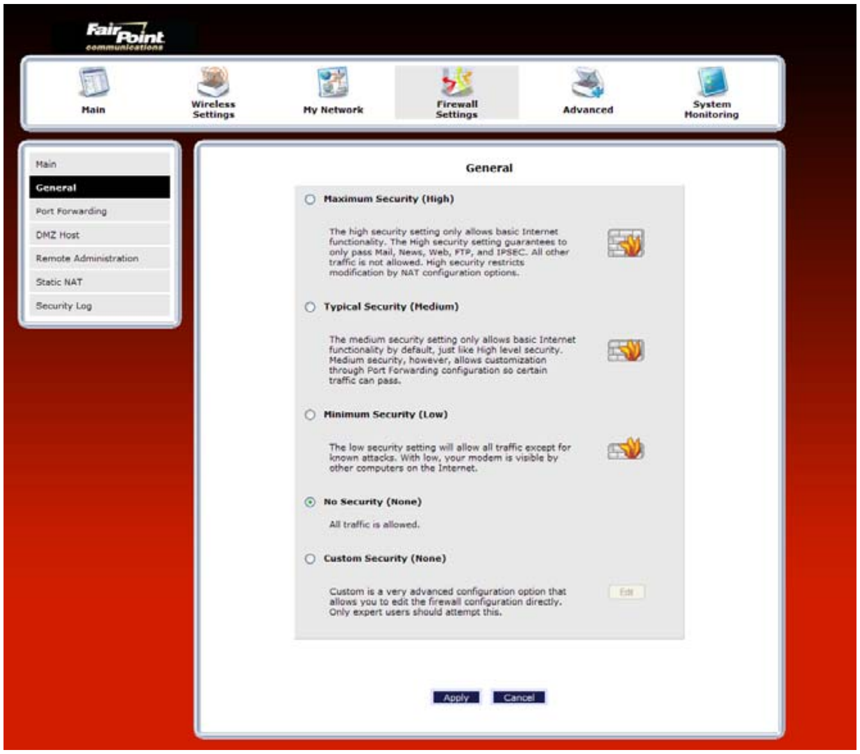
15. FIREWALL SETTINGS

15.1 General Firewall Security Settings

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.

IMPORTANT: It is recommended that you do not change the settings in this **User Defined Firewall Rules** screen. If you need to reset your Router to factory default settings, push the reset button on the rear of the Router. Or follow the instructions in section 16.2, "Restore Defaults," to restore the Router to factory default settings.
The factory default security level for your Router is **No Security (None).**



General

○ **Maximum Security (High)**

The high security setting only allows basic Internet functionality. The High security setting guarantees to only pass Mail, News, Web, FTP, and IPSEC. All other traffic is not allowed. High security restricts modification by NAT configuration options.

○ **Typical Security (Medium)**

The medium security setting only allows basic Internet functionality by default, just like High level security. Medium security, however, allows customization through Port Forwarding configuration so certain traffic can pass.

○ **Minimum Security (Low)**

The low security setting will allow all traffic except for known attacks. With low, your modem is visible by other computers on the Internet.

● **No Security (None)**

All traffic is allowed.

○ **Custom Security (None)**

Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this.

General Firewall Settings	
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 Router is visible to other computers on the Internet.
No Security (None)	Factory Default = No Security (None) The Firewall is disabled. (All traffic is passed)
Custom Security (Custom)	Custom is a security option that allows you to edit the firewall configuration directly. Note: Only the most advanced users should try this.

15.2 Editing Firewall Security Rules

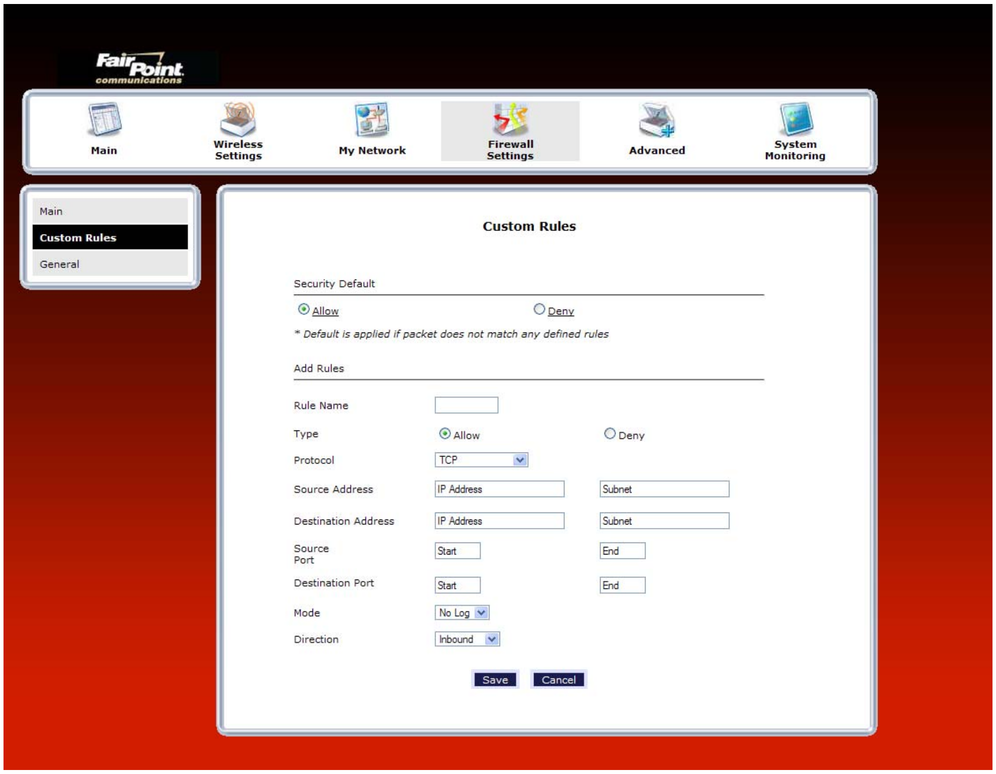
To edit the firewall security rules and customize them to your preference, at the **General** screen, select the security option that want to edit, and then click **Apply**.

To set up custom security rules, select the **Custom Security (None)** option, and then click **Apply.** Next, click the **Edit** button to go to the **Custom Rules** screen.

IMPORTANT: Custom Security is a very advanced configuration option that allows you to edit the firewall configuration directly. Only expert users should attempt this. It is recommended that you do not change the settings in this screen. If you need to reset your Router to factory default settings, push the reset button on the rear of the Router. Or follow the instructions in section 16.2, “Restore Defaults,” to restore the Router to default settings.

The **Custom Rules** screen allows you to configure the security parameters on your Inbound and Outbound traffic. Inbound rules will restrict inbound traffic from the WAN to the LAN. Outbound rules will restrict outbound traffic from the LAN to WAN. Enter the desired parameters in the Custom Rules screen, and then click **Save** to allow the settings to take effect in your Router.

NOTE: The default security setting is applied if a packet does not match any defines rules. Clicking **Save** allows the firewall rules to be saved to flash (a temporary storage area in your Router).



Custom Rules

Security Default

● Allow ○ Deny

** Default is applied if packet does not match any defined rules*

Add Rules

Rule Name

Type ● Allow ○ Deny

Protocol TCP

Source Address IP Address Subnet

Destination Address IP Address Subnet

Source Port Start End

Destination Port Start End

Mode No Log

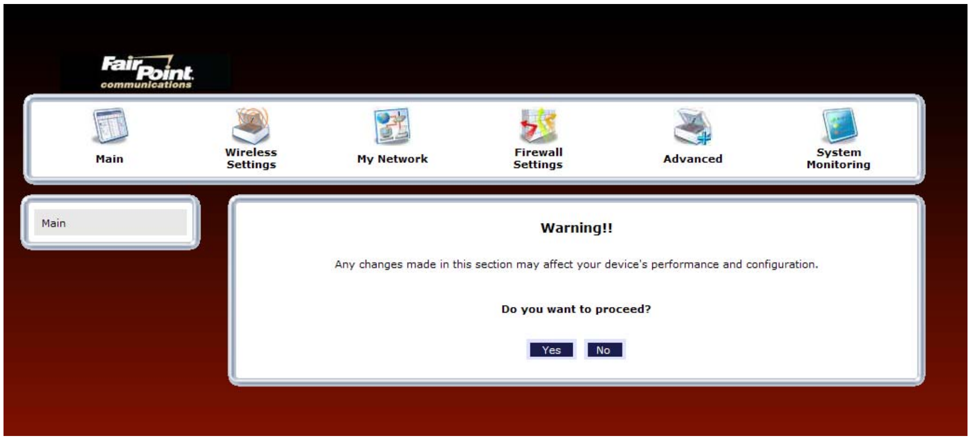
Direction Inbound

15.3 Port Forwarding

To access the Port Forwarding screen, from the top navigational menu, select **Firewall Settings.** Then select **Port Forwarding** from the menu options at the left of the screen. A warning screen will display the following message:

> **Any changes made in this section may affect your device's performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.



Warning!!

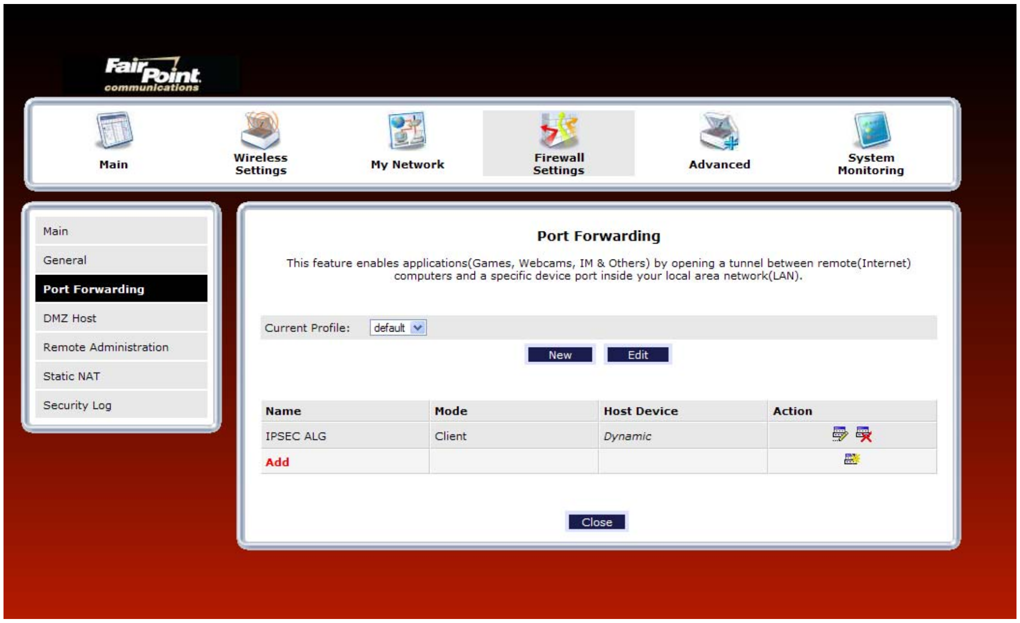
Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

If you clicked **Yes**, in the preceding warning screen, the following **Port Forwarding** screen will be displayed. This feature enables applications (Games, Webcams, IM & Others) by opening a tunnel between remote (Internet) computers and a specific device port inside your local area network (LAN).

The **Port Forwarding** screen allows you to do the following:

- Edit connection profiles, create new connection profiles
- Configure port forwarding services: predefined, customized, and port forwarding/port triggering services



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: default

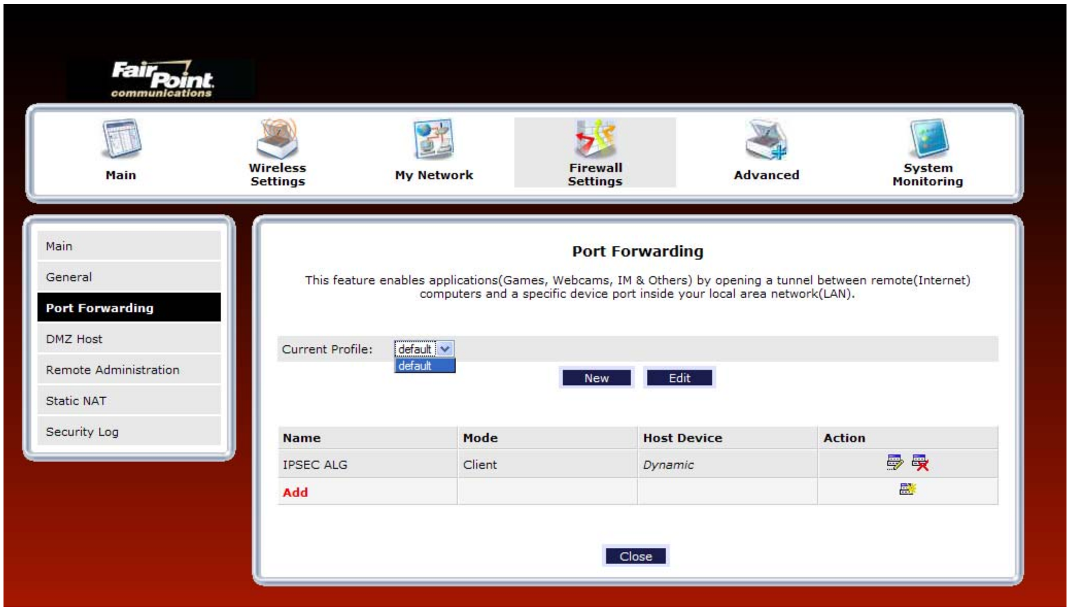
Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

15.3.1 Editing a Profile Name

Port Forwarding services can be added to connection profiles. To edit an existing profile name, and then later add port forwarding services to the profile, follow the instructions in this section.

To edit a connection profile name, in the **Port Forwarding** screen, click the **Current Profile** drop-down menu, and then select the name of the profile that you want to edit. Next, click **Edit** 📝.

NOTE: If you have not previously configured a profile, the "Default" profile will be displayed.



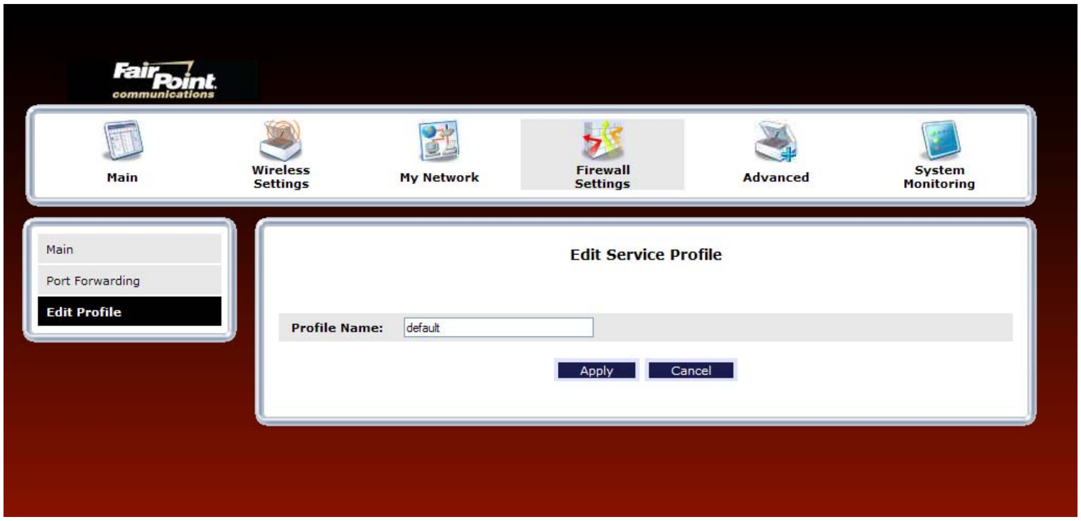
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: default

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

If you have selected a profile and clicked **Edit**, the following screen will appear. In the following example, "Default" has been selected from the **Current Profile** drop-down menu displayed in the preceding screen. This is the profile name that will be edited.

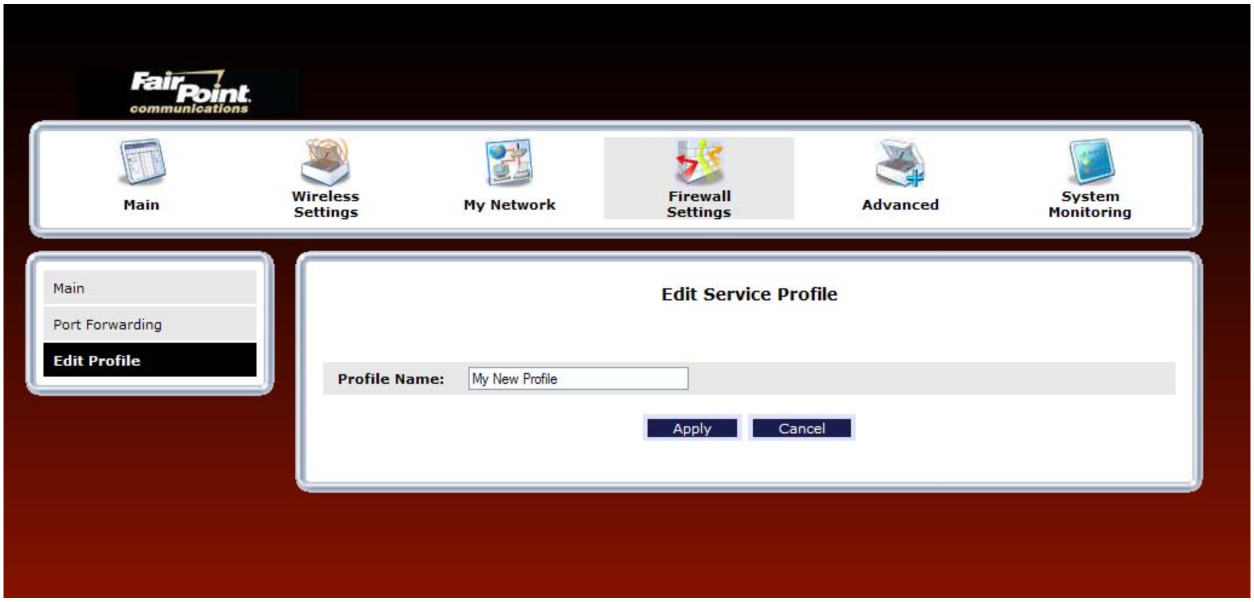


Edit Service Profile

Profile Name: default

Type the name of your choice in the field provided. Then, click **Apply** to allow the change to take effect.

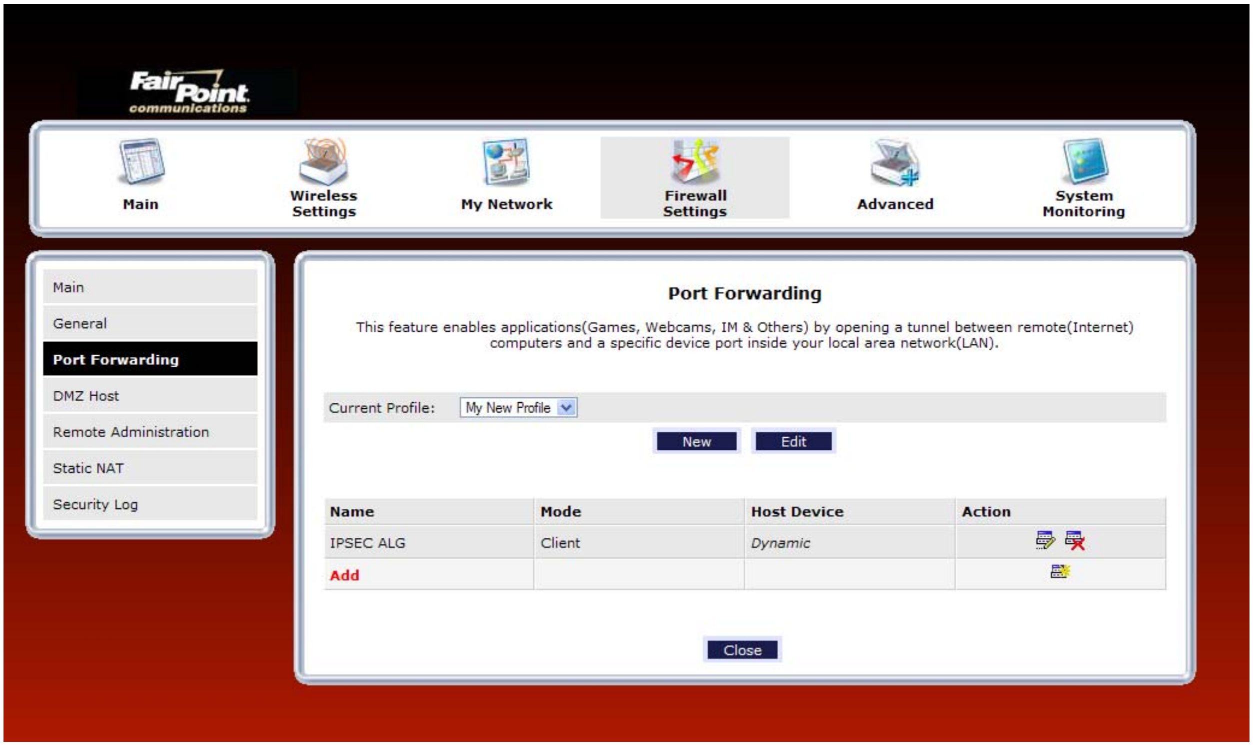
NOTE: If you reset your Router to factory default settings, the default profile “Default” will be displayed, and any previously configured settings will be lost.



Edit Service Profile

Profile Name: My New Profile

The name you entered should now be displayed in the **Current Profile** drop-down menu.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

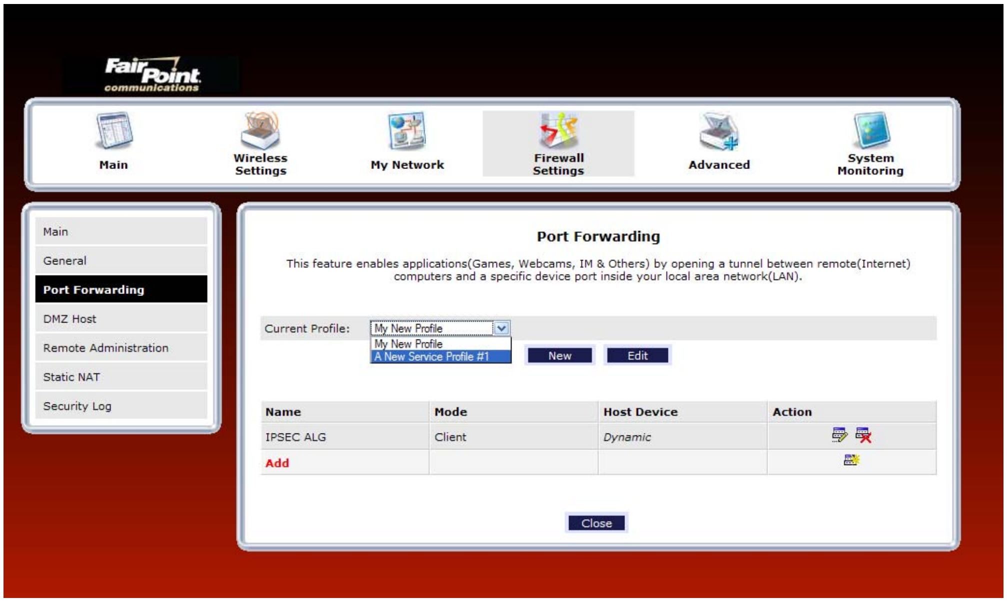
Current Profile: My New Profile

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	✎ ✗
Add			✎

15.3.2 Creating a New Connection Profile

If you want to create a new profile, and then later add port forwarding services to the new profile, follow the instructions in this section.

To create a new connection profile, in the **Port Forwarding** screen, click **New**. Then, from the **Current Profile** drop-down menu, select **A New Service Profile #1.**



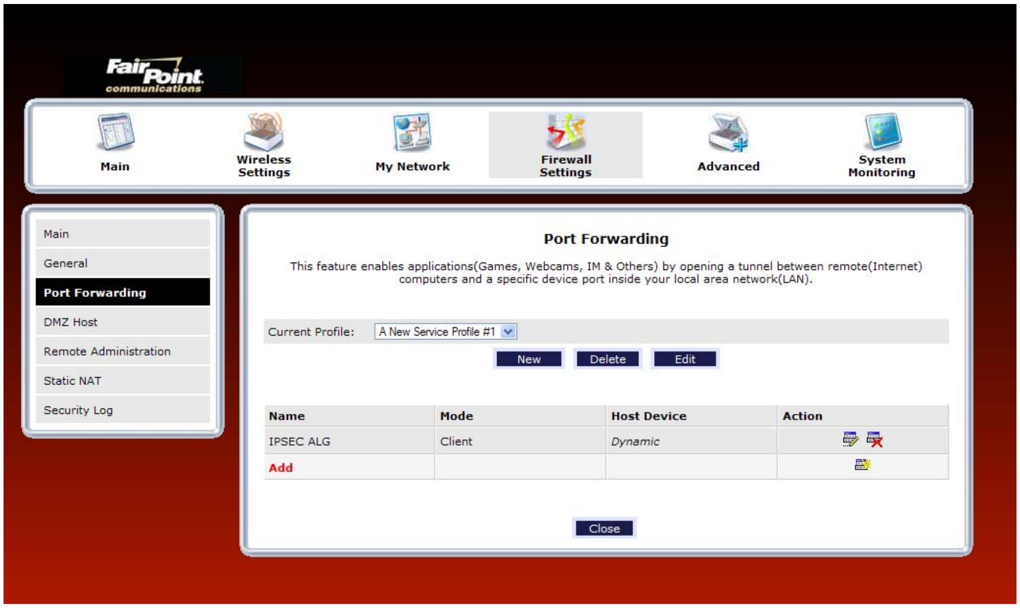
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: My New Profile

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

Next, click the **Edit** button to edit the profile.



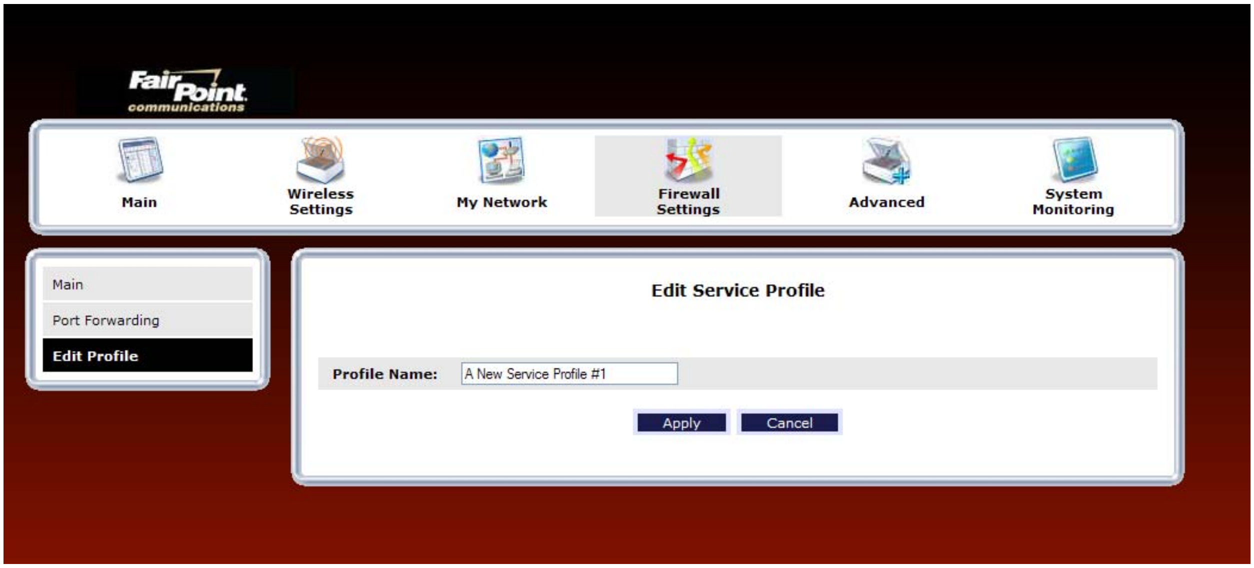
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: A New Service Profile #1

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

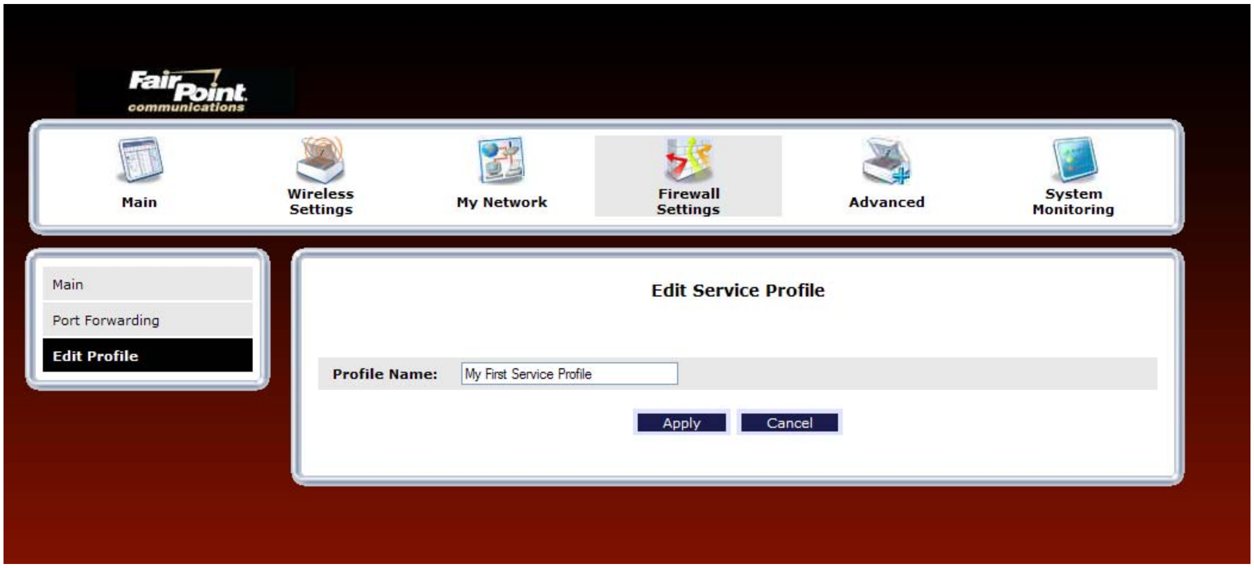
If you clicked the **Edit** button, the following screen will appear. Type the profile name of your choice in the field, and then click **Apply** to allow the change to take effect.



Edit Service Profile

Profile Name: A New Service Profile #1

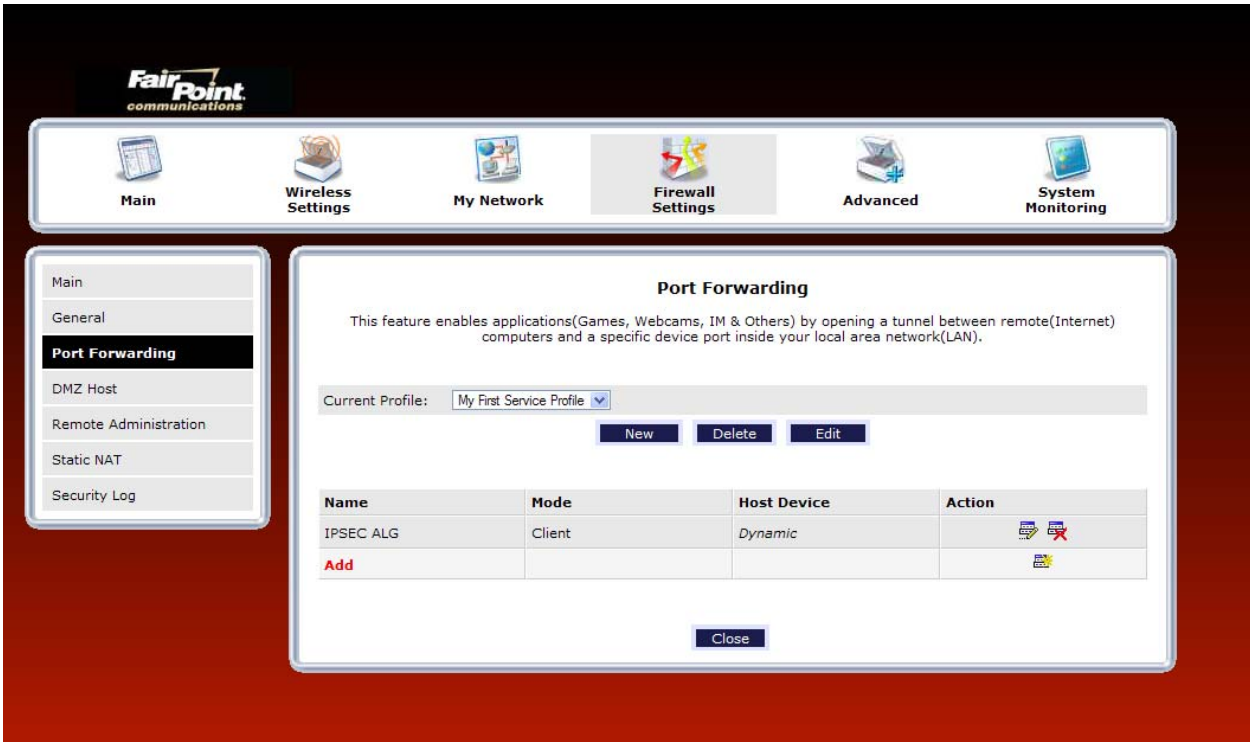
For example, **"My First Service Profile"** is the name that has been entered in the **Profile Name** field. Click **Apply**.



Edit Service Profile

Profile Name: My First Service Profile

If you clicked **Apply**, the following screen will be displayed. The **Current Profile** field now displays the profile name that you entered.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: My First Service Profile

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

15.3.3 Configuring Port Forwarding Services

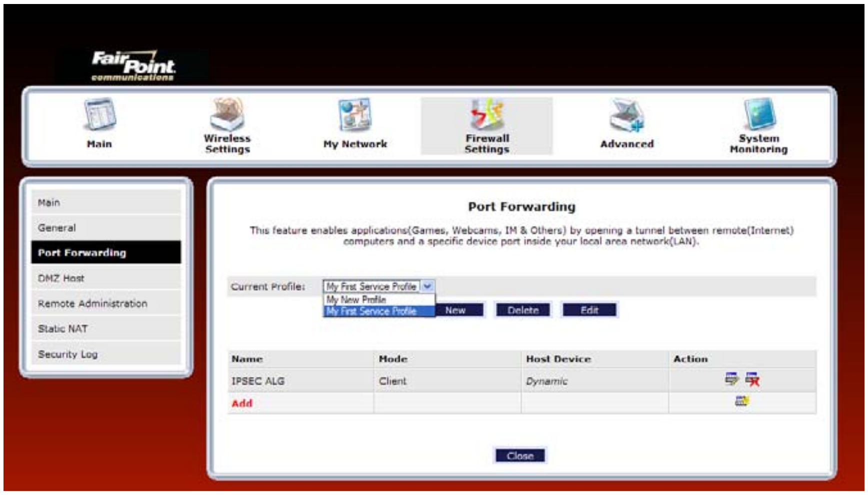
Port Forwarding Services contain specific service settings. The service can then be associated with connection profiles, allowing you to customize profiles for specific users. For example, if you want to attach specific services to a profile or if you want to set up a different connection setting for a profile. You can create new service profiles and customize them to your preference.

Your Router contains a list of predefined Port Forwarding services, and you can select any service from this list. By selecting your specific service and setting up a profile, you will ensure that the appropriate ports on your Router are open and that the required application traffic can pass through your local area network (LAN). For a list of supported services, go to section 18, “Port Forwarding Services.”

NOTE: You can create up to four service profiles and attach an unlimited number of services to each profile. The current profile labeled “Default” is the factory default profile.

15.3.3.1 Adding Port Forwarding Services to a Profile

To add a predefined service to a profile, in the **Port Forwarding** screen, click the **Current Profile** drop-down menu, and then select the name of the profile to which you want to add services. Next, click **Add.**



Port Forwarding

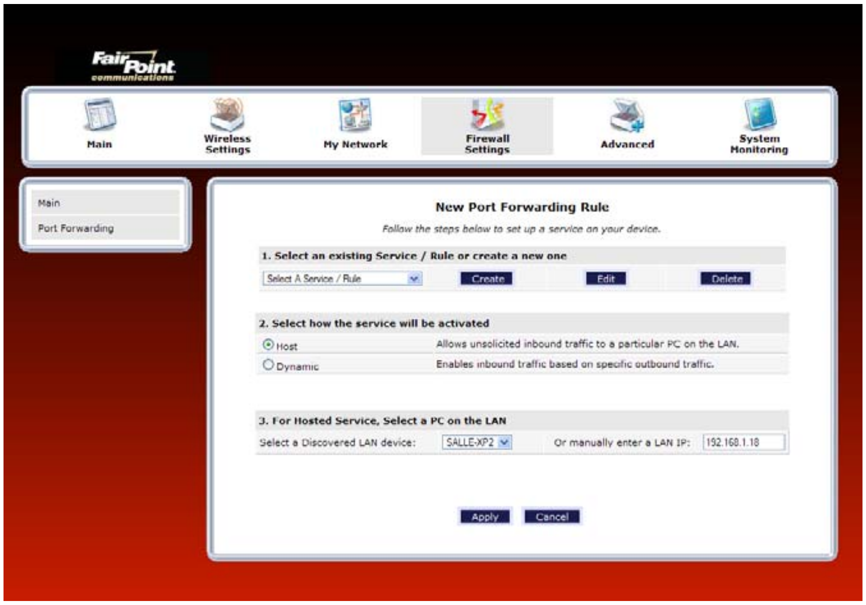
This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: My First Service Profile

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
Add			

If you clicked **Add**, the following **New Port Forwarding Rule** screen will appear. Using this screen, you can do any of the following:

- Add a predefined service to a profile
- Create a customized service
- Edit an existing service profile
- Delete an existing profile



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

2. Select how the service will be activated

● Host Allows unsolicited inbound traffic to a particular PC on the LAN.

○ Dynamic Enables inbound traffic based on specific outbound traffic.

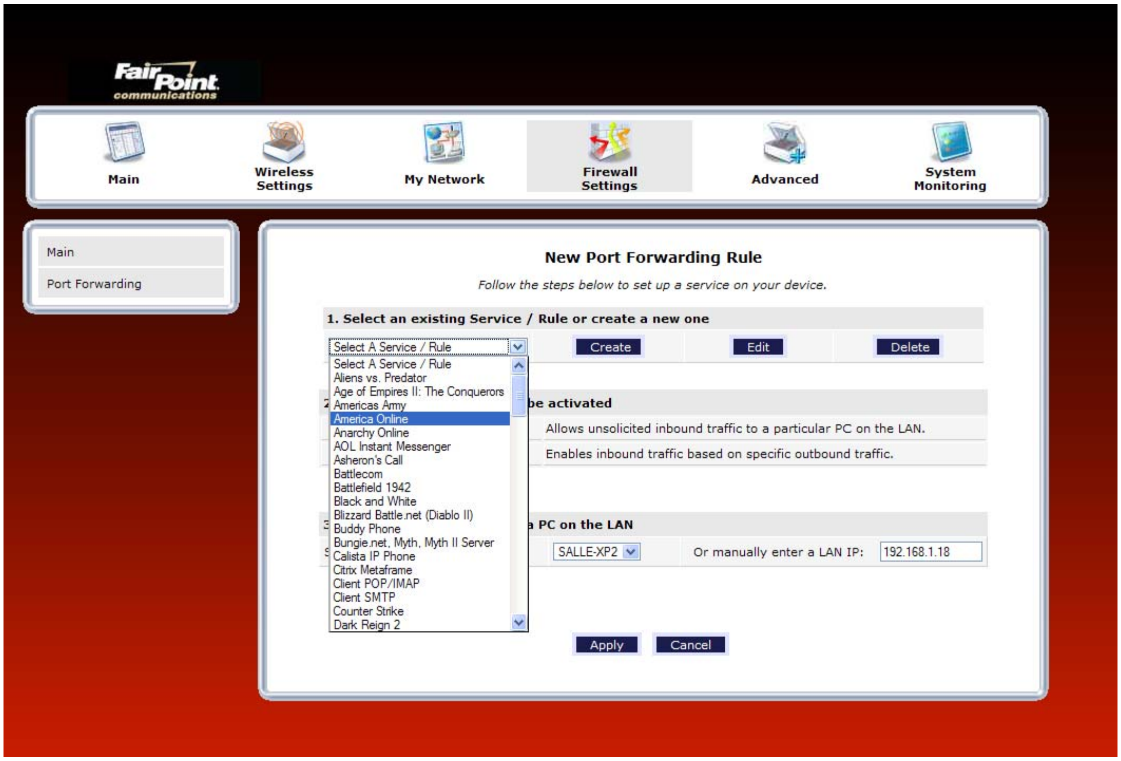
3. For Hosted Service, Select a PC on the LAN

Select a Discovered LAN device: SALLE-XP2 Or manually enter a LAN IP: 192.168.1.18

15.3.3.2 Adding a Predefined Port Forwarding Service to a Profile

To add a predefined port forwarding service to a profile, in the **New Port Forwarding Rule** screen, perform the following steps:

1. Select the desired service from the **Select a Service** drop-down menu. After you have selected a service, it will appear in the window.



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

be activated

Allows unsolicited inbound traffic to a particular PC on the LAN.

Enables inbound traffic based on specific outbound traffic.

a PC on the LAN

Or manually enter a LAN IP: 192.168.1.18

2. Select the option that describes how you want the service to be activated.

- **Host:** Allows the unsolicited inbound traffic to a particular PC on the LAN
- **Dynamic:** Enables inbound traffic based on specific outbound traffic

3. Select the desired IP address from the drop-down menu or manually enter the LAN IP address of the device that you want to host the service.

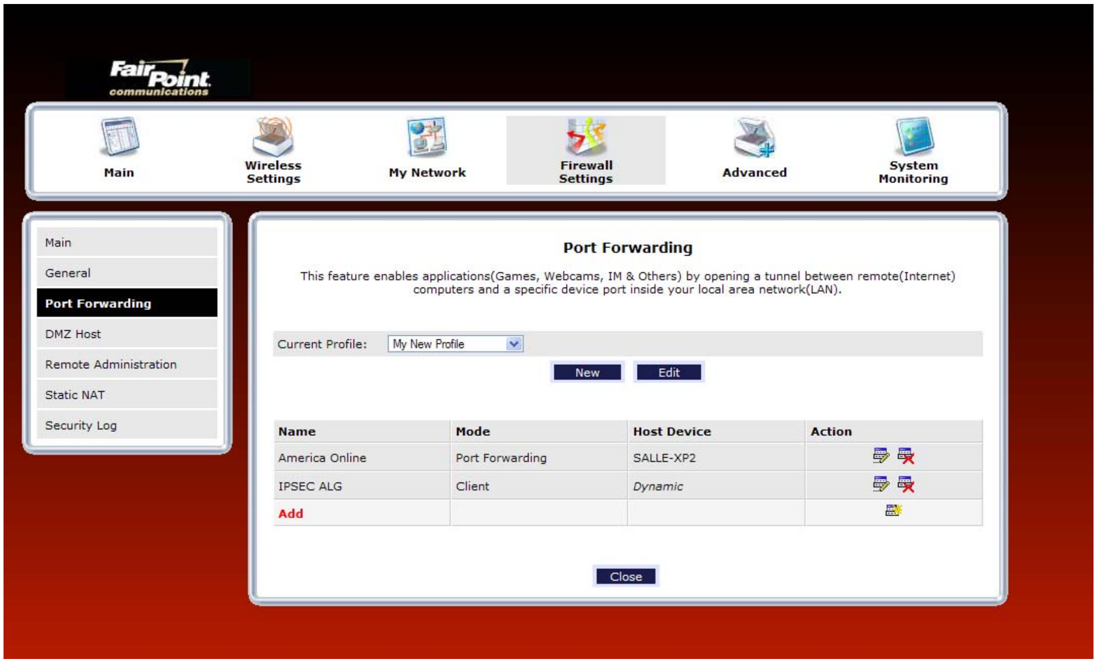
4. Click **Apply** to allow the settings to take effect.

NOTE: If you click **Cancel** in the **New Port Forwarding Rule** screen, the service you selected will be displayed; however, it will not be assigned to a device on the LAN. You must click **Apply** to allow the settings to take effect.

If you clicked **Apply**, the following screen will be displayed. In this example, the screen shows that service “America Online” has been added to the “Default” profile.

- To add additional predefined services, in the **Port Forwarding** screen, first select the desired profile from the **Current Profile** drop-down menu. Next, click **Add** and then repeat the preceding steps 1 through 4.
- To view the details of a service you have added, in the **Action** field click the details icon 📝.

- To delete a service from your list of active services, at the **Port Forwarding** screen, click the delete icon next to the service that you want to delete. Then click **OK** in the pop-up screen to confirm your decision. The service will be deleted from the Router's list of active services.



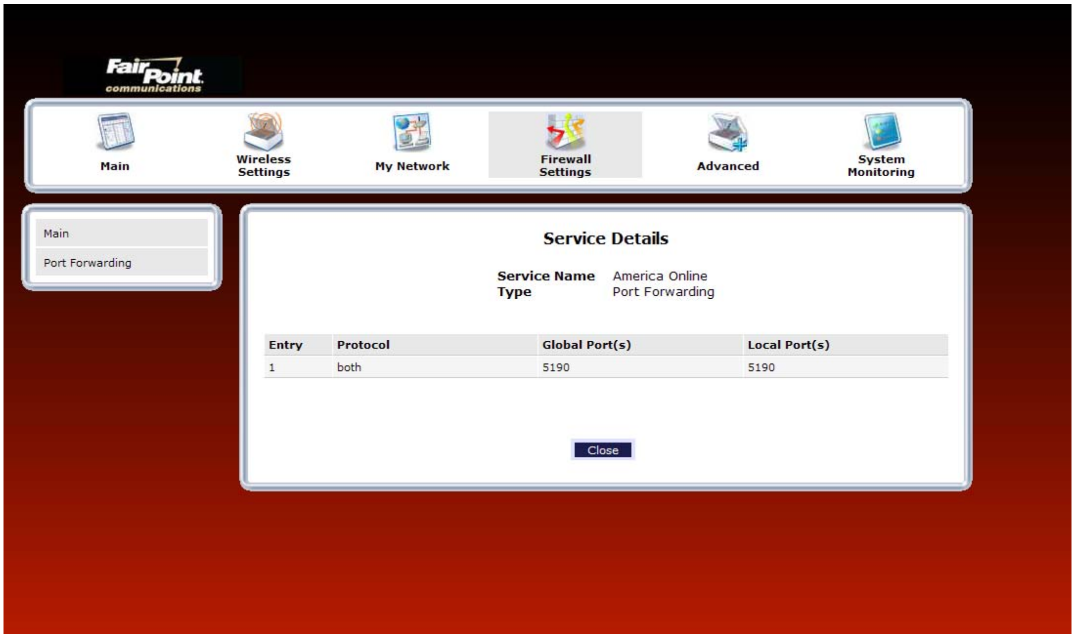
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: My New Profile

Name	Mode	Host Device	Action
America Online	Port Forwarding	SALLE-XP2	
IPSEC ALG	Client	*Dynamic*	
Add			

If you clicked the details icon in the preceding screen, the following screen will be displayed. Click **Cancel** when you are ready to return to the **Port Forwarding** screen.



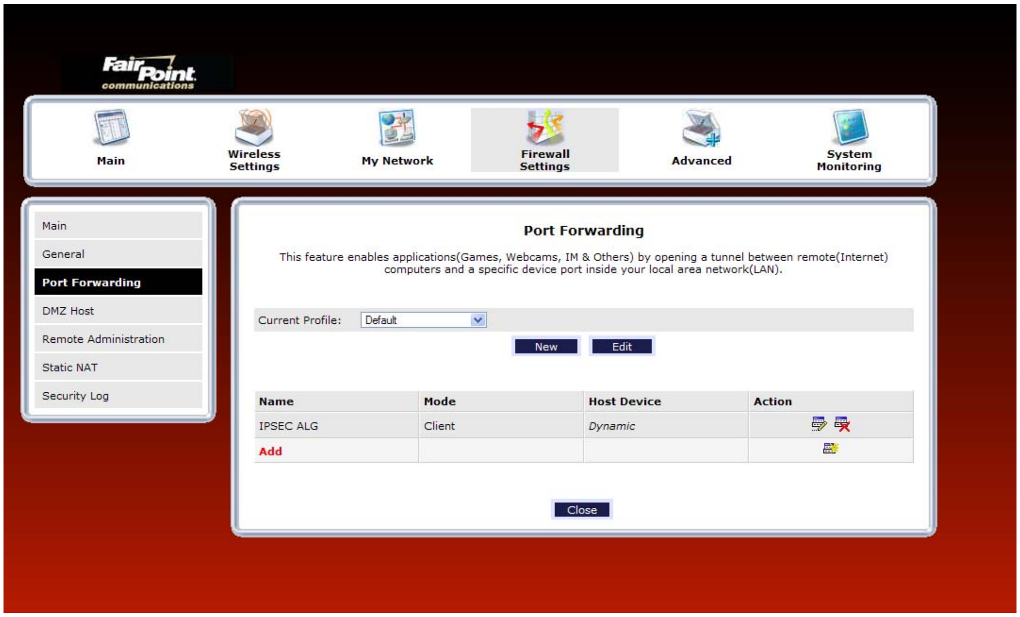
Service Details

Service Name America Online
Type Port Forwarding

Entry	Protocol	Global Port(s)	Local Port(s)
1	both	5190	5190

15.3.3.3 Creating a Customized Port Forwarding Service

To create a customized port forwarding service, click **Add** in the **Port Forwarding** screen.



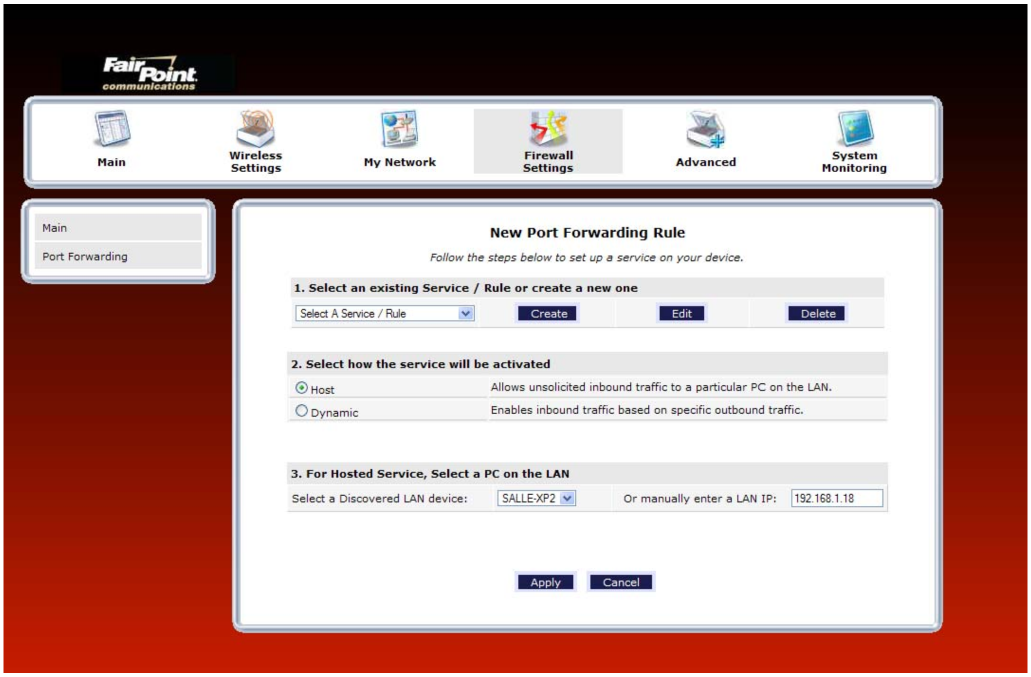
Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: Default

Name	Mode	Host Device	Action
IPSEC ALG	Client	Dynamic	
Add			

If you clicked **Add,** the following screen will be displayed. Click **Create.**



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

Select A Service / Rule

2. Select how the service will be activated

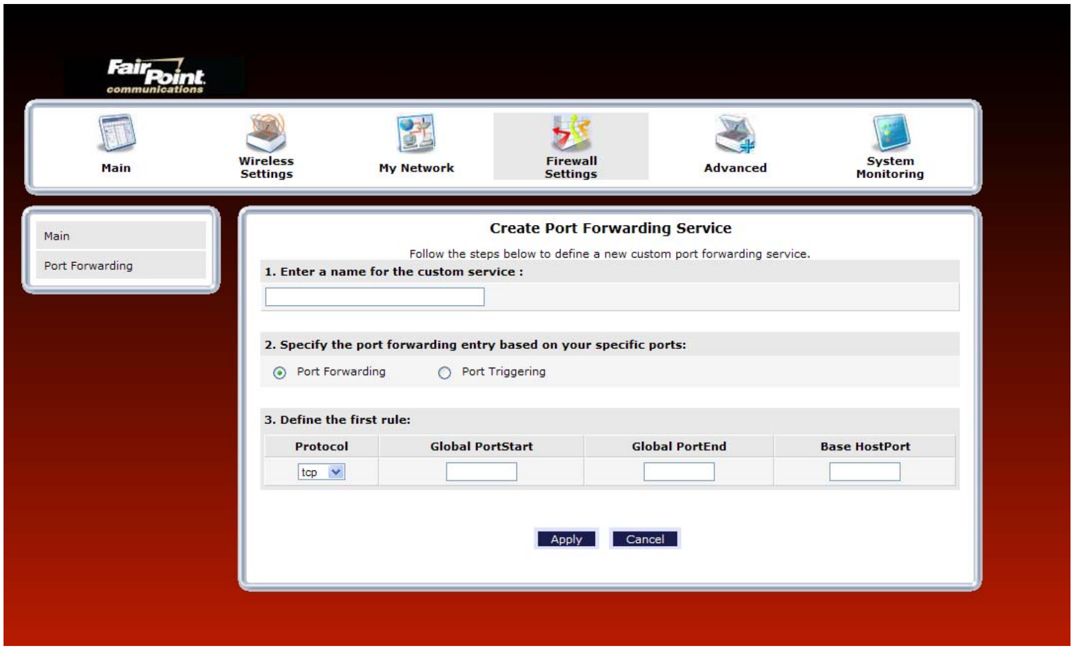
● Host	Allows unsolicited inbound traffic to a particular PC on the LAN.
○ Dynamic	Enables inbound traffic based on specific outbound traffic.

3. For Hosted Service, Select a PC on the LAN

Select a Discovered LAN device: SALLE-XP2 Or manually enter a LAN IP: 192.168.1.18

If you clicked **Create**, the following **Create Port Forwarding Service** screen will appear. Using this screen, you can create port forwarding and port triggering services for your Router. The following sections explain how to customize these services in your Router.

- **Port Forwarding Ranges of Ports**: This option allows you to forward a range of WAN ports to an IP address on the LAN.
- **Trigger Ports:** This option allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic.



Create Port Forwarding Service

Follow the steps below to define a new custom port forwarding service.

1. Enter a name for the custom service :

2. Specify the port forwarding entry based on your specific ports:

● Port Forwarding ○ Port Triggering

3. Define the first rule:

Protocol	Global PortStart	Global PortEnd	Base HostPort
tcp			

15.3.3.3.1 Creating a Service Based on Specific Port Forwarding Ports

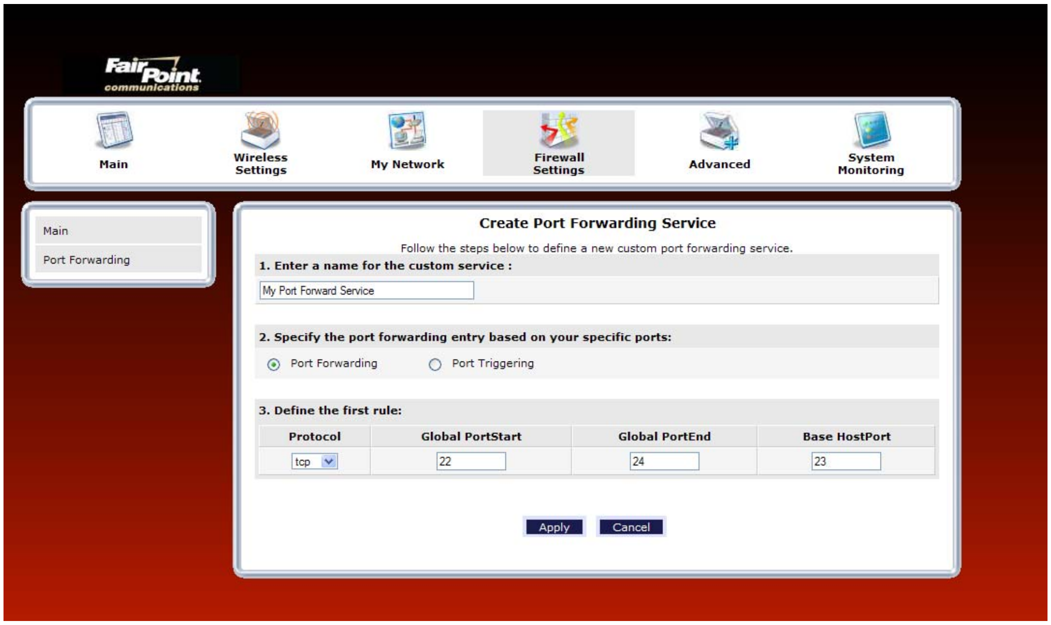
The Port Forwarding feature allows you to forward a range of WAN ports to an IP address on the LAN. You can set up a port forwarding entry based on your specific ports.

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.

To create a port forwarding service based on specific port forwarding ports, at the **Create Port Forwarding Service** screen, do the following:

1. Type the name of the custom service that you are creating in the field provided. This will be the name of the port forwarding service for which you are configuring specific Port Forwarding rules.
2. Click the **Port Forwarding** option.
3. Select the desired protocol from the **Protoco**l drop-down menu.
4. Enter the desired Global Port Start, Global Port End, and Base Host Port values in the fields provided, as shown in the example below.
5. Click **Apply** to allow the changes to take effect.

NOTE: If you clicked **Cancel** in the **Create Port Forwarding Service** screen, the service you created will be displayed; however, it will not be activated in your Router. You must click **Apply** to allow the settings to take effect.



Create Port Forwarding Service

Follow the steps below to define a new custom port forwarding service.

1. Enter a name for the custom service : My Port Forward Service

2. Specify the port forwarding entry based on your specific ports:

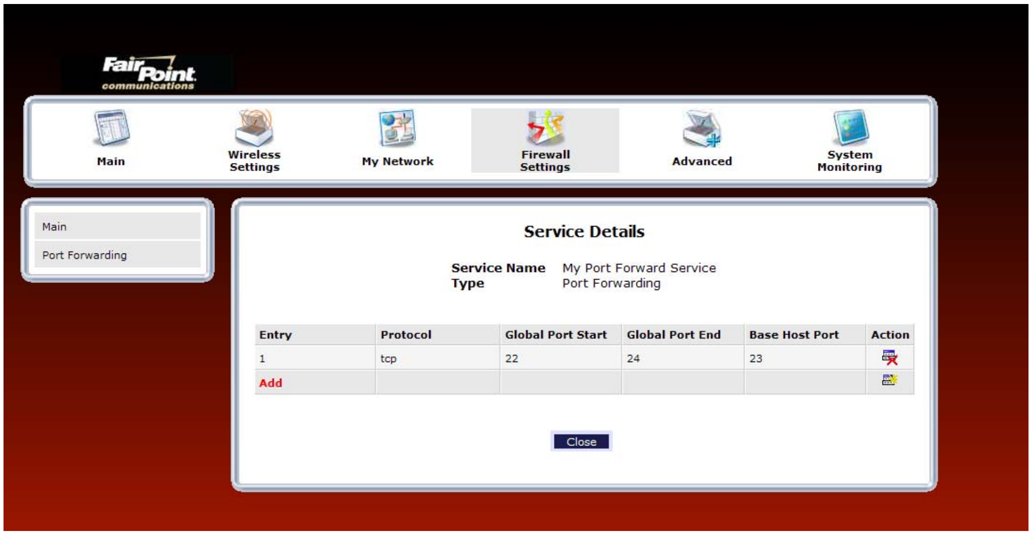
● Port Forwarding ○ Port Triggering

3. Define the first rule:

Protocol	Global PortStart	Global PortEnd	Base HostPort
tcp	22	24	23

Port Forwarding Service	
Protocol	TCP – Transmission Control Protocol UDP – User Datagram Protocol
Global Port Start	The WAN-side TCP/UDP start port.
Global Port End	The WAN-side TCP/UDP end port.
Base Host Port	The port on the WAN that will host the port forwarding service selected. Base Host Port is the first port that will be used for a specific service when configured for a range of ports.
Direction/ Port Directon	The port direction for the port forwarding rule.

If you clicked **Apply,** the following **Service Details** screen will be displayed. Click **Done**.

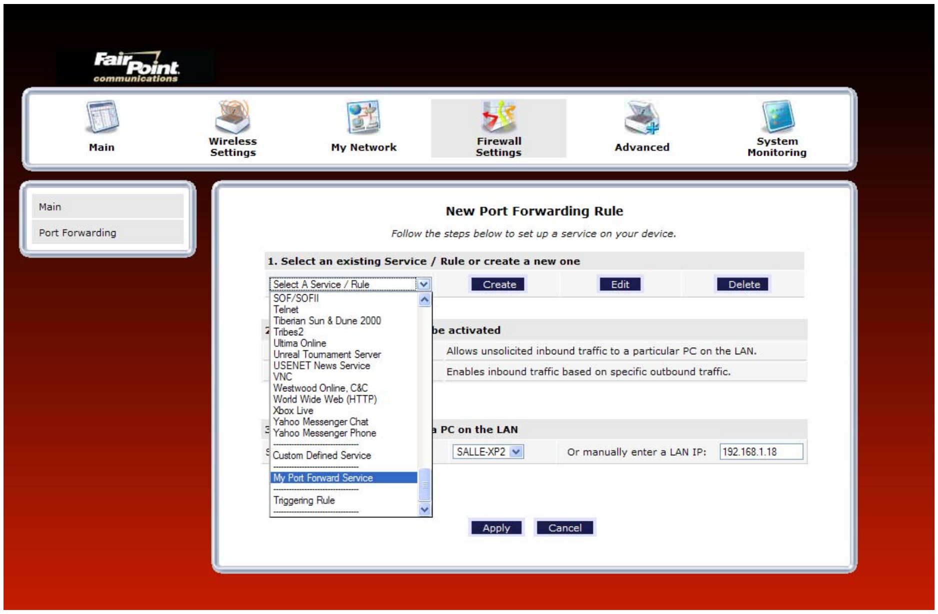


Service Details

Service Name My Port Forward Service
Type Port Forwarding

Entry	Protocol	Global Port Start	Global Port End	Base Host Port	Action
1	tcp	22	24	23	
Add					

6. Return to the **New Port Forwarding Rule** screen and, from the drop-down menu, select the name of the custom service that you created (the name should appear at the bottom of the list under **Custom Defined Service**).



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

be activated

Allows unsolicited inbound traffic to a particular PC on the LAN.

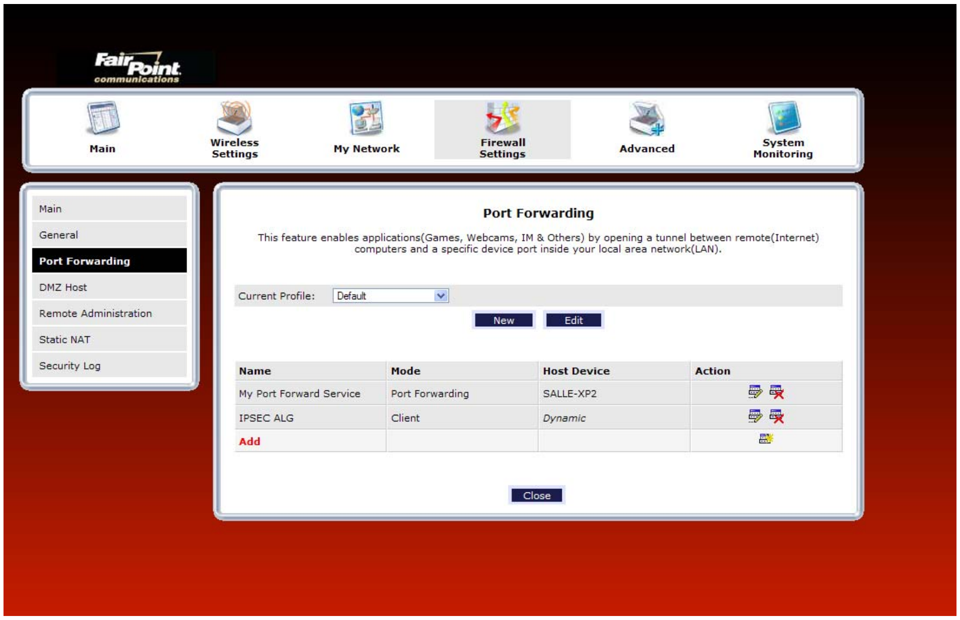
Enables inbound traffic based on specific outbound traffic.

a PC on the LAN

SALLE-XP2 Or manually enter a LAN IP: 192.168.1.18

7. Select how the service will be activated.
   - Host allows unsolicited inbound traffic to a particular PC on the LAN.
   - Dynamic enables inbound traffic based on specific outbound traffic.
8. Select the IP address of the device that will host the service (select a device from the **Select a Discovered LAN device** drop-down menu or type an IP address in the field provided).
9. Click **Apply** to allow the service to be added to the Router's list of active services.

If you clicked **Apply**, the following screen will appear. The Port Forwarding service has been added to the list of active services. To add additional port forwarding services to your Router, repeat steps 1 through 9.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: Default

Name	Mode	Host Device	Action
My Port Forward Service	Port Forwarding	SALLE-XP2	
IPSEC ALG	Client	*Dynamic*	
Add			

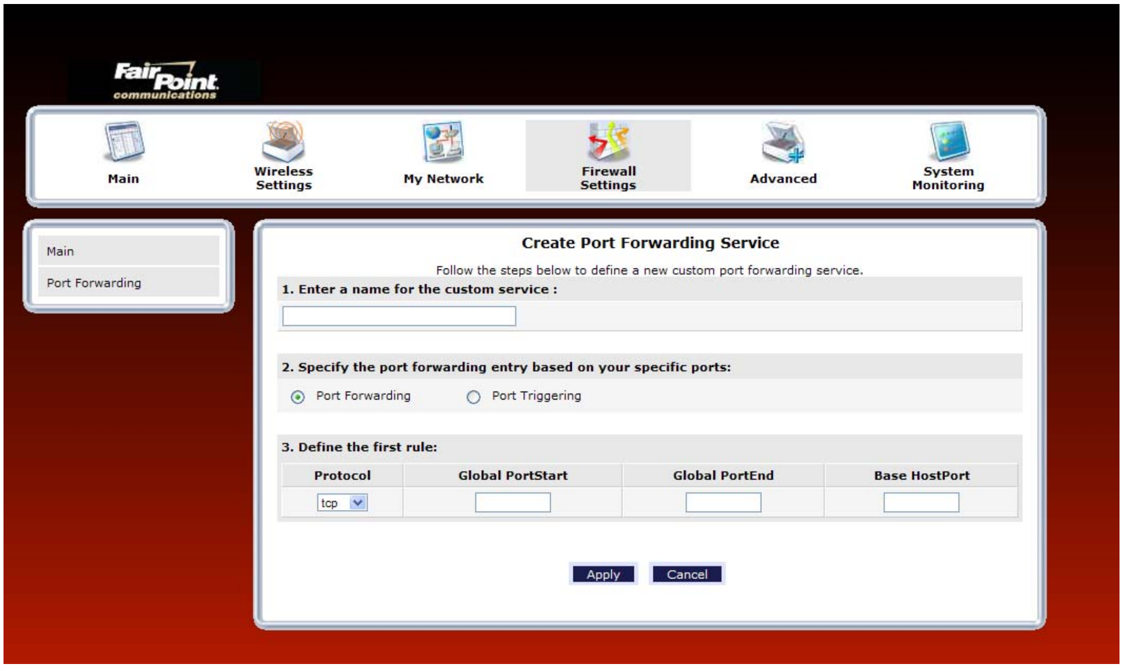
15.3.3.3.2 Creating a Service Based on Specific Port Triggering Ports

The Trigger Ports feature allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic. 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.

To create a port forwarding service based on specific port triggering ports, at the **Create Port Forwarding Service** screen, do the following:

1. Click the **Port Triggering** option. (By factory default, the **Port Forwarding** option will be selected.)



Create Port Forwarding Service

Follow the steps below to define a new custom port forwarding service.

1. Enter a name for the custom service :

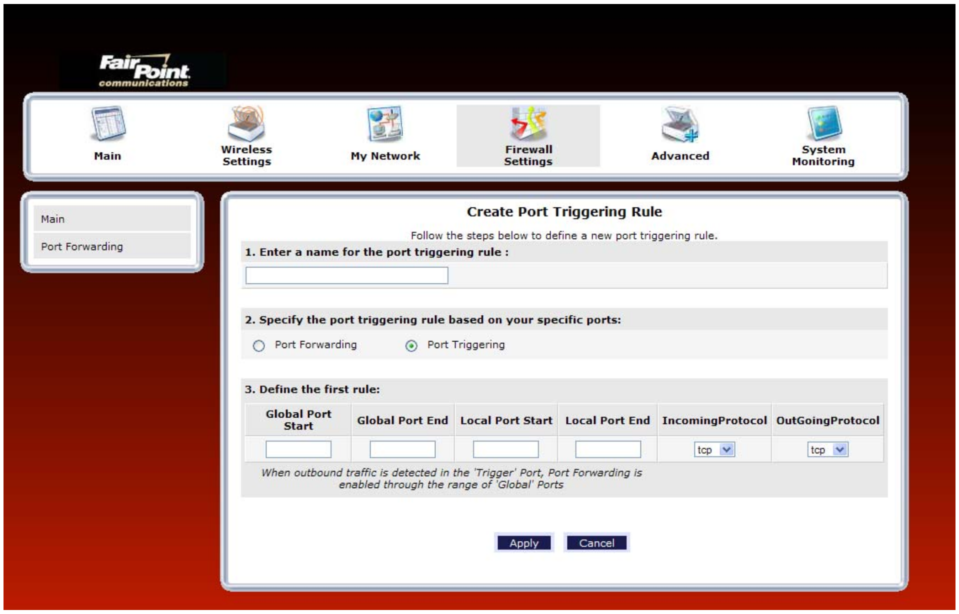
2. Specify the port forwarding entry based on your specific ports:

● Port Forwarding ○ Port Triggering

3. Define the first rule:

Protocol	Global PortStart	Global PortEnd	Base HostPort
tcp			

If you clicked the **Port Triggering** option in the preceding screen, the following **Create Port Triggering Rule** screen will be displayed.



Create Port Triggering Rule

Follow the steps below to define a new port triggering rule.

1. Enter a name for the port triggering rule :

2. Specify the port triggering rule based on your specific ports:

○ Port Forwarding ● Port Triggering

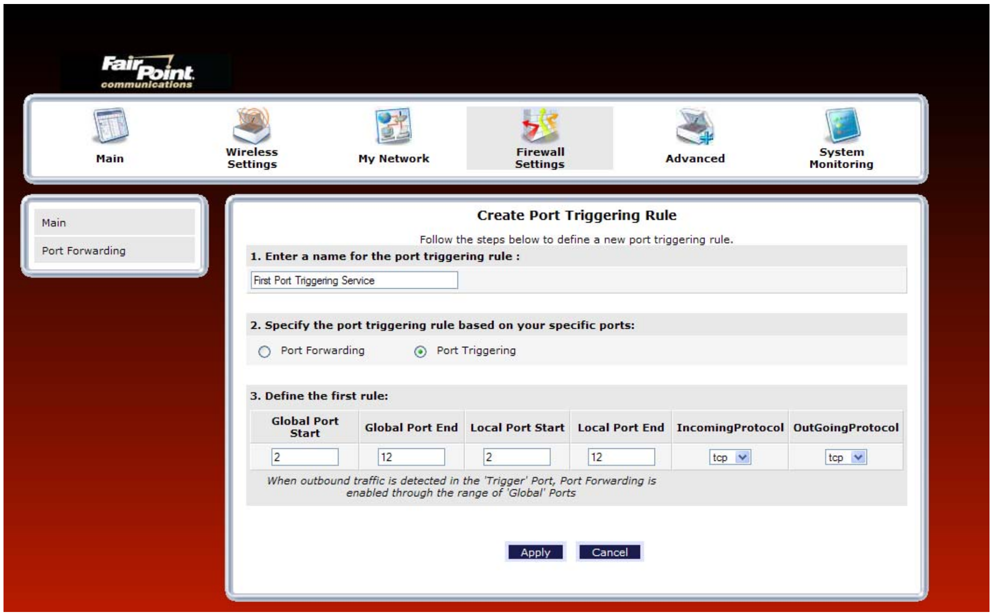
3. Define the first rule:

Global Port Start	Global Port End	Local Port Start	Local Port End	IncomingProtocol	OutGoingProtocol
				tcp	tcp

When outbound traffic is detected in the 'Trigger' Port, Port Forwarding is enabled through the range of 'Global' Ports

2. Type the name of the custom service that you are creating in the field provided. This will be the name of the port forwarding service for which you are configuring specific Port Triggering rules.
3. Enter the desired Global Port Start, Global Port End, Local Port Start, and Local Port End values in the fields provided, as shown in the example below.
4. Select the desired Incoming and Outgoing protocol for the rule.
5. Click **Apply** to allow the changes to take effect.

NOTE: If you clicked **Cancel** in the **Create Port Triggering Service** screen, the values you entered will be displayed; however, they will not be active in your Router. You must click **Apply** to allow the settings to take effect.



Create Port Triggering Rule

Follow the steps below to define a new port triggering rule.

1. Enter a name for the port triggering rule :

First Port Triggering Service

2. Specify the port triggering rule based on your specific ports:

○ Port Forwarding ● Port Triggering

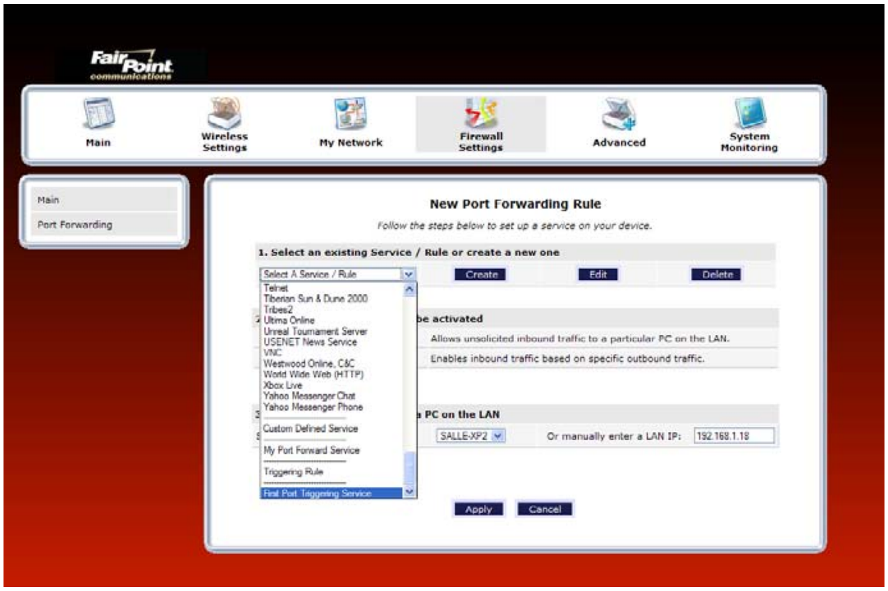
3. Define the first rule:

Global Port Start	Global Port End	Local Port Start	Local Port End	IncomingProtocol	OutGoingProtocol
2	12	2	12	tcp	tcp

When outbound traffic is detected in the 'Trigger' Port, Port Forwarding is enabled through the range of 'Global' Ports

Port Triggering Service	
Global Port Start	The WAN side TCP/UDP start port.
Global Port End	The WAN side TCP/UDP end port.
Local Port Start	The local LAN side TCP/UDP start port.
Local Port End	The local LAN side TCP/UDP end port.
Incoming Protocol	The protocol to use for inbound traffic.
Outgoing Protocol	The protocol to use for outbound traffic.

6. After you click **Apply,** the following screen will be displayed. From the drop-down list, select name of your custom port triggering rule (the name will appear at the bottom of the list under **Triggering Rule**).
7. Click **Apply** to allow the service to be added to the Router's list of active services.



New Port Forwarding Rule

Follow the steps below to set up a service on your device.

1. Select an existing Service / Rule or create a new one

be activated

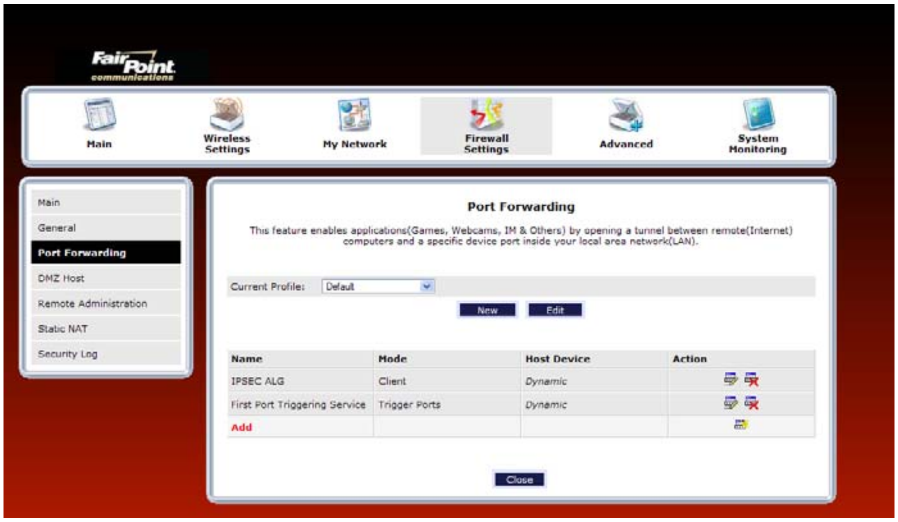
Allows unsolicited inbound traffic to a particular PC on the LAN.

Enables inbound traffic based on specific outbound traffic.

PC on the LAN

Or manually enter a LAN IP: 192.168.1.18

If you click **Apply**, the following screen will appear. The Port Triggering service has been added to the list of active services. To add additional port triggering services to your Router, repeat steps 1 through 7.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

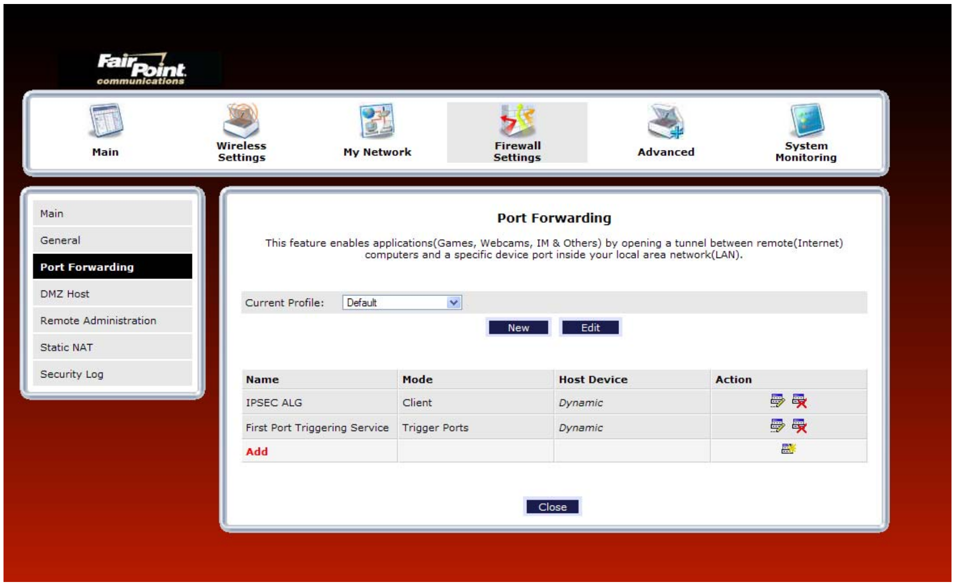
Current Profile: Default

Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	
First Port Triggering Service	Trigger Ports	*Dynamic*	
Add			

15.3.3.4 Deleting a Port Forwarding or Port Triggering Service

If you have created a port forwarding or port triggering service and have added it to your Router’s list of active services, at the **Port Forwarding** screen you can do one of the following:

- Click the delete icon adjacent to the service you want to delete.
- Click the details icon adjacent to the service you want to view.



Port Forwarding

This feature enables applications(Games, Webcams, IM & Others) by opening a tunnel between remote(Internet) computers and a specific device port inside your local area network(LAN).

Current Profile: Default

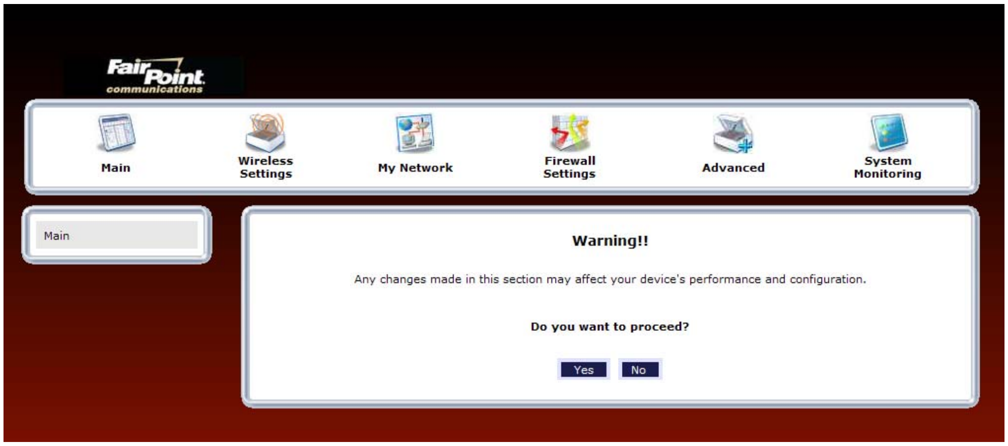
Name	Mode	Host Device	Action
IPSEC ALG	Client	*Dynamic*	✎ ✗
First Port Triggering Service	Trigger Ports	*Dynamic*	✎ ✗
Add			✎

15.4 DMZ Host—Single IP Address Passthrough

In the **Firewall Settings** screen, select **DMZ Host** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

> **Any changes made in this section may affect your device’s performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.



Warning!!

Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

15.4.1 Enabling DMZ Host

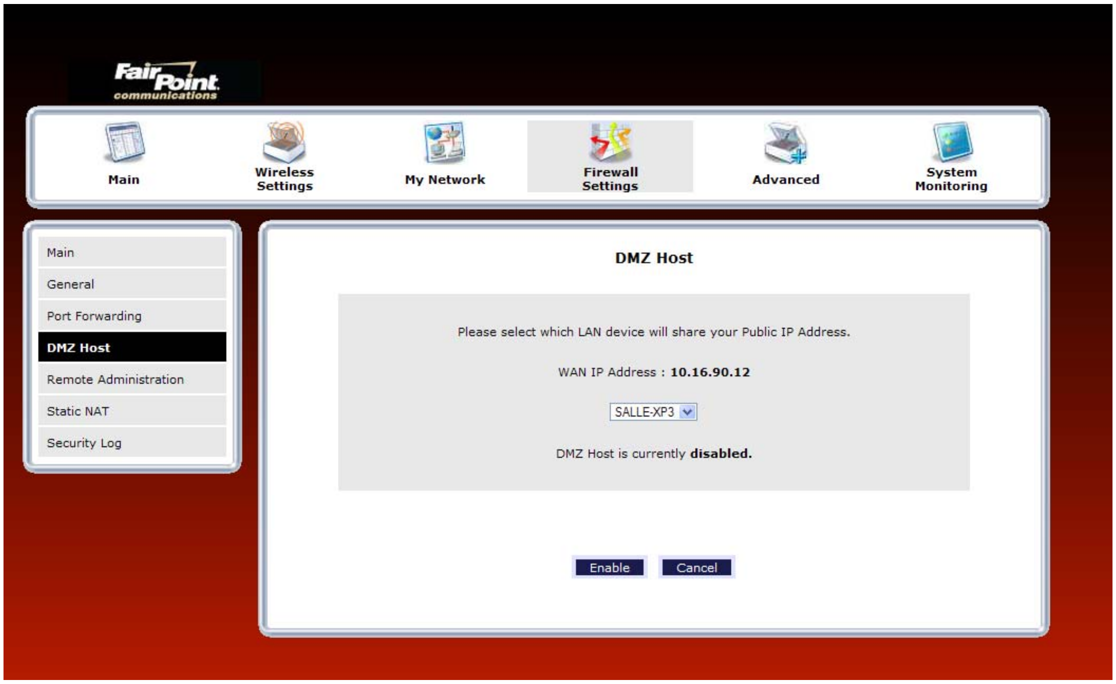
If you clicked **Yes**, in the preceding warning screen, the following **DMZ Host** screen will be displayed. The demilitarized zone (DMZ) feature allows you to select one device on the LAN that will share the WAN-assigned IP address. By enabling DMZ, the selected device becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for DMZ. If you are using Bridge protocol, you will not be able to configure DMZ Host in the Router.

IMPORTANT:

1. Before you configure DMZ Host, configure your PC settings to obtain an IP address from VersaLink automatically. If needed, refer to your computer's Windows help screen for instructions.
2. If you have previously enabled Public LAN, you will need to disable Public LAN and enable the DHCP for Private LAN and the Private LAN settings before you configure DMZ Host.
3. DMZ Host and Static NAT are mutually exclusive features. Before you enable DMZ Host, confirm that Static NAT is disabled. If needed, refer to section 15.6.2 for details on disabling Static NAT.
4. Enabling DMZ severely affects the vulnerability of the selected computer.

To configure DMZ Host, in the **DMZ Host** screen, select a device from the drop-down menu. The selected device will share your WAN IP address. Next, click **Enable** to allow the setting to take effect.

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



DMZ Host

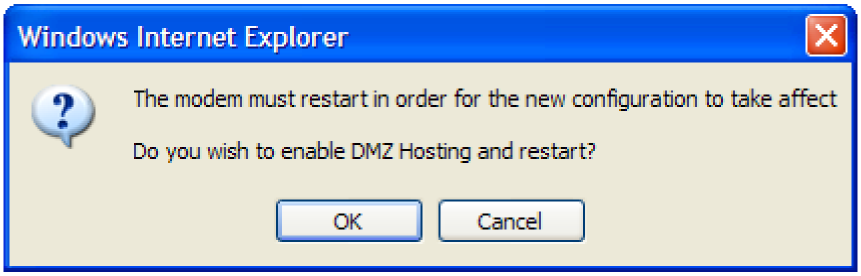
Please select which LAN device will share your Public IP Address.

WAN IP Address : **10.16.90.12**

SALLE-XP3

DMZ Host is currently **disabled.**

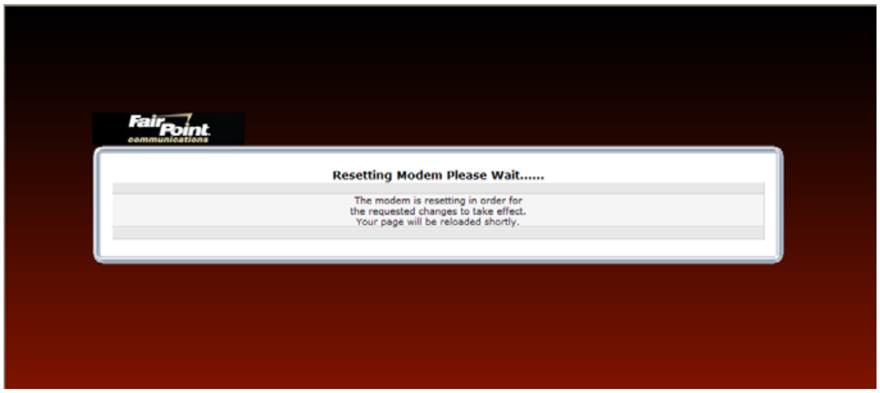
If you clicked **Enable** in the preceding screen, the following pop-up screen will appear. The Router must be reset to allow the new configuration to take effect. Click **OK** to continue.



The modem must restart in order for the new configuration to take affect

Do you wish to enable DMZ Hosting and restart?

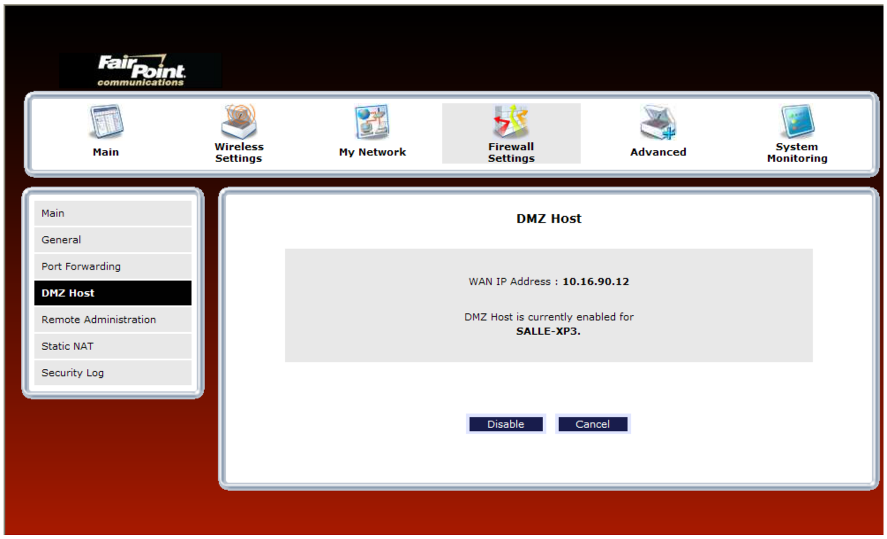
If you clicked **OK**, the following screen will appear. After a brief delay, the home page will be displayed. Confirm that you have a DSL link and that your PPP Status displays **UP.** (If necessary, click the **Connect** button to establish a PPP session).



Resetting Modem Please Wait......

The modem is resetting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

To confirm that DMZ Host has been enabled, select **Firewall Settings** in the top navigational menu, and then click **DMZ Host** in the submenu options at the left of the screen. Next, click **Yes** in the warning screen. The following **DMZ Host** screen will be displayed. This screen shows that DMZ Host is currently enabled for the selected device.



DMZ Host

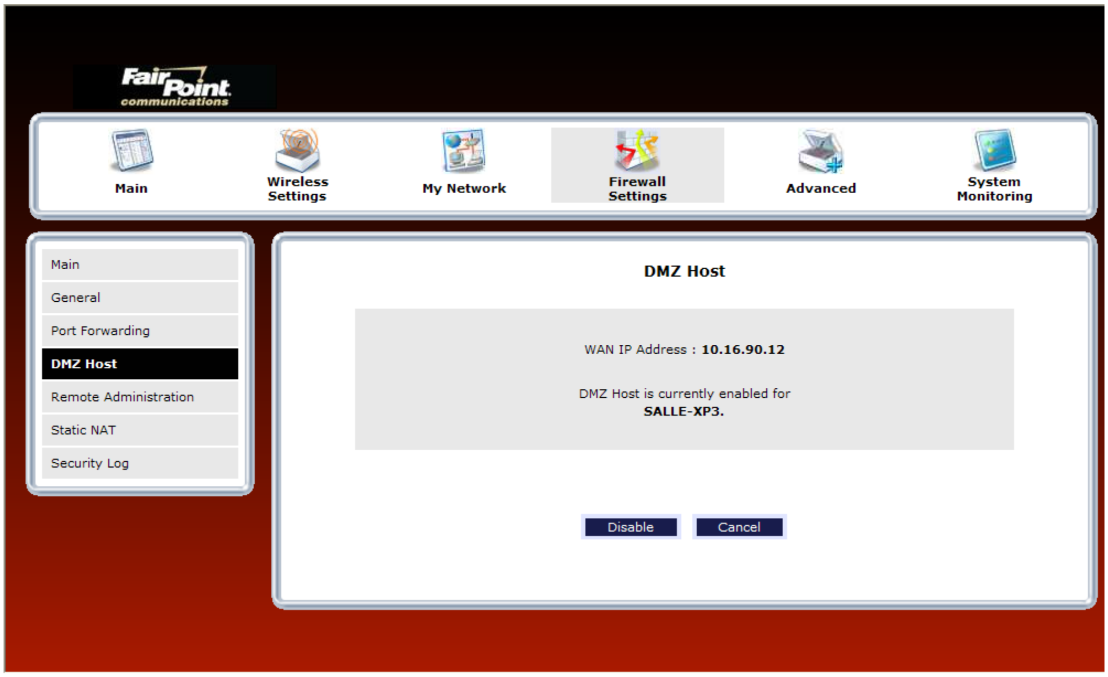
WAN IP Address : **10.16.90.12**

DMZ Host is currently enabled for
SALLE-XP3.

IMPORTANT: After you disable DMZ Host, you may need to release and renew your IP address to communicate with the Modem.

15.4.2 Disabling DMZ Host

To disable DMZ Host (if it has been previously enabled), click **Disable** in the DMZ Host screen.

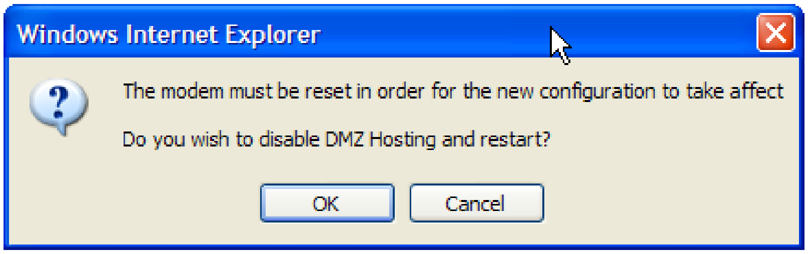


DMZ Host

WAN IP Address : **10.16.90.12**

DMZ Host is currently enabled for
SALLE-XP3.

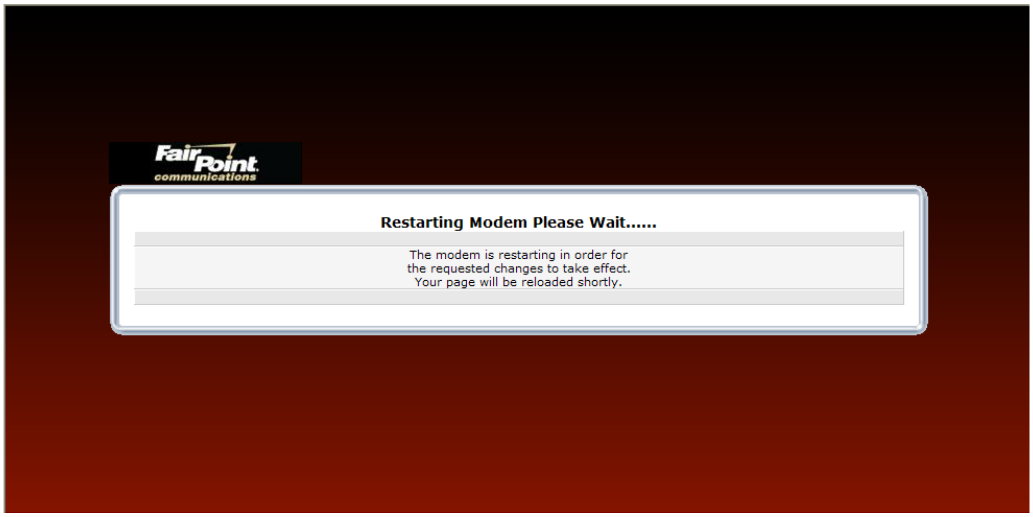
If you clicked **Disable**, the following screen will be displayed. The Router must be reset to allow the new configuration to take effect. Click **OK** to continue.



The modem must be reset in order for the new configuration to take affect

Do you wish to disable DMZ Hosting and restart?

If you clicked **OK**, the following screen will appear. A the home page confirm that you have a DSL link and that your PPP Status displays **UP.** (If necessary, click the **Connect** button to establish a PPP session).



Restarting Modem Please Wait......

The modem is restarting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

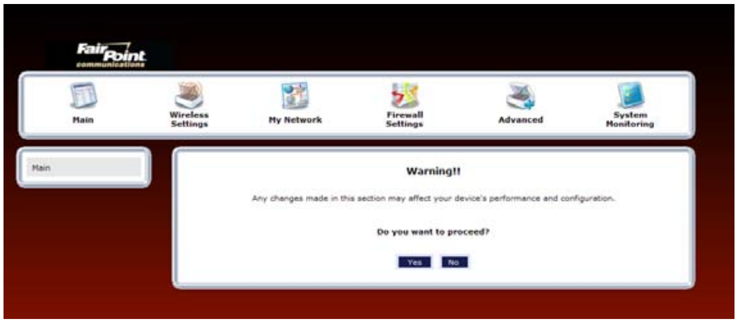
IMPORTANT: After you disable DMZ Host, you may need to release and renew your IP address to communicate with the Modem.

15.5 Remote Administration

In the **Firewall Settings** screen, select **Remote Administration** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

> **Any changes made in this section may affect your device's performance and configuration. Do you want to proceed?**

Click **Yes** to proceed.



Warning!!

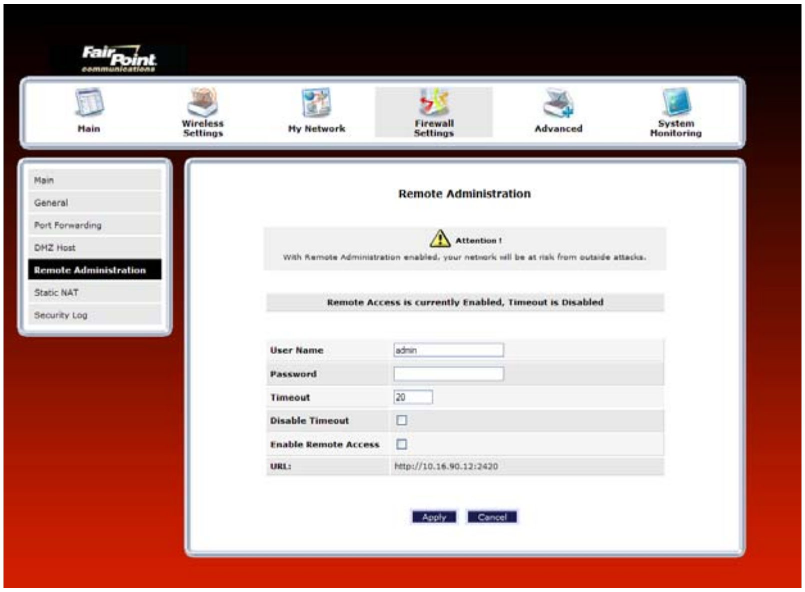
Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

If you clicked **Yes** in the warning screen, the following **Remote Administration** screen will appear. Follow the steps below to configure Remote Administration in your Router.

> **NOTE:** The User Name and Password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks. The user name and password are case sensitive.

1. Type the administrator's User Name. (By default **admin** appears in this field; however, you can change this value, if desired).
2. Type the administrator's Password.
3. Enter the number of minutes after which you want remote access to time out.
4. Click the **Enable Remote Access** box (a check mark will appear in the box).
5. Click **Apply** to allow the settings to take effect.



Remote Administration

Attention !

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

Remote Access is currently Enabled, Timeout is Disabled

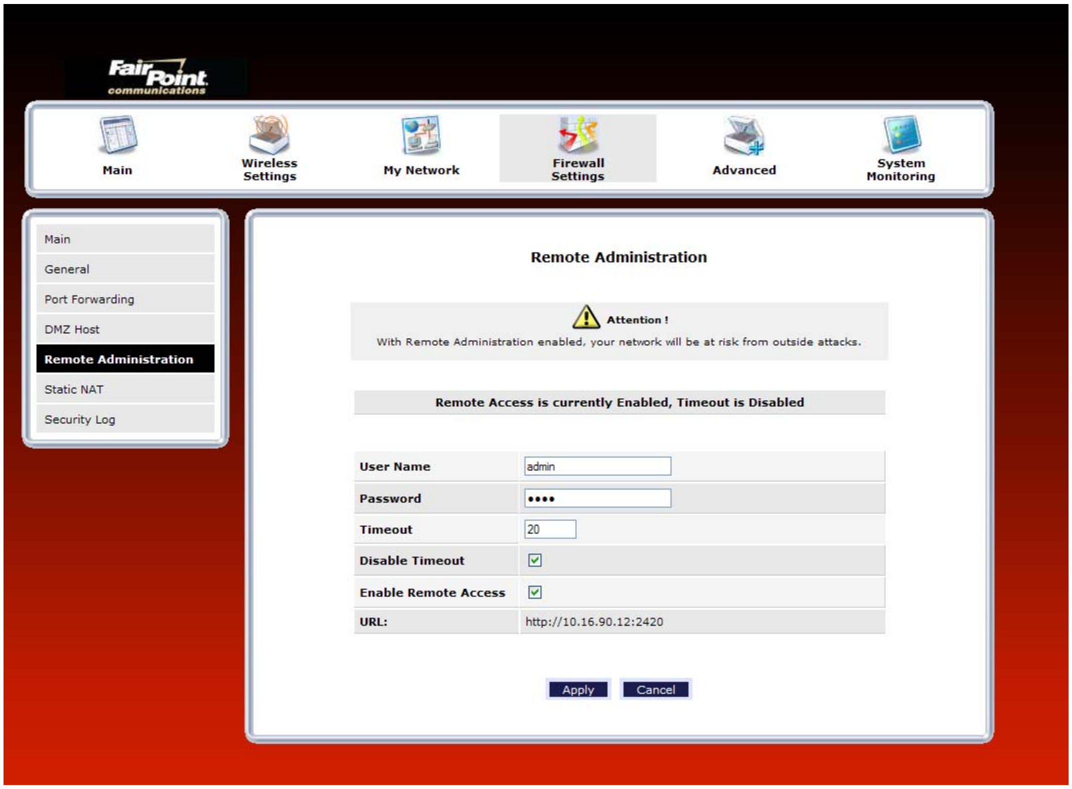
User Name	admin
Password	
Timeout	20
Disable Timeout	☐
Enable Remote Access	☐
URL:	http://10.16.90.12:2420

Remote Administration	
User Name	Enter the user name in this field.
Password	Enter your password in this field.
Timeout	Default = 20 minutes Enter the number of minutes after which remote access will be deactivated. (It will also be deactivated if the Router is reset to factory defaults).
Disable Timeout	Click this box (a check mark will appear) to activate the Disable Timeout feature. This means that once you enable Remote Access, it will remain on until you reset the Router to factory defaults. This function overrides any timeout values. Deselect the box to deactivate this feature.
Enable Remote Access	Click this box (a check mark will appear) to enable Remote Access. Deselect the box to disable this feature.
Remote URL	Displays the URL of the remote management device (VersaLink).

The following screen shows a check mark in the **Enable Remote Access** and **Disable Timeout** check boxes. The following message is displayed:

Remote access is currently enabled. After 20 minutes of inactivity, or on reboot, remote access will be automatically disabled.

After 20 minutes of inactivity or on reboot, Remote Access will be automatically disabled. To disable Remote Access, click the **Enable Remote Access** box to clear the check mark. Then click **Apply** to allow the change to take effect.



Remote Administration

Attention !

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

Remote Access is currently Enabled, Timeout is Disabled

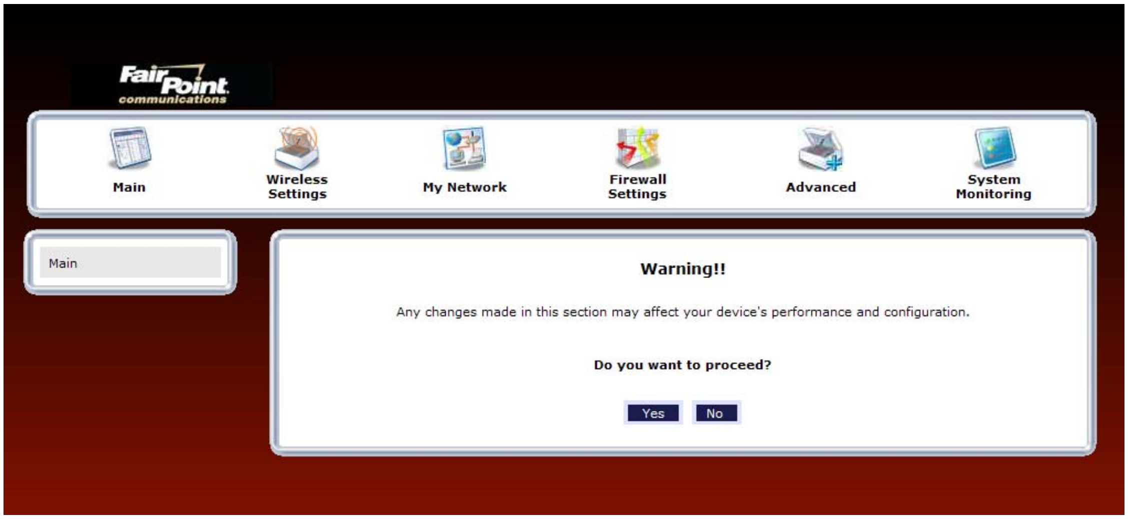
User Name	admin
Password	••••
Timeout	20
Disable Timeout	☑
Enable Remote Access	☑
URL:	http://10.16.90.12:2420

15.6 Static NAT

In the **Firewall Settings** screen, select **Static NAT** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

> **Any changes made in this section may affect your device’s performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.



Warning!!

Any changes made in this section may affect your device's performance and configuration.

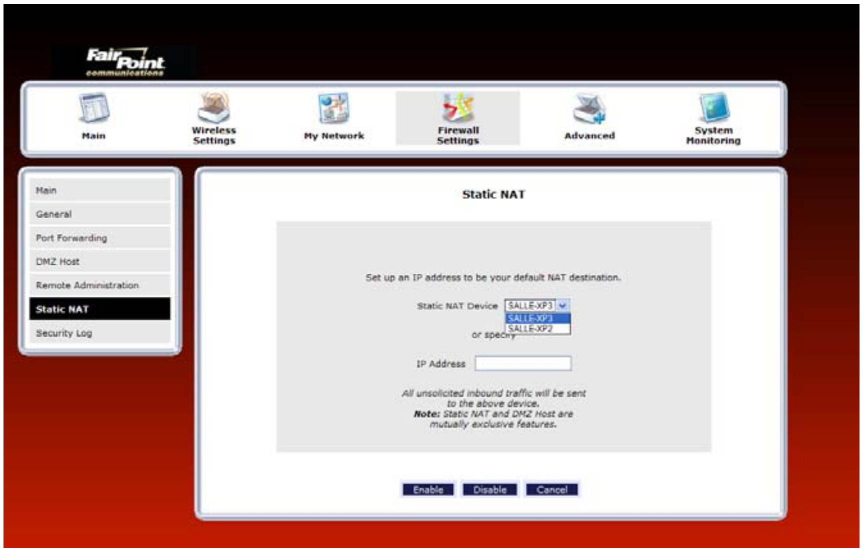
Do you want to proceed?

15.6.1 Enabling Static NAT

If you clicked **Yes** in the warning screen, the following **Static NAT** screen will appear. The **Static NAT** screen allows you to configure your Router to work with the special NAT services. When the Router is configured for Static NAT, any unsolicited packets arriving at the WAN will be forwarded to the selected device. This feature can be used when you want to host a server for a specific application.

IMPORTANT:
Static NAT and DMZ Host are mutually exclusive features. Before you enable static NAT, confirm that DMZ Host is disabled. If needed, refer to section 15.4.2 for details on disabling DMZ Host.

To enable Static NAT, select a device from the **Static NAT Device** drop-down menu, or enter the IP address of the device to which you want to assign Static NAT. Next, click **Enable.**



Static NAT

Set up an IP address to be your default NAT destination.

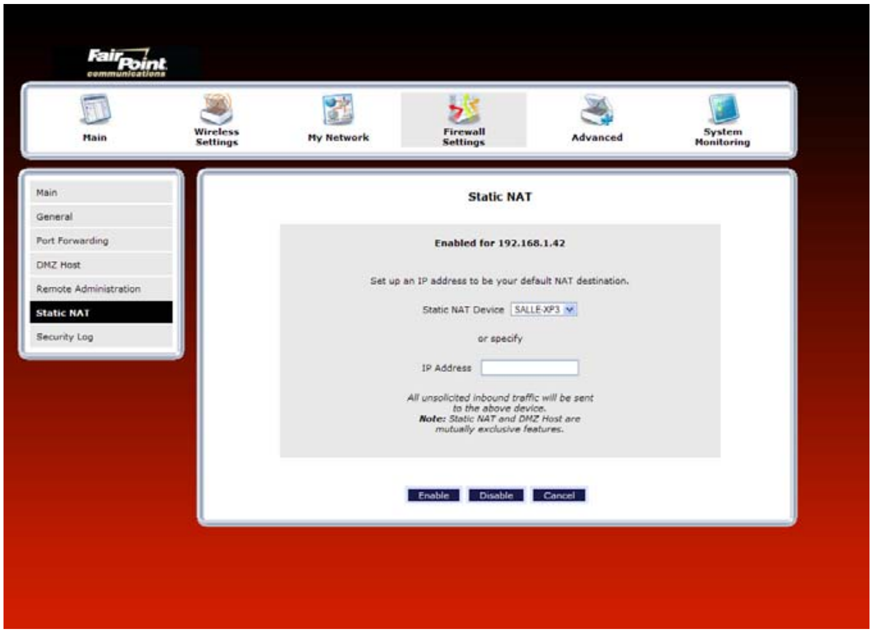
Static NAT Device SALLE-XP3

or specify

IP Address

All unsolicited inbound traffic will be sent to the above device.
***Note:** Static NAT and DMZ Host are mutually exclusive features.*

The following screen shows that Static NAT has been enabled for the device you selected.



Static NAT

Enabled for 192.168.1.42

Set up an IP address to be your default NAT destination.

Static NAT Device SALLE-XP3

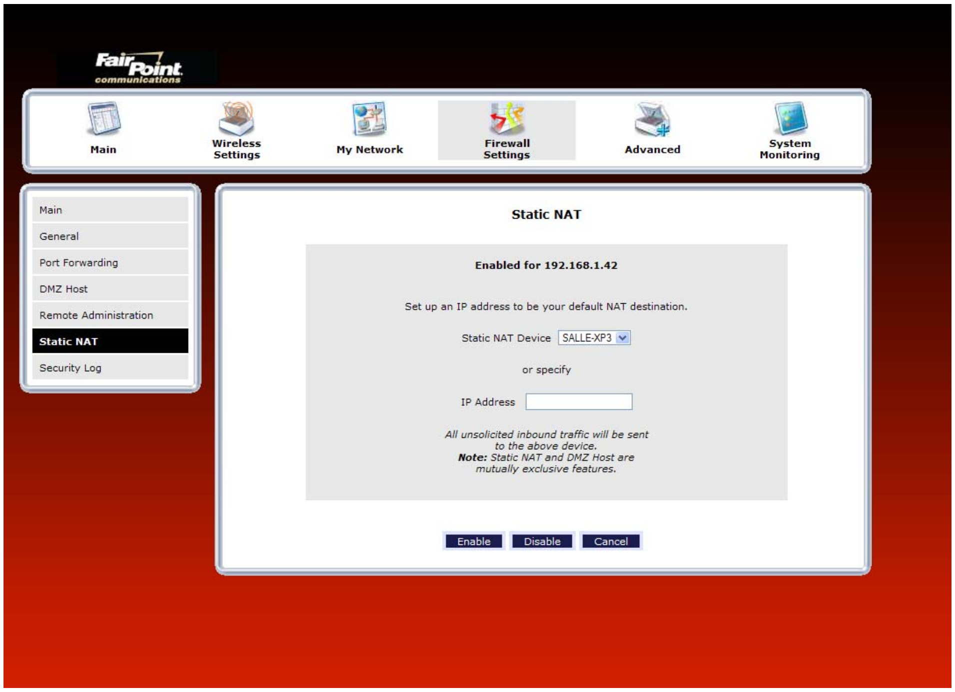
or specify

IP Address

All unsolicited inbound traffic will be sent to the above device.
***Note:** Static NAT and DMZ Host are mutually exclusive features.*

15.6.2 Disabling Static NAT

To disable Static NAT (if it has been previously enabled), click **Disable** in the **Static NAT** screen.



Static NAT

Enabled for 192.168.1.42

Set up an IP address to be your default NAT destination.

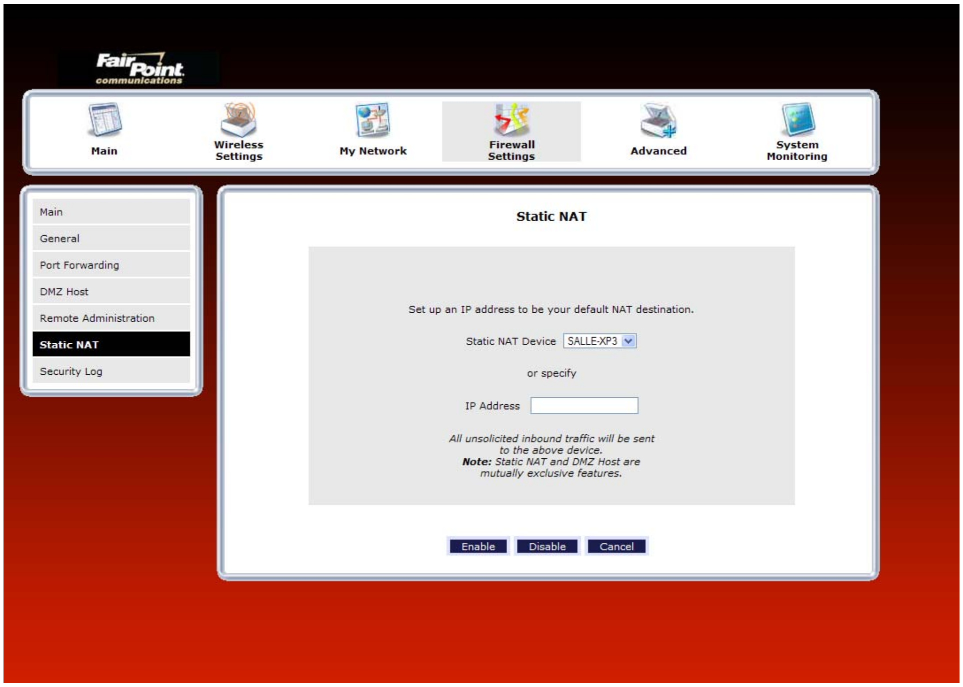
Static NAT Device SALLE-XP3

or specify

IP Address

All unsolicited inbound traffic will be sent to the above device.
***Note:** Static NAT and DMZ Host are mutually exclusive features.*

After you have disabled Static NAT the following screen will show no devices enabled for static NAT.



Static NAT

Set up an IP address to be your default NAT destination.

Static NAT Device SALLE-XP3

or specify

IP Address

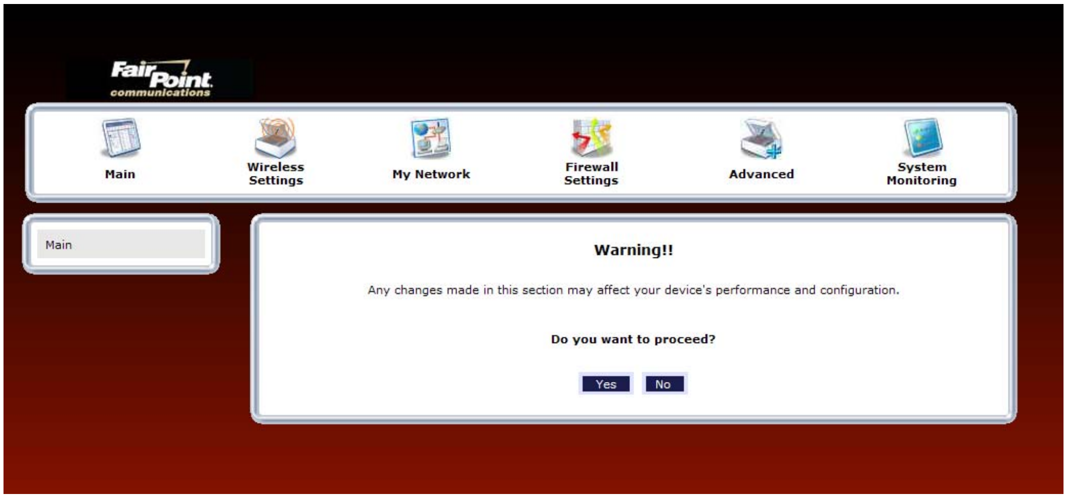
All unsolicited inbound traffic will be sent to the above device.
***Note:** Static NAT and DMZ Host are mutually exclusive features.*

15.7 Security Log

In the **Firewall Settings** screen, select **Security Log** from the submenu options displayed at the left of the screen. A warning screen will display the following message:

> **Any changes made in this section may affect your device's performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.

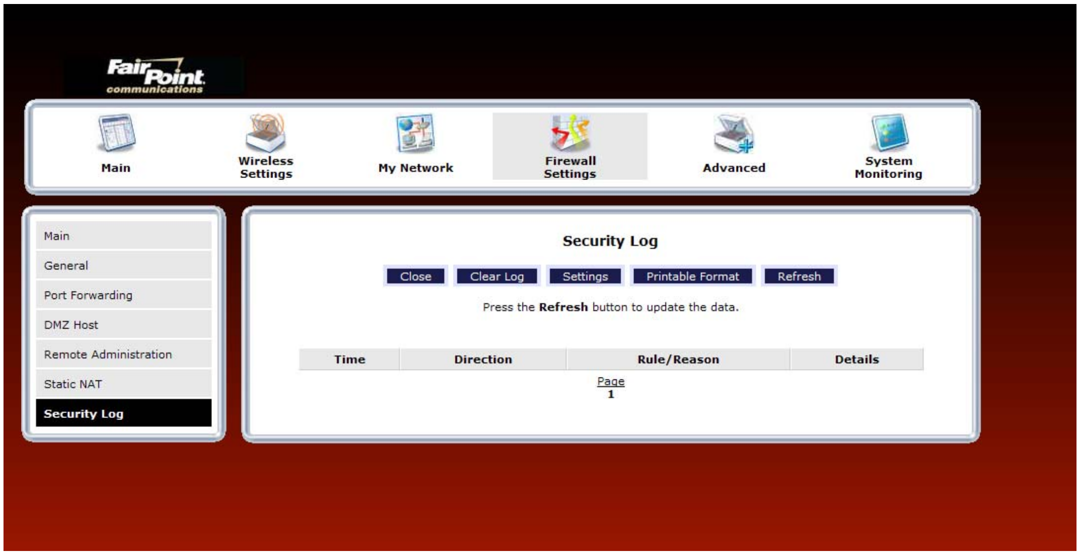


Warning!!

Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

If you clicked **Yes** in the warning screen, the following **Security Log** screen will appear. This screen alerts you of noteworthy information sent to VersaLink from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur.



Security Log

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

Time	Direction	Rule/Reason	Details

Page
1

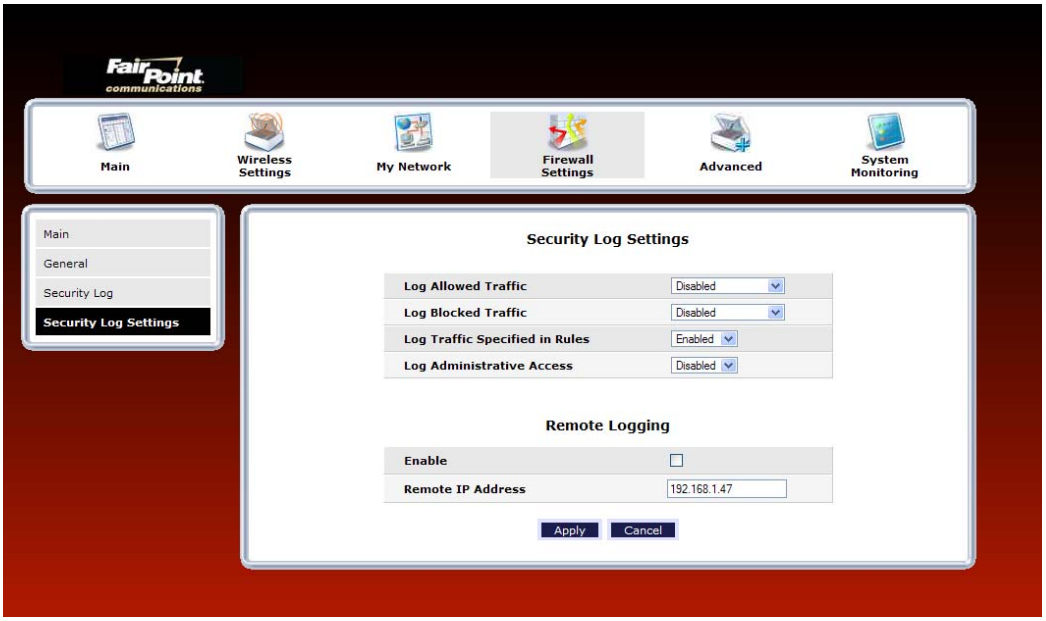
Security Log	
Close	Clicking this button closes the security log screen.
Clear log	Clicking this button removes all entries from the log.
Settings	Clicking this button opens a new window that contains configuration settings for selecting the information that you want logged.
Printable/savable format	Clicking this button opens a new window that contains a list of all the logged packets that can be saved or printed. You can send a copy of the Firewall log to a designated printer.
Refresh	Clicking this button updates the screen so that it displays the most current data.
Time	Displays the time that the packet was sent.
Direction/Source	Displays the direction of transmission.
Rule/Reason	Displays the internal rule that caused the logged event. The internal rule is set up under Firewall rules.
Details	Displays details about logged event.

If you clicked **Settings** in the preceding **Security Log** screen, the following **Firewall Log Settings** screen will appear. This screen allows you to configure firewall remote logging. Remote logging allows the firewall logs to be sent to a machine running a syslog server.

NOTE: The syslog server must be configured to isten on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT_syslog and 3Csyslog.

To configure Remote Logging, do the following:

1. Select the desired firewall log settings from the drop-down menus.
2. Click the **Enable** check box below **Remote Logging** (a check mark will appear in the box).
3. Type the IP address of the syslog server in the **Remote IP Address** field.
4. Click **Apply** to allow the settings to take effect.



Security Log Settings

Log Allowed Traffic	Disabled
Log Blocked Traffic	Disabled
Log Traffic Specified in Rules	Enabled
Log Administrative Access	Disabled

Remote Logging

Enable	☐
Remote IP Address	192.168.1.47

16. ADVANCED

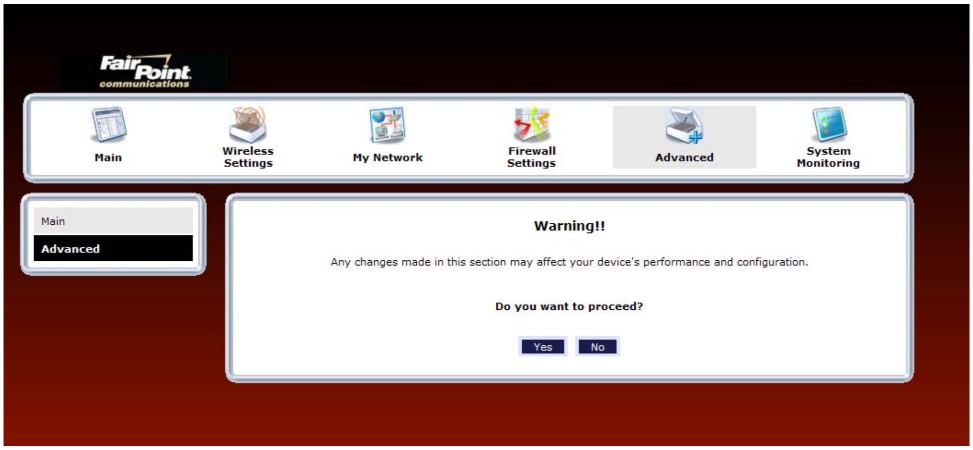
The following sections discuss the advanced features of your Router, such as IP address distribution, firmware upgrades, etc.

IMPORTANT: This section assumes that you have active DSL and Internet service.

If you select **Advanced** in the top navigational menu, a warning screen will display the following message:

> **Any changes made in this section may affect your device's performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.

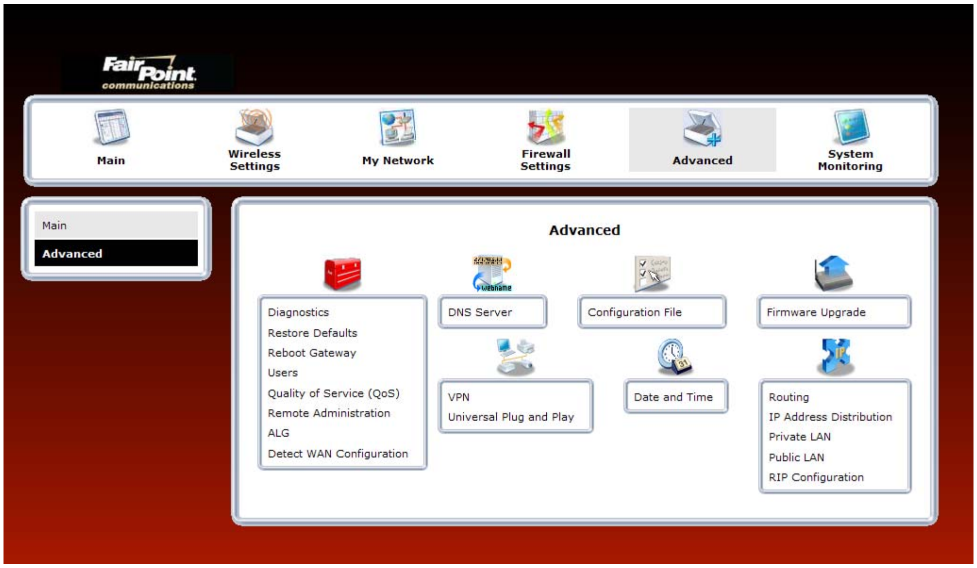


Warning!!

Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

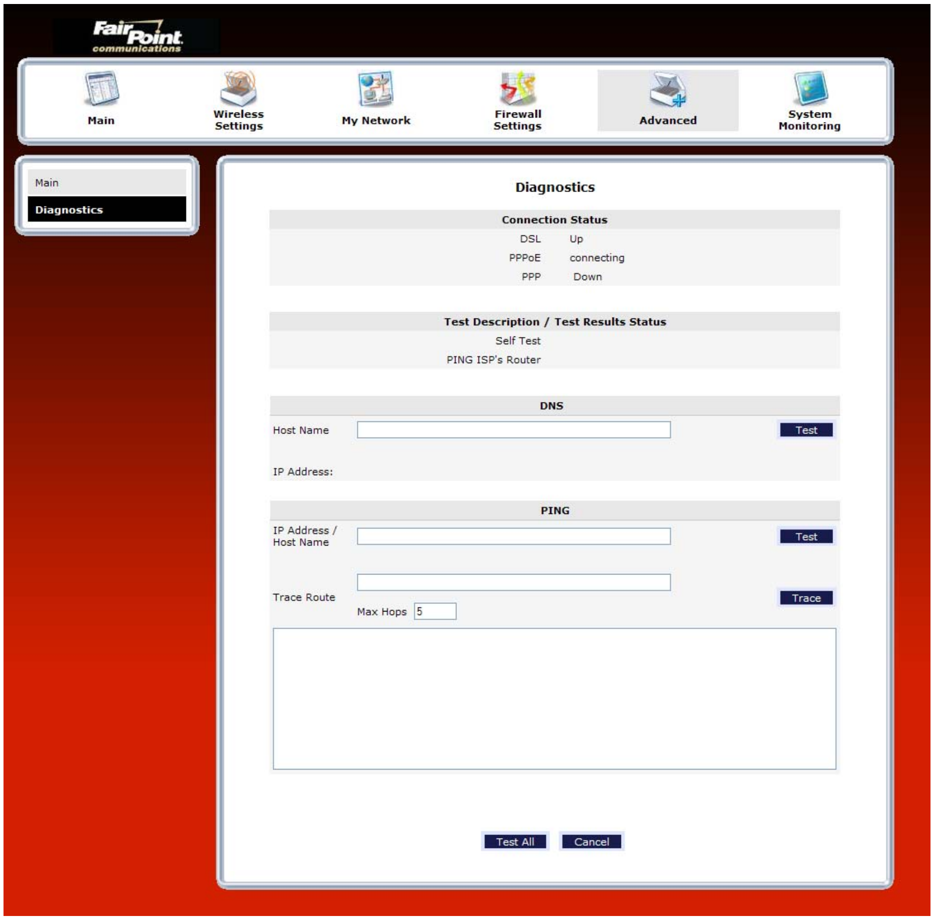
If you clicked **Yes** in the preceding warning screen, the following screen will appear. The **Advanced** screen allows you to access various configurable features in your Router. To access a feature, click the link of the feature that you want to access. The features shown in this page will be discussed in the following sections.



16.1 Diagnostics

In the **Advanced** screen, click **Diagnostics.** The following screen will appear. Using this screen, you can run the following diagnostics tests:

- To run a DNS test, type the appropriate host name in the field provided, and then click **test.**
- To run a PING test, type the appropriate IP address or host name in the field provided, and then click **test.**
- To run a Trace Route, type the appropriate IP address or host name in the field provided, and then click **trace.**
- To run a full diagnostic test on your Router, click **Test All.**



Diagnostics

Connection Status	
DSL	Up
PPPoE	connecting
PPP	Down

Test Description / Test Results Status

Self Test

PING ISP's Router

DNS

Host Name

IP Address:

PING

IP Address / Host Name

Trace Route

Max Hops 5

If you want to PING using the System Self Test screen (diagnostics page) shown above, enter your **DNS** or **IP** address in the fields provided and click on the **test** button. The System Self Test will run a diagnostic test that executes independent of firewall security settings. See the following table for test descriptions and possible responses.

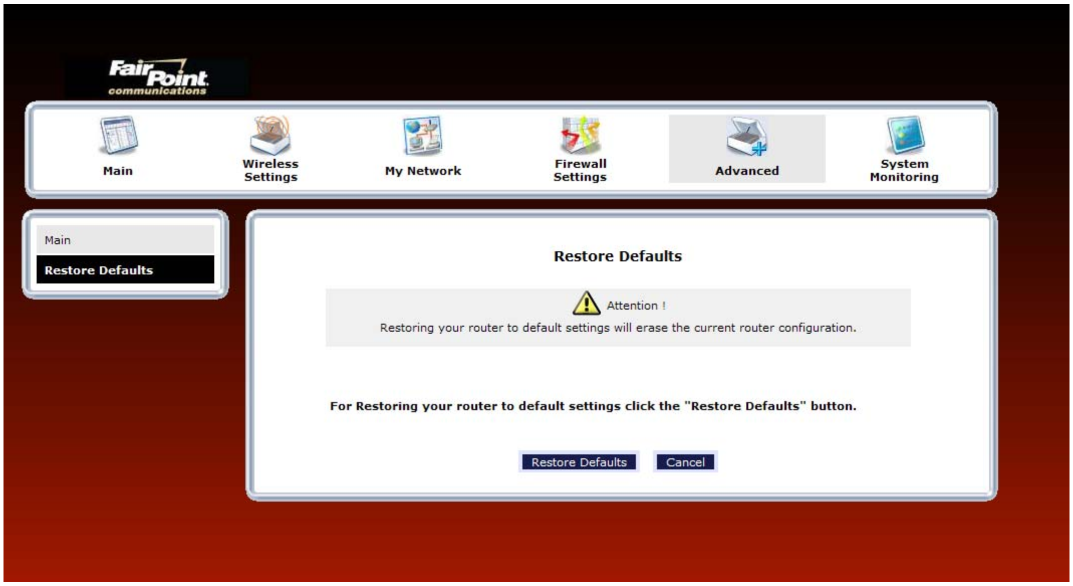
If you want to PING using the MS-DOS (shell) window, first you will need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on VersaLink's firewall settings.) If your firewall is set to **Medium** or **High**, you will not be able to PING. You must set your firewall security setting to **Low** or **None**.

Diagnostics	
DSL	VersaLink checks the status of the DSL connection. Possible Responses: Connection Up: VersaLink is operating correctly and has obtained synchronization with the opposing network device. Connection down: VersaLink is operating correctly, but has not synchronized with the opposing device.
PPPoE	Indicates that a PPPoE session is or is not established. Possible Responses: Session Up: A valid PPPoE session has been detected. No Session: Currently there is no active PPPoE session established. Initiating Session: A PPP session must be connected from the home page.
PPP	Indicates that a PPPoE or PPPoA session must already be established. Possible Responses: Connection Up: VersaLink has established a connection No Connection: There is no PPP connection Initiating Connection: The PPP connection process has been initiated Connection Halted: A successful PPP connection was halted Cannot Connect: A PPP connection could not be made because of a PPPoE session failure. Authorization Failure: The user name or password is incorrect. Link Control Protocol Failed: Reestablish the session (from the home page).
Test Description / Test Results	
Self Test	Performs an integrity check of certain internal components of VersaLink.
PING ISP's Router	Performs an IP network check (i.e., an IP Ping) of the service provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. Possible Responses: Success: VersaLink has detected an IP Remote Router connection. No Response: The IP Remote Router does not answer the IP Ping. Could not test: The test could not be executed due to Router settings. Check your DSL link or your PPP session. You must have both a DSL link and a PPP connection established to execute a PING.
DNS	Performs a test to try to resolve the name of a particular host. The host name is entered in the input box. Possible Responses: Success: VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box. No Response: VersaLink has failed to obtain the resolved address. Host not found: The DNS Server was unable to find an address for the given host name. No data, enter host name: No host name is specified. Could not test: The test could not be executed due to VersaLink settings. Check your DSL link or your PPP session. You must have both a DSL link and a PPP connection established to execute a PING.
IP Address	IP Address of the Host Name.
PING (via IP Address or Host Name)	Performs an IP connectivity check to a remote computer either within or beyond the service provider's network. You can PING a remote computer via the IP address or the DNS address. If your PING fails, try a different IP or DNS address. Possible Responses: Success: The Remote Host computer was detected. No Response: There was no response to the Ping from the remote computer. No name or address to PING: No host name or IP address was specified. Could not test: The test could not be executed due to Router settings. Check your DSL link or your PPP session. You must have both a DSL link and a PPP connection established to execute a PING.
Trace Route	Determines the route taken to destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Trace Route is used to determine where the packet is stopped on the network.

16.2 Restore Defaults

In the **Advanced** screen, click **Restore Defaults.** This screen allows you to restore the Router to its factory default settings. To restore the Router, click the **Restore Defaults** button**.**

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



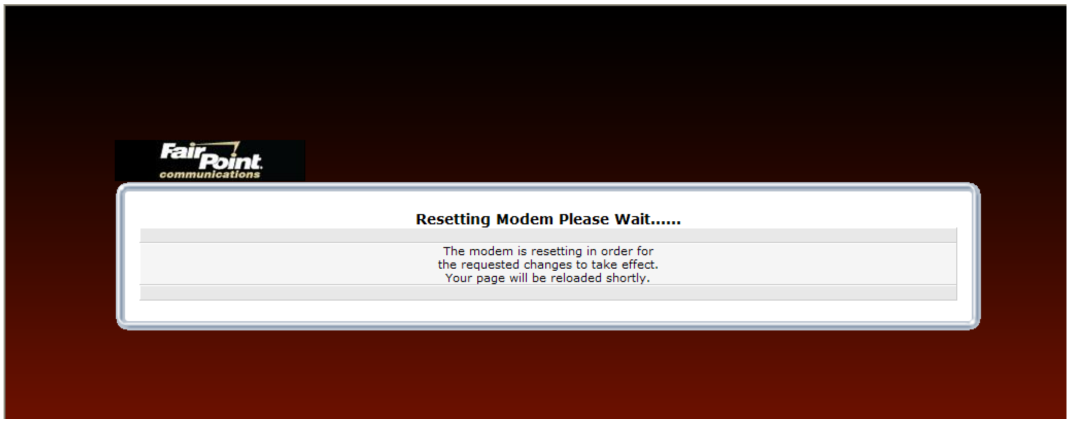
Restore Defaults

Attention !

Restoring your router to default settings will erase the current router configuration.

For Restoring your router to default settings click the "Restore Defaults" button.

If you clicked **Restore Defaults**, the following screen will appear. Please wait a brief moment while the Router resets.



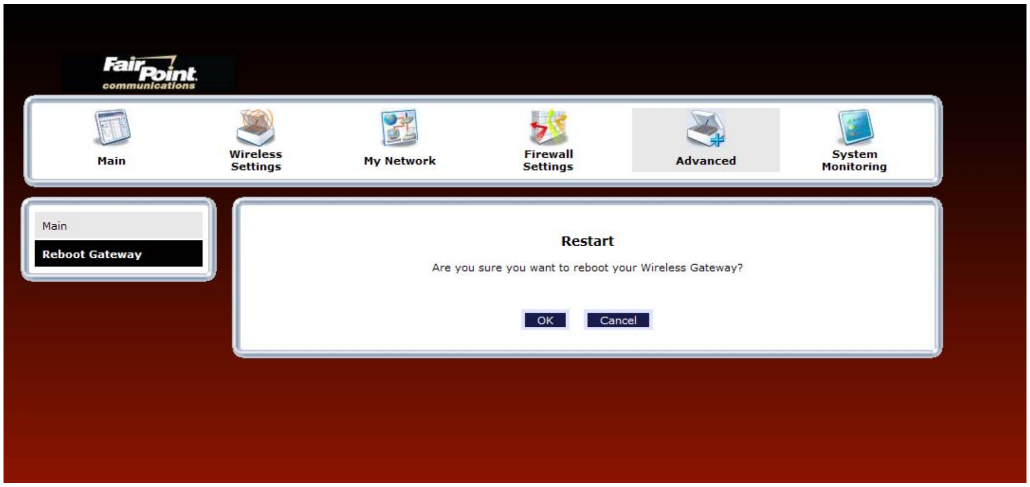
Resetting Modem Please Wait......

The modem is resetting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

After the Router has reset, follow the instructions explained in section 8.1 to log on to your Router.

16.3 Reboot Gateway

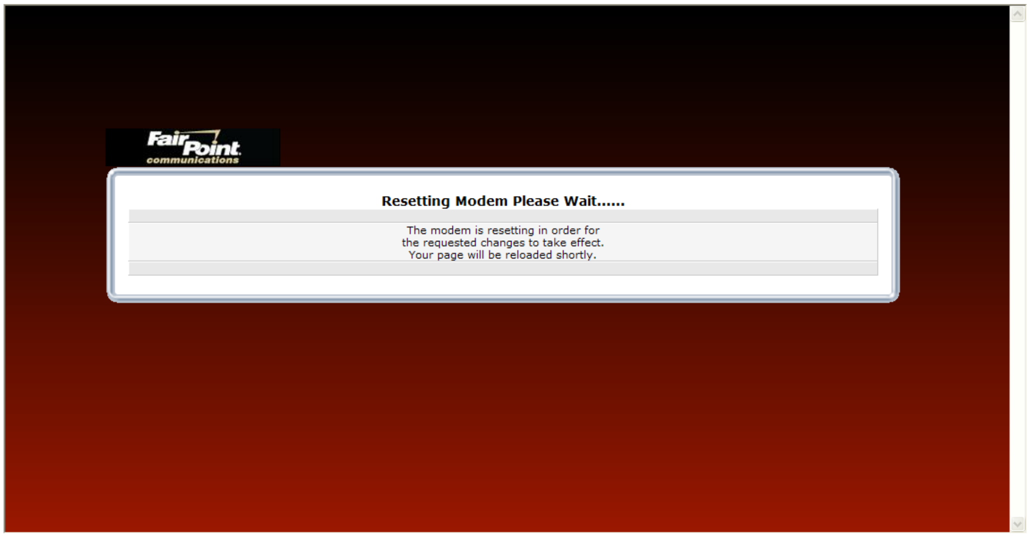
In the **Advanced** screen, click **Reboot Gateway.** This screen allows you to reboot your Router without losing any customized settings that you have made in the Router. Click **OK** to reboot your Router.



Restart

Are you sure you want to reboot your Wireless Gateway?

If you clicked **OK**, the following screen will appear. Please wait a brief moment while the Router reboots.



Resetting Modem Please Wait......

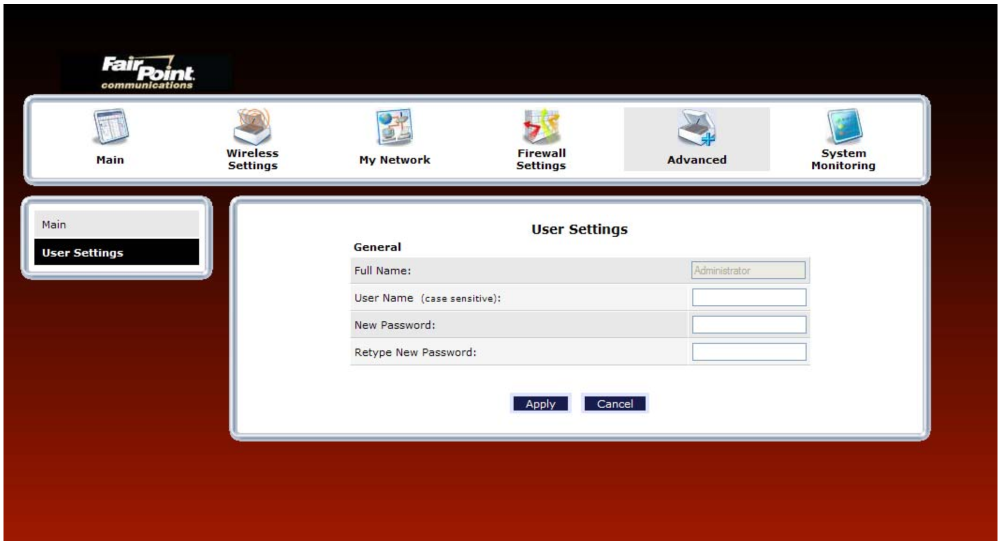
The modem is resetting in order for
the requested changes to take effect.
Your page will be reloaded shortly.

16.4 Users

In the **Advanced** screen, click **Users**. The following **User Settings** screen allows you to change the administrator's user name and password. Type the desired values in the fields provided, and then click **Apply** to allow the settings to take effect. Refer to section 8.2, "Changing the Password," for details on this feature.

NOTE:

1. If the Router is password protected and you are not an authorized user, you will not be able to change the values in this screen. (The Router cannot be configured unless an authorized user is logged on.) Contact your network administrator for further instructions.
2. The values typed in the password fields will be masked for security purposes.
3. This feature changes the Administrator's password, not the PPP password.



User Settings

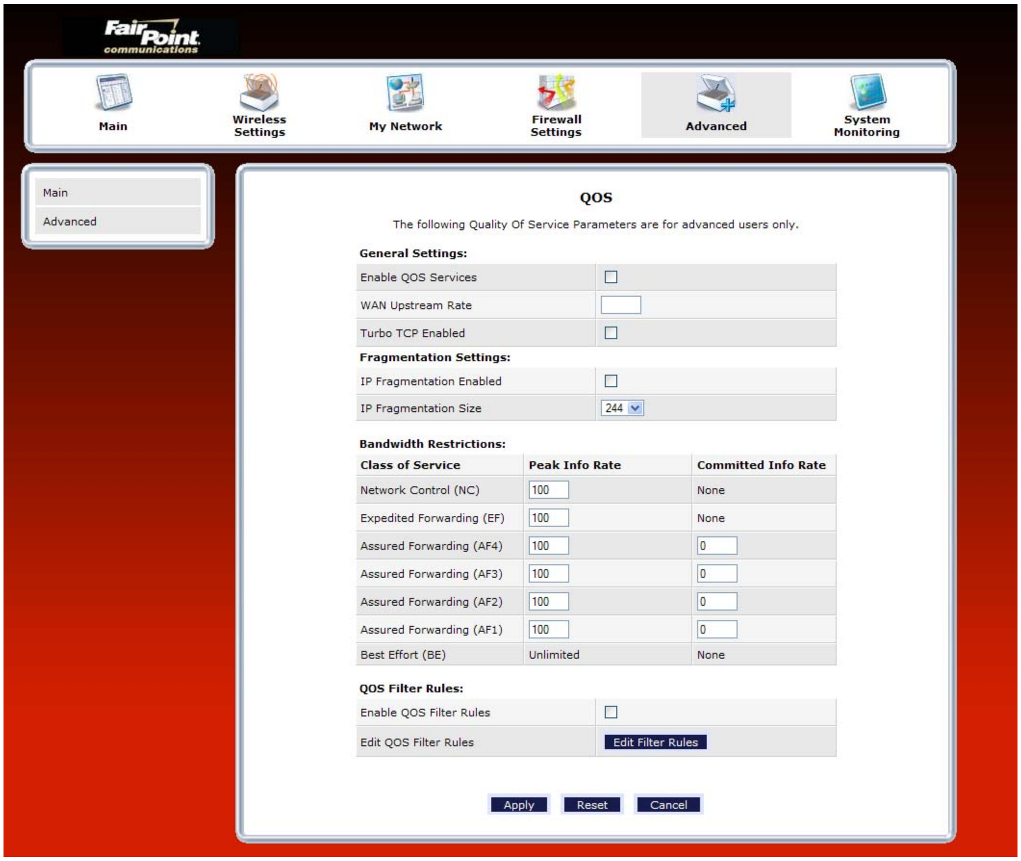
General

Full Name:	Administrator
User Name (case sensitive):	
New Password:	
Retype New Password:	

User Settings	
Full Name	Displays the Administrator name. This field will be dimmed and unavailable for changes.
User Name	Type the Administrators user name. (This field is case sensitive.)
New Password	Type the administrator's new password.
Retype New Password	Confirm the administrator's new password.

16.5 Quality of Service

In the **Advanced** screen, click **Quality of Service (QOS).** This screen allows you to configure Quality of Service parameters in the Router. Select the desired Quality of Service settings, and then click **Apply** to allow the setting to take effect.



QOS

The following Quality Of Service Parameters are for advanced users only.

General Settings:

Enable QOS Services	□
WAN Upstream Rate	
Turbo TCP Enabled	□

Fragmentation Settings:

IP Fragmentation Enabled	□
IP Fragmentation Size	244

Bandwidth Restrictions:

Class of Service	Peak Info Rate	Committed Info Rate
Network Control (NC)	100	None
Expedited Forwarding (EF)	100	None
Assured Forwarding (AF4)	100	0
Assured Forwarding (AF3)	100	0
Assured Forwarding (AF2)	100	0
Assured Forwarding (AF1)	100	0
Best Effort (BE)	Unlimited	None

QOS Filter Rules:

Enable QOS Filter Rules	□
Edit QOS Filter Rules	Edit Filter Rules

16.6 Remote Administration

In the **Advanced** screen, click **Remote Administration**. This screen allows you to configure your Router so that it can be accessed remotely via a URL. Configure this feature to allow maintenance or troubleshooting for your Router.

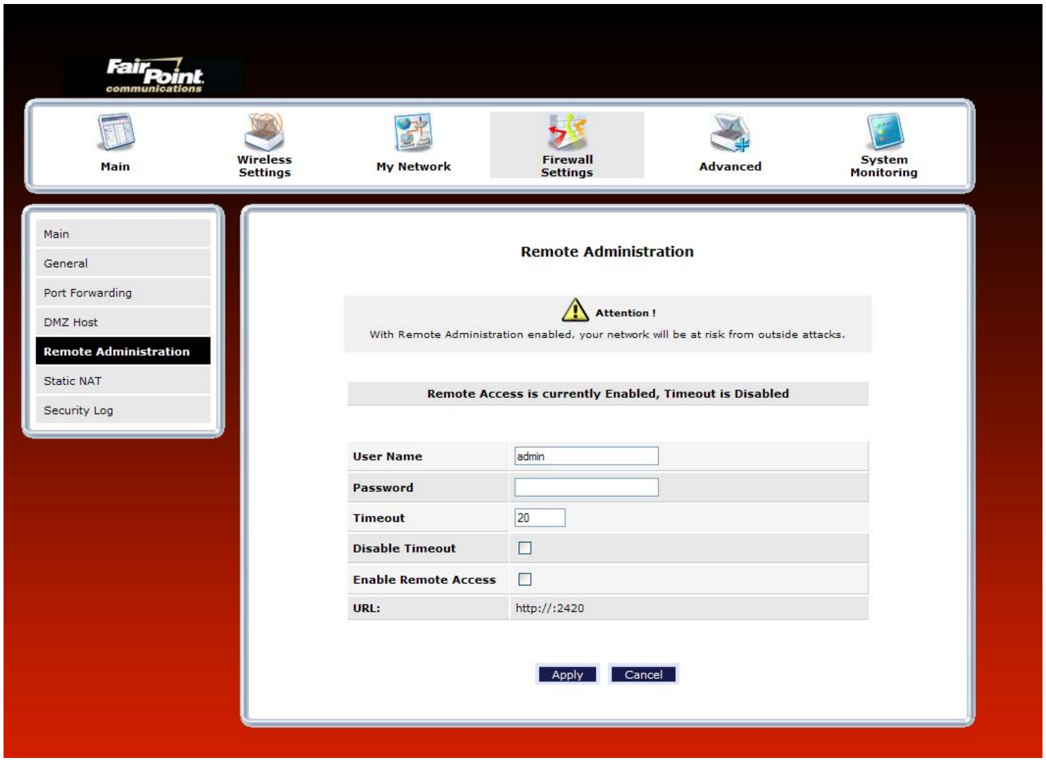
WARNING: With Remote Administration enabled, your network will be at risk from outside attacks.

To enable Remote Administration, do the following:

1. Type the desired user name.
2. Type the desired password.

   NOTE: The password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks in the **Password** field. The password is case sensitive.
3. Enter the number of minutes after which remote access will disconnect, if it is idle.

   NOTE: If you click the **Disable Timeout** check box (a check mark will appear in the box), this will override the preceding timeout minutes, and remote access will remain activated once you enable it.
4. Click the **Enable Remote Access** check box (a check mark will appear in the box).
5. Click **Apply** to allow the settings to take effect.



Remote Administration

Attention !

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

Remote Access is currently Enabled, Timeout is Disabled

User Name	admin
Password	
Timeout	20
Disable Timeout	□
Enable Remote Access	□
URL:	http://:2420

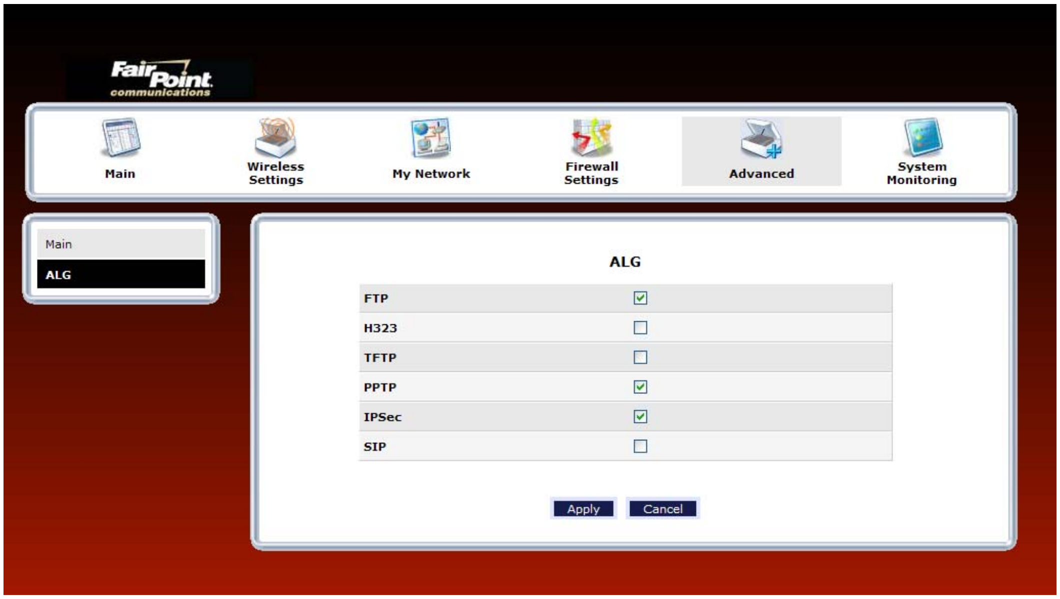
Remote Administration	
User Name	Default = admin The name used for the Remote Administration session. The only valid characters are (a-z, A-Z, 0-9). The user name must be at least 6 characters and must not exceed 12 characters long.
Password	The password used for the remote administration session. Do not use spaces or double-quotes in the password field. The user name must be at least 6 characters and must not exceed 12 characters long.
Timeout	Default = 20 minutes The interval (in minutes) after which the remote access will disconnect, if it is idle.
Disable Timeout	Default = deactivated To activate the Disable Timeout feature, click this box (a check mark will appear). Clear the box to deactivate this feature.
Enable Remote Access	Default = deactivated Click this box (a check mark will appear) to activate Enable Remote Access. Clear the box to deactivate this feature.
Remote URL	Displays the URL for the remote access session.

16.7 ALG

In the Advanced screen, click ALG. This screen allows you to configure your Router so that it can be accessed remotely via a URL. Configure this feature to allow maintenance or troubleshooting for your Router. This page enables you to configure application-level gateway (ALG) services for your Gateway. Click on the box of each service that you want to enable (a check mark will appear in the box). After you have configured the desired settings, click **Save** to save the settings.

Enabling an ALG service opens the IP ports associated with the corresponding service. For example, if you have an IPSec client running on a LAN-side PC attached to the Router, it is necessary to enable the IPSec ALG. Enabling IPSec opens the default ports used by IPSec, 500 and 1500 so that traffic to and from the IPSec client may pass through.

NOTE: When the firewall level is set to “High,” some services may not be configurable.



ALG

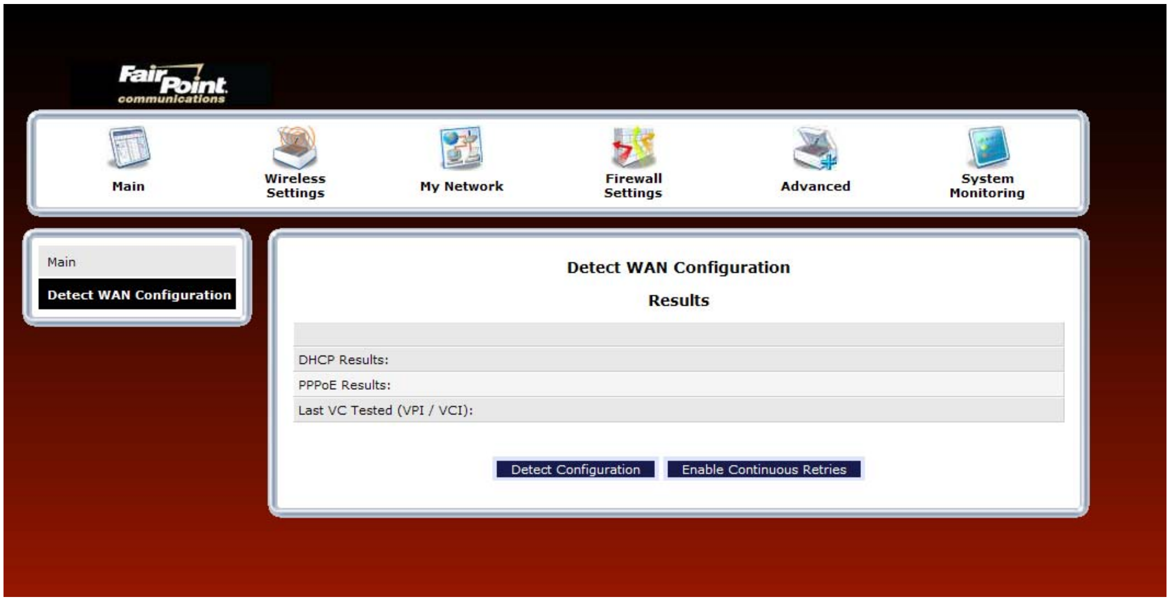
FTP	☑
H323	☐
TFTP	☐
PPTP	☑
IPSec	☑
SIP	☐

16.8 Detect WAN Configuration

In the **Advanced** screen, click **Detect WAN Configuration**. This screen displays the details of your WAN connection.

NOTE: If you have not established and DSL connection with your ISP's equipment and have not established an Internet connection with your ISP, the Router will report **Detection Disabled**. Confirm that you have Internet connection with your ISP. If problems persist, contact your ISP.

To check your WAN connection, click **Detect Configuration.** The Router will be reset.



Detect WAN Configuration

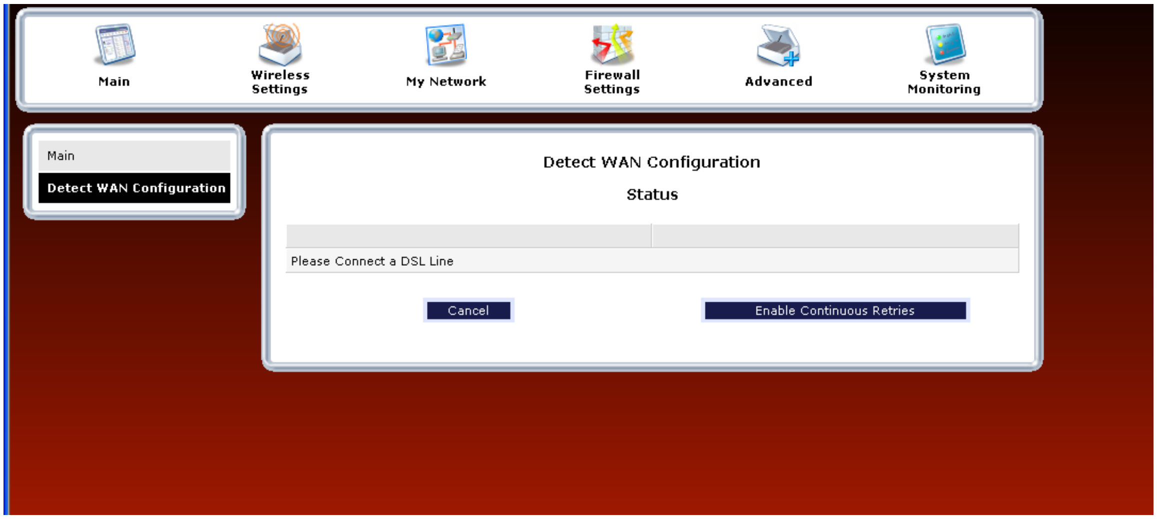
Results

DHCP Results:

PPPoE Results:

Last VC Tested (VPI / VCI):

If no connection is detected, the following screen will appear. Click **Enable Continuous Retries**. The Router will automatically continue to check the WAN connection. After a WAN connection is detected, the Router will report the results.

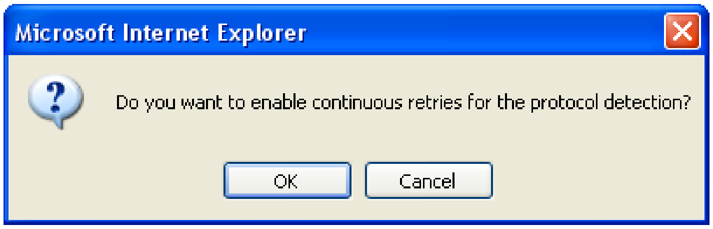


Detect WAN Configuration

Status

Please Connect a DSL Line

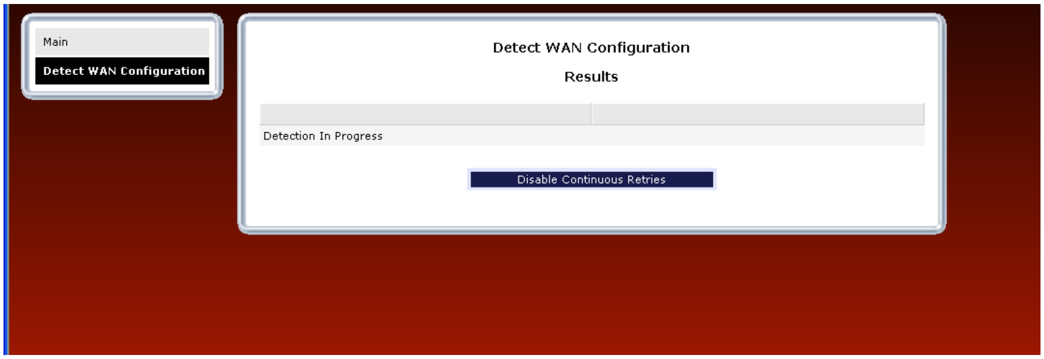
If you clicked **Enable Continuous Retries**, the following pop-up screen will appear. Click **OK** to continue.



Microsoft Internet Explorer

Do you want to enable continuous retries for the protocol detection?

If you clicked **OK**, the following screen will appear. If want to disable continuous retries, click **Disable Continuous Retries.**



Detect WAN Configuration

Results

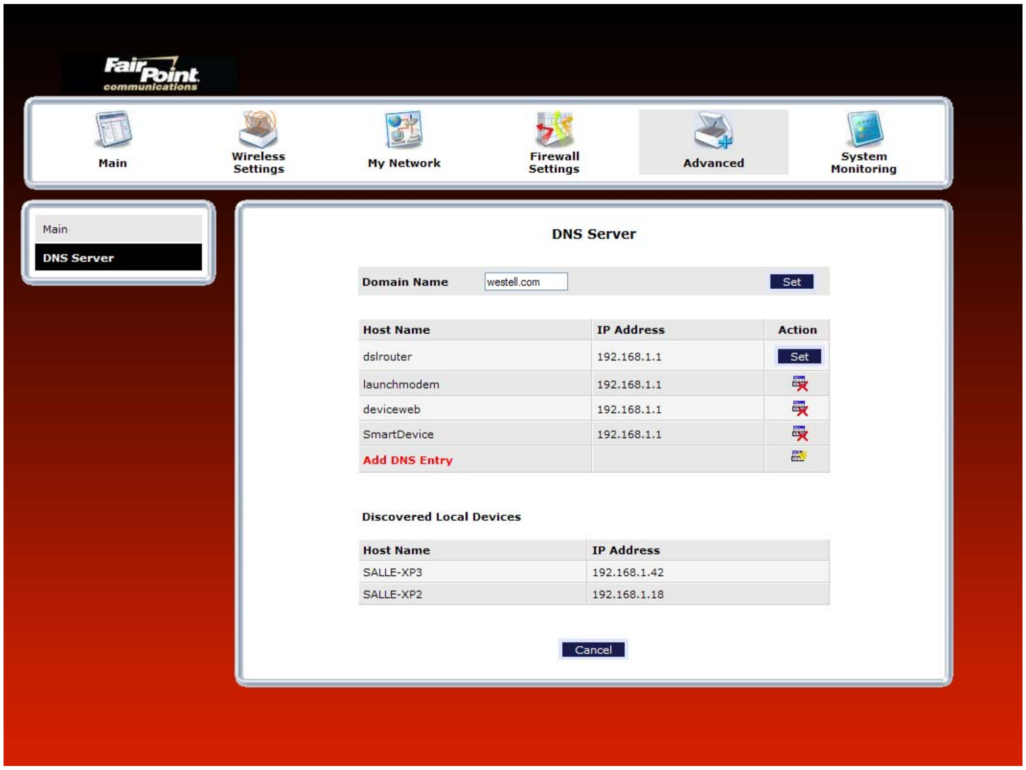
Detection In Progress

16.9 DNS Server

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

Do any of the following:

- To rename the Domain Name, type a domain in the **Domain Name** field and then click **Set**.
- To add a host name, click **Add DNS Entry**



DNS Server

Domain Name	westell.com	Set

Host Name	IP Address	Action
dslrouter	192.168.1.1	Set
launchmodem	192.168.1.1	✗
deviceweb	192.168.1.1	✗
SmartDevice	192.168.1.1	✗
Add DNS Entry		+

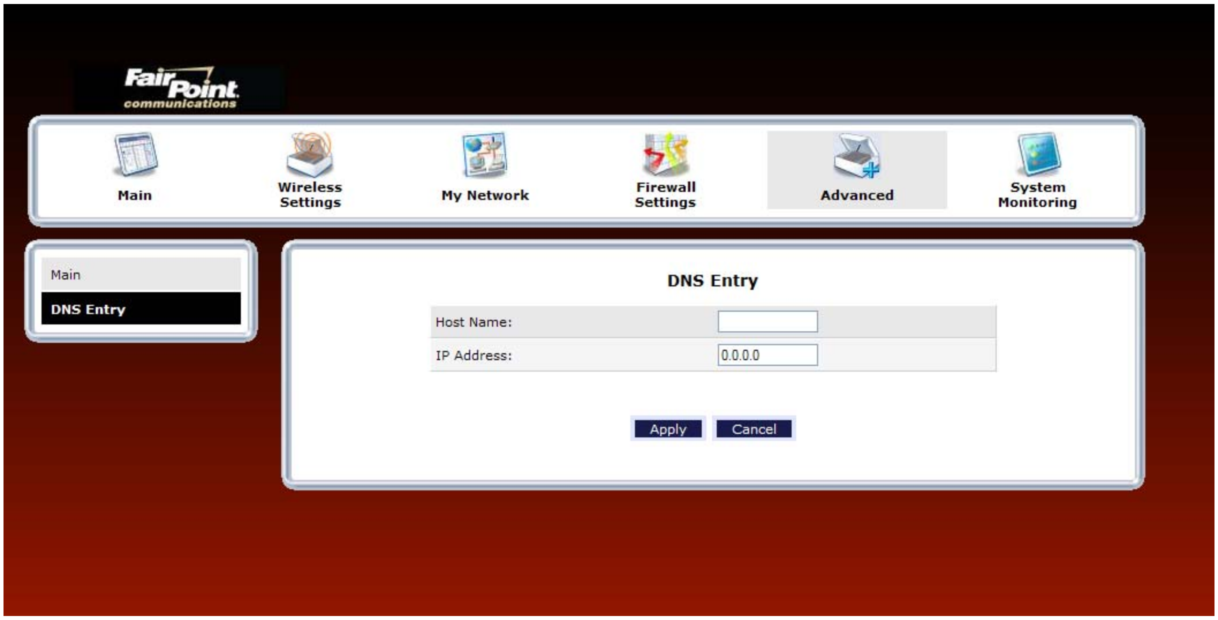
Discovered Local Devices

Host Name	IP Address
SALLE-XP3	192.168.1.42
SALLE-XP2	192.168.1.18

Cancel

Domain Name NOTE: Some ISP's may require the name for identification purposes.	This field allows you to enter a Domain Name for your Router To add a Domain Name, in the field under User Assigned DNS, type in your new domain name and click **Set.**
Host Name	This field allows you to enter a HOST name for Router. To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the IP address and click **Set.**
IP Address	Displays the IP address that is assigned to the Host Name.
Discover Local Devices	
This field displays a list of the computers on the LAN that were assigned a DHCP Address. The DNS name and IP address entry of each discovered device is displayed. (The values in this field will be displayed barring any propagation delays. If 'No Discovered Devices' is displayed, manually refresh the screen.)	

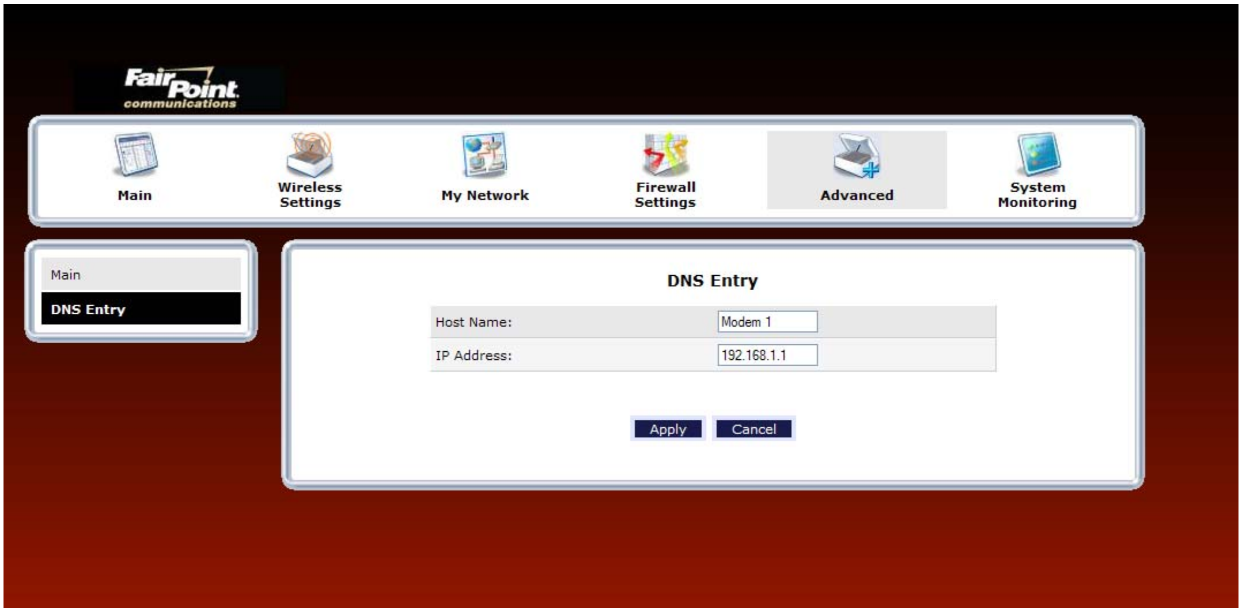
If you clicked **ADD DNS Entry**, the following screen will appear. Type the **Host Name** and **IP Address** in the fields provided. Then, click **Apply** to continue.



DNS Entry

Host Name:	
IP Address:	0.0.0.0

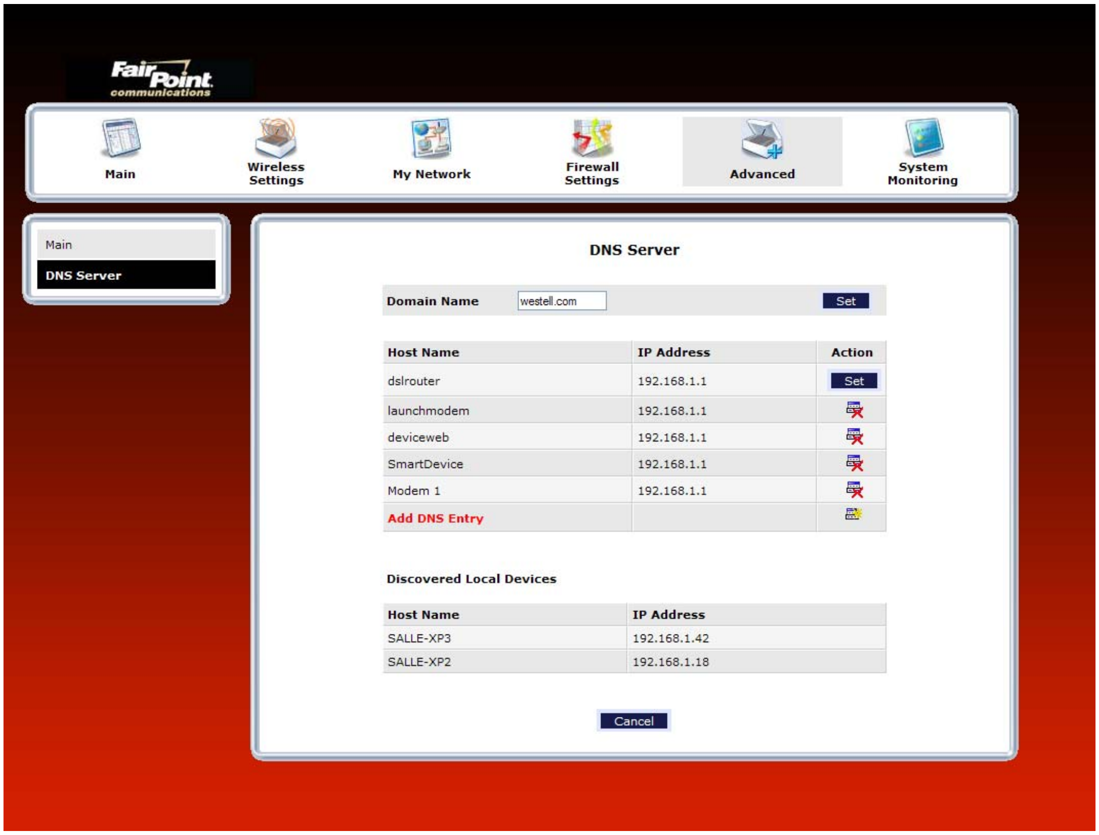
For example, the following screen shows DNS values in the fields. Click **Apply**.



DNS Entry

Host Name:	Modem 1
IP Address:	192.168.1.1

If you clicked **Apply**, the following screen will be displayed. This screen shows that the **Host Name** and **IP Address** have been added to the DNS server. If you want to delete a DNS entry, click the delete icon ✗ next to the Host Name and IP address that you want to delete.



DNS Server

Domain Name	westell.com	Set

Host Name	IP Address	Action
dslrouter	192.168.1.1	Set
launchmodem	192.168.1.1	✗
deviceweb	192.168.1.1	✗
SmartDevice	192.168.1.1	✗
Modem 1	192.168.1.1	✗
Add DNS Entry		

Discovered Local Devices

Host Name	IP Address
SALLE-XP3	192.168.1.42
SALLE-XP2	192.168.1.18

Cancel

16.10 Configuration File

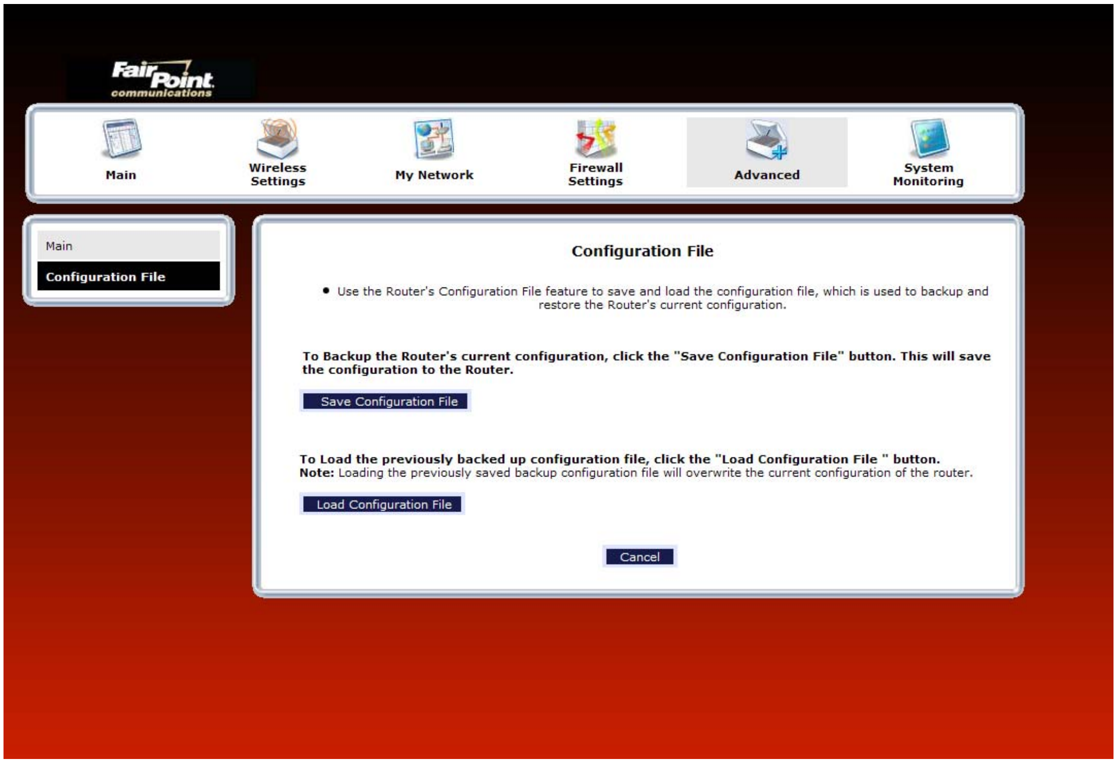
In the **Advanced** screen, click **Configuration File.** This screen allows you to save and load configuration files, which are used to back up and restore the Router's current configuration.

NOTE: Backup settings are stored in a separate area of flash, not to an external backup source.

Do one of the following:

- Click **Save Configuration File** to back up the Router's current configuration.
- Click **Load Configuration File** to load a previously backed up configuration file.

IMPORTANT: Loading a previously backed up configuration file will overwrite the Router's current configuration, and any data the Router has reported will be lost.



Configuration File

- Use the Router's Configuration File feature to save and load the configuration file, which is used to backup and restore the Router's current configuration.

To Backup the Router's current configuration, click the "Save Configuration File" button. This will save the configuration to the Router.

To Load the previously backed up configuration file, click the "Load Configuration File " button.
Note: Loading the previously saved backup configuration file will overwrite the current configuration of the router.

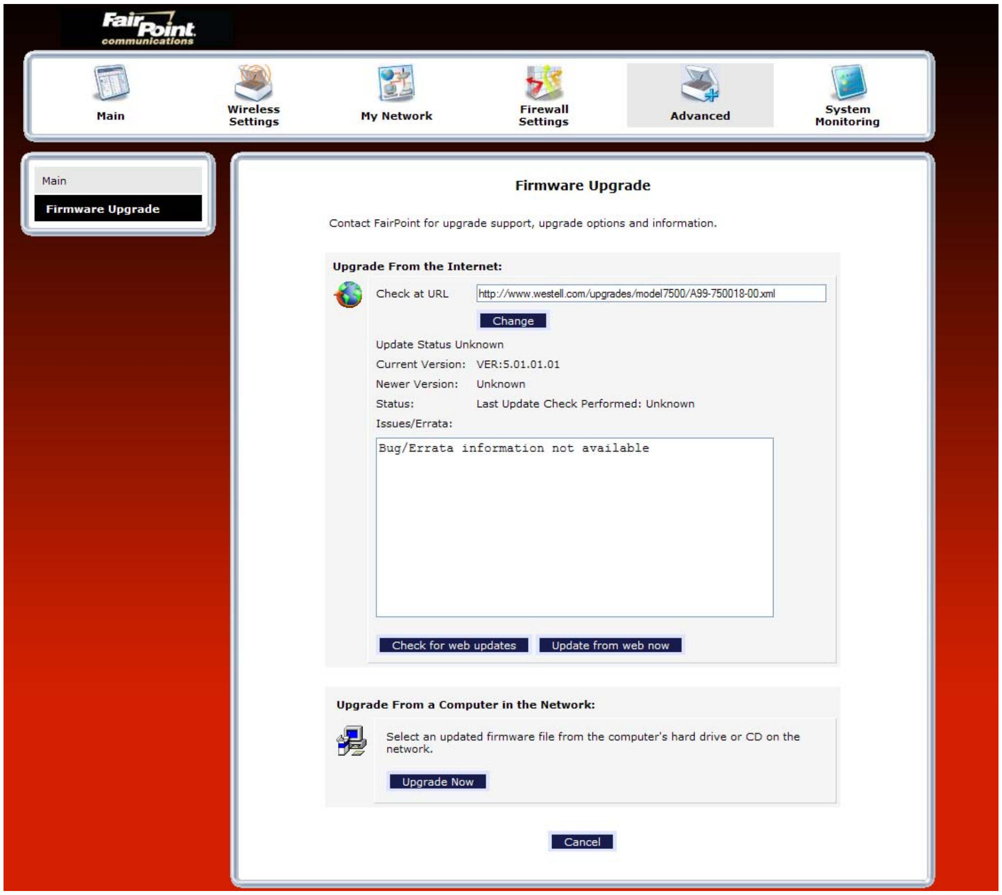
16.11 Firmware Upgrade

In the **Advanced** screen, click **Firmware Upgrade.** This screen is used to update the firmware that controls the operation of your Router. The updated firmware may be loaded from a CD-ROM, from a file stored on a local hard drive within your network, or from an update file stored on an Internet server.

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

Do any of the following:

- Click **change** to edit the path of the firmware update file. The path will appear in the **Check at URL** field.
- Click **check for web updates** to retrieve the firmware update file and display any available update information. You must be connected to the Internet to use this option. **NOTE:** If you click **check for web updates** and the page returns "bug information not available," this indicates that the firmware update file is not available.
- Click **update from web now** to download the firmware update file and to automatically update the Router firmware if an update is available and applicable. You must be connected to the Internet to use this option.
- Click **upgrade now** to retrieve the firmware update file from a local hard drive or CD-ROM on your Network. Internet connection is not required for this option.



Firmware Upgrade

Contact FairPoint for upgrade support, upgrade options and information.

Upgrade From the Internet:

Check at URL http://www.westell.com/upgrades/model7500/A99-750018-00.xml

Update Status Unknown

Current Version: VER:5.01.01.01

Newer Version: Unknown

Status: Last Update Check Performed: Unknown

Issues/Errata:

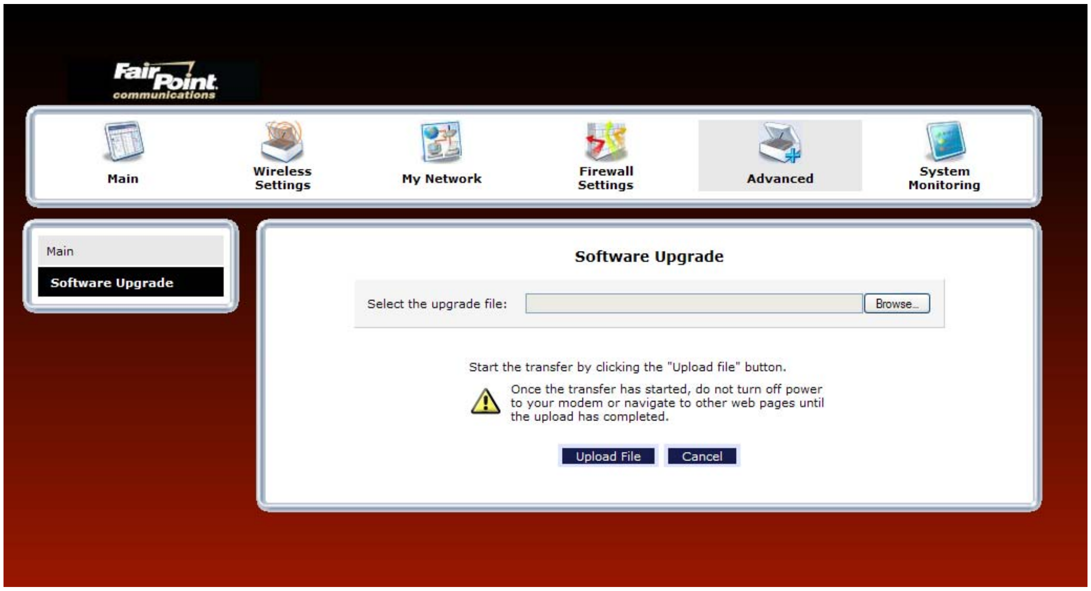
Bug/Errata information not available

Upgrade From a Computer in the Network:

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

If you clicked **Upgrade Now,** the following screen will appear.

IMPORTANT: Once the transfer has started, do not turn off your Router’s power, and do not navigate to other Web pages until the upload has completed.



Software Upgrade

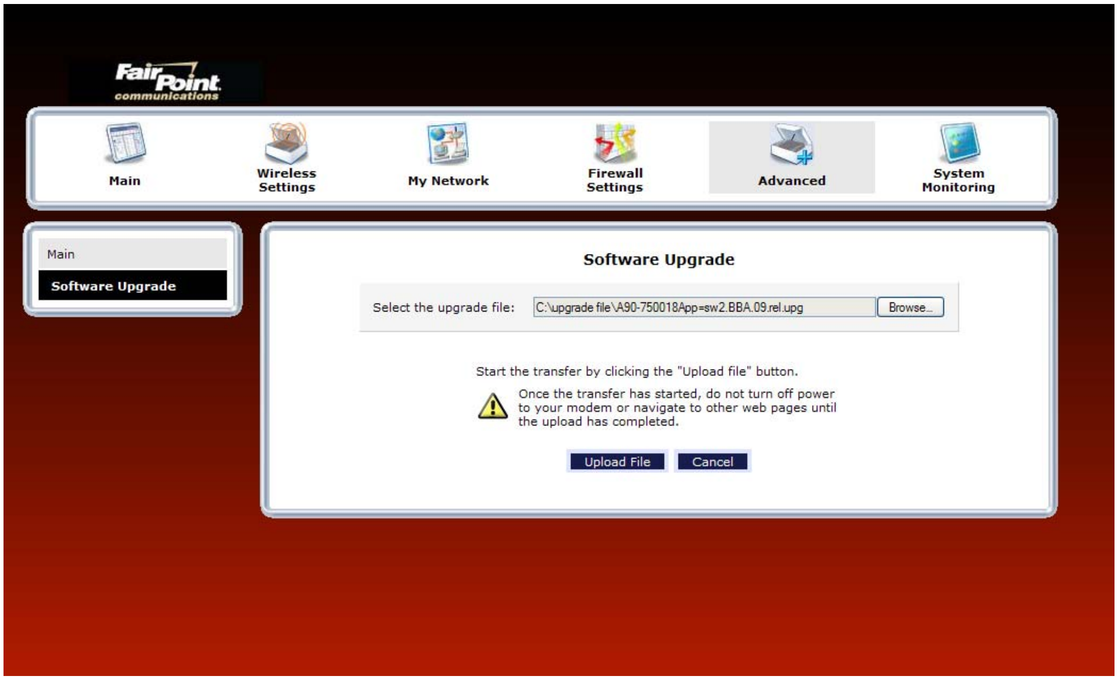
Select the upgrade file:

Start the transfer by clicking the "Upload file" button.

Once the transfer has started, do not turn off power to your modem or navigate to other web pages until the upload has completed.

Click **Browse** and then navigate to the location of the upgrade file; the path will appear in the window. Next, click **Upload file** to begin the upload to your Router.

IMPORTANT: Once the transfer has started, do not turn off your Router’s power, and do not navigate to other Web pages until the upload has completed.



Software Upgrade

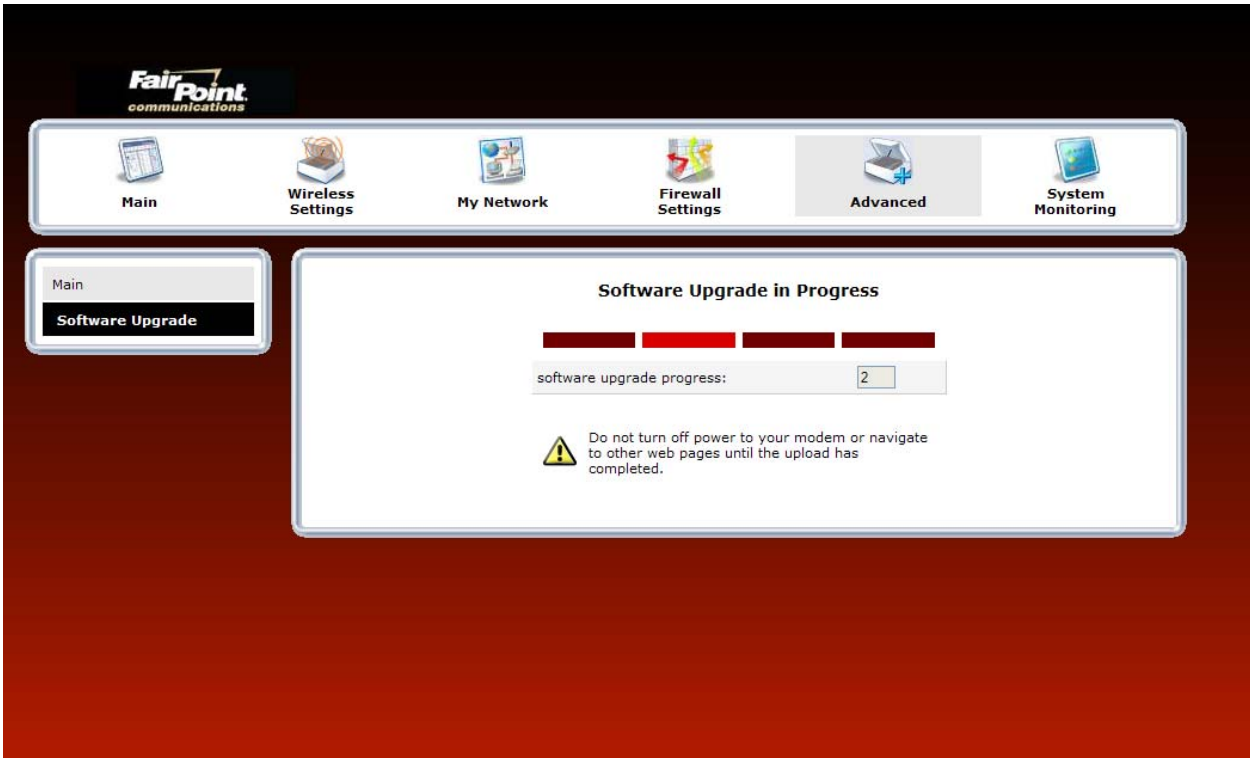
Select the upgrade file: C:\upgrade file\A90-750018App=sw2.BBA.09.rel.upg

Start the transfer by clicking the "Upload file" button.

Once the transfer has started, do not turn off power to your modem or navigate to other web pages until the upload has completed.

After the upload has completed, the following screen will appear. Please wait a brief moment while your Router is being reset.

IMPORTANT: Do not turn off power to your modem or navigate to other web pages until the upload has completed.



Software Upgrade in Progress

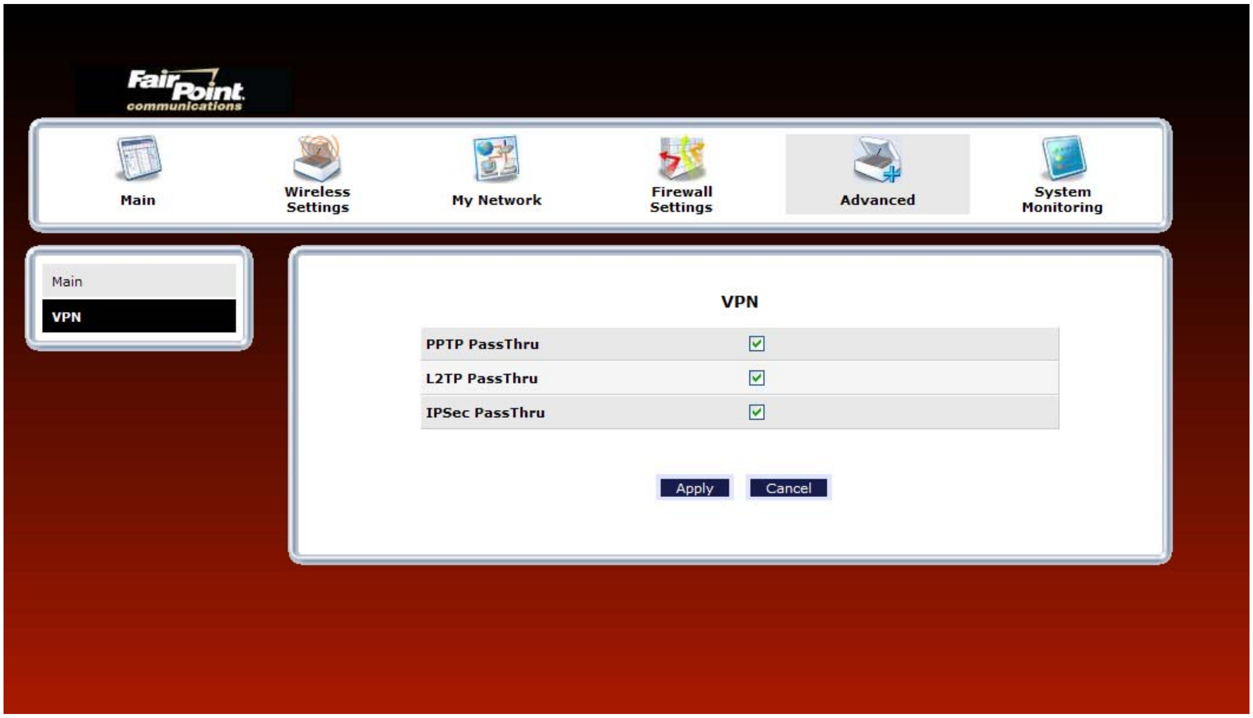
software upgrade progress: 2

Do not turn off power to your modem or navigate to other web pages until the upload has completed.

After the Router has been reset, the home page will appear. Confirm that you have a DSL link and that the PPP Status displays **UP.** (If necessary, click **Connect** to establish your PPP session.)

16.12 VPN

In the **Advanced** screen, click **VPN.** This feature allows you to select the VPN options for your Router.



VPN

PPTP PassThru	☑
L2TP PassThru	☑
IPSec PassThru	☑

VPN	
PPTP Passthrough	Factory Default = Enabled If enabled (a check mark will appear in the box), PPTP will work through the Gateway's NAT function.
L2TP Passthrough	Factory Default = Enabled If enabled, IPSec using ESP and L2TP can be supported via an ALG.
IPSec Passthrough	Factory Default = Enabled If enabled, IPSec using ESP can be supported via an ALG. IPSec using AH cannot be supported through NAT.

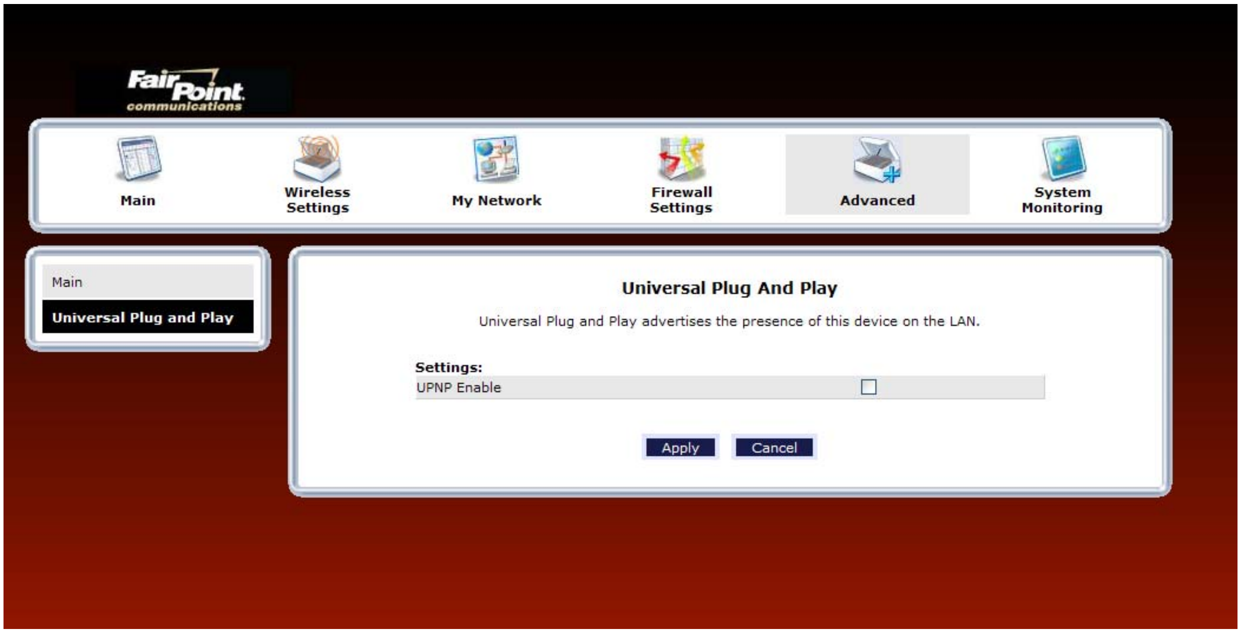
16.13 Universal Plug and Play

In the **Advanced** screen, click **Universal Plug and Play.** This feature advertises the presence of your Router on the LAN.

To enable UPnP in your Router, do the following:

1. Click the **UPNP Enable** box (a check mark will appear in the box).
2. Click **Apply** to allow the change to take effect.
3. Click **OK** in the pop-up screen to reset the Router.

NOTE: By factory default UPnP is disabled. If you have previously enabled UPNP and now want to disable it, click the **UPnP Enable** box to remove the check mark, and then click **Apply**.



Universal Plug And Play

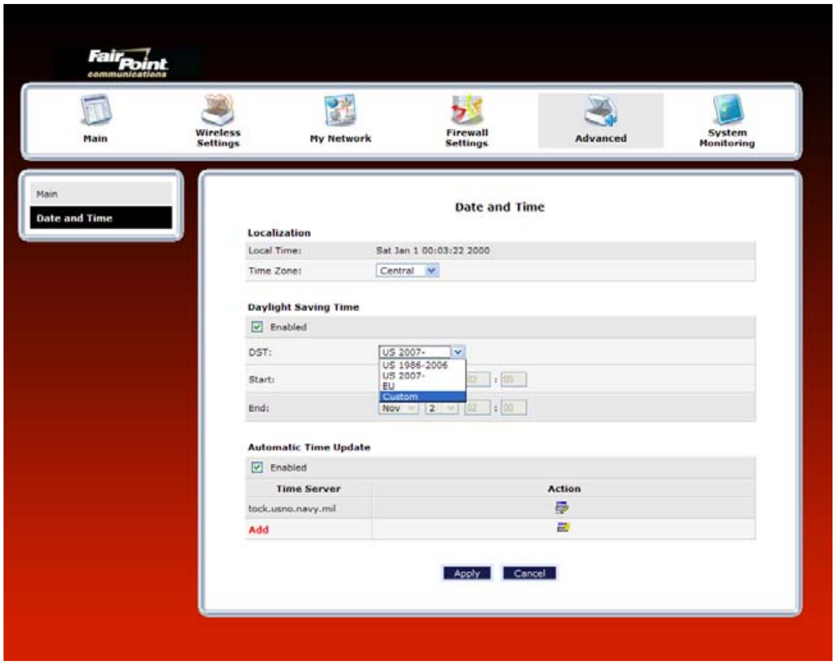
Universal Plug and Play advertises the presence of this device on the LAN.

Settings:

UPNP Enable □

16.14 Date and Time

In the **Advanced** screen, click **Date and Time.** This feature allows you to set the date and time values on your Router. Enter the desired settings, and then click **Apply**.



Date and Time

Localization

Local Time:	Sat Jan 1 00:03:22 2000
Time Zone:	Central

Daylight Saving Time

☑ Enabled

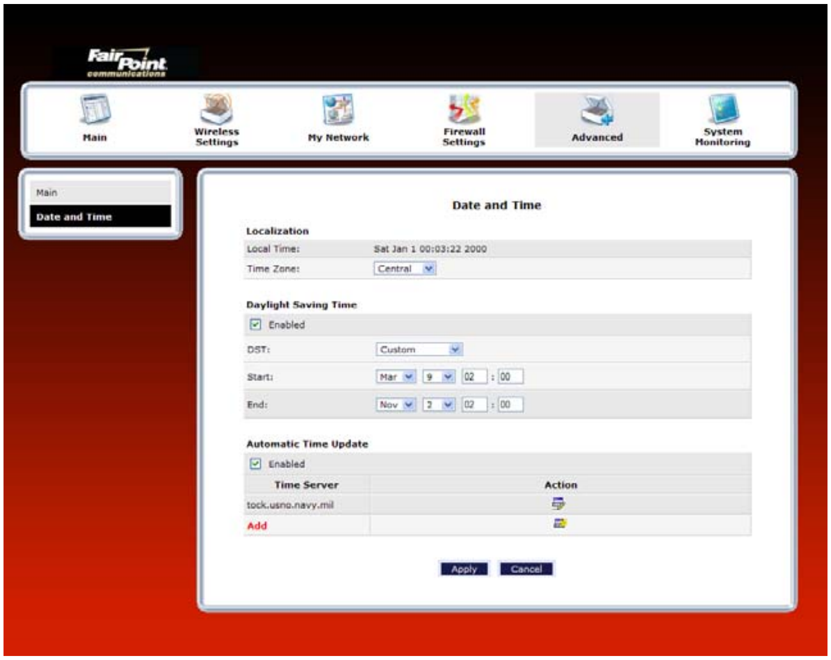
DST:	US 2007-
Start:	02 : 00
End:	Nov 2 02 : 00

Automatic Time Update

☑ Enabled

Time Server	Action
tock.usno.navy.mil	
Add	

For example, if you selected **Custom** from the **DST** drop-down menu, the following screen will appear. Place a check mark in the **Daylight Saving Time Enabled** check box, and then enter the desired Start and End values in the fields provided. Click **Apply** to save the settings.



Date and Time

Localization

Local Time:	Sat Jan 1 00:03:22 2000
Time Zone:	Central

Daylight Saving Time

☑ Enabled

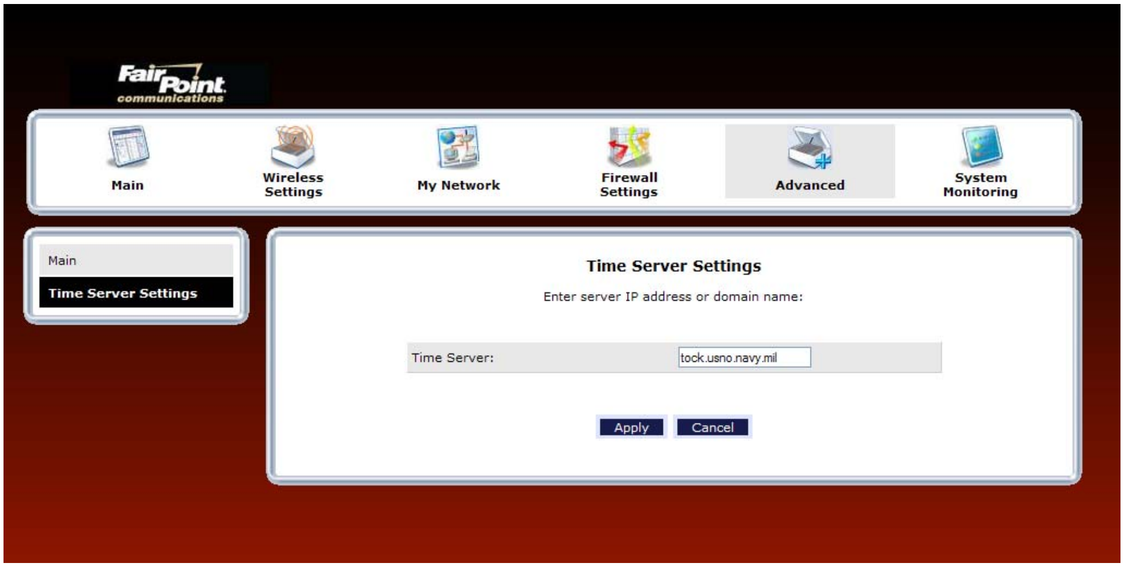
DST:	Custom
Start:	Mar 9 02 : 00
End:	Nov 2 02 : 00

Automatic Time Update

☑ Enabled

Time Server	Action
tock.usno.navy.mil	
Add	

To edit the time server settings, in the **Date and Time** screen, click the adjacent edit icon. The following screen will appear. Next, enter the IP address or domain name of the server you want to use. After you have entered the desired value, click **Apply** to save the settings.

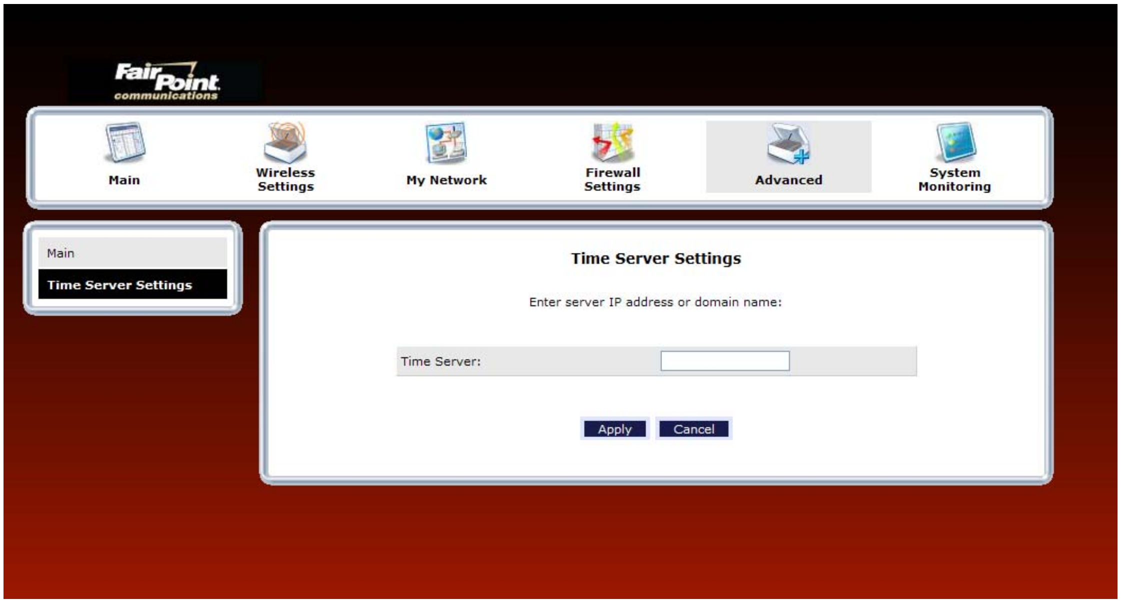


Time Server Settings

Enter server IP address or domain name:

Time Server: tock.usno.navy.mil

To add a time server entry, at the **Date and Time** screen, click **Add**. The following screen will appear. Next, enter the IP address or domain name of the server you want to use. After you have entered the desired value, click **Apply** to save the settings.



Time Server Settings

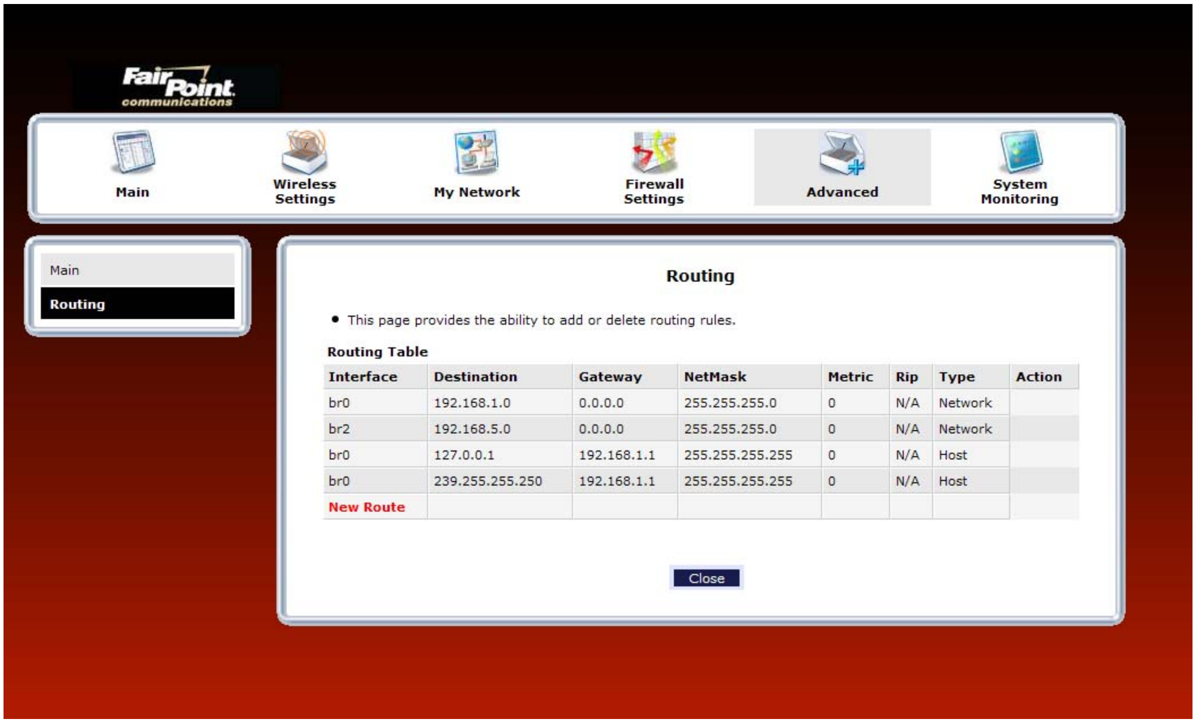
Enter server IP address or domain name:

Time Server:

16.15 Routing

In the **Advanced** screen, click **Routing**. The Routing table maintains the routes or paths of where specific types of data will be routed across a network.

To add a new static route in the Router, click **New Route.**



Routing

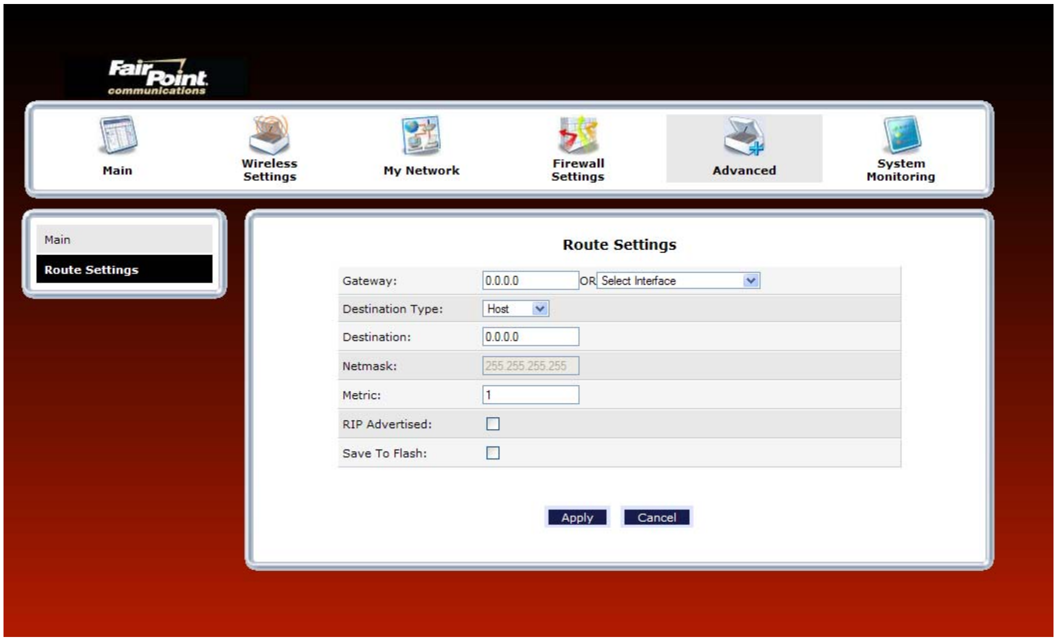
- This page provides the ability to add or delete routing rules.

Routing Table

Interface	Destination	Gateway	NetMask	Metric	Rip	Type	Action
br0	192.168.1.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br2	192.168.5.0	0.0.0.0	255.255.255.0	0	N/A	Network	
br0	127.0.0.1	192.168.1.1	255.255.255.255	0	N/A	Host	
br0	239.255.255.250	192.168.1.1	255.255.255.255	0	N/A	Host	
New Route							

Routing	
IP Interfaces	The list of active interfaces on the Router and their IP and Subnet mask address. br0 is the local LAN interface. ppp0 is the WAN interface
Destination	The IP address or subnet of the Route.
Gateway	Indicates were to send the packet if it matches this route.
Netmask	If the Route is a Network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box should be selected.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
Type	Indicates the type of route: Network route or Host route.

If you clicked **New Route,** the following screen will appear. Enter the appropriate values in the fields, and then click **Apply**.

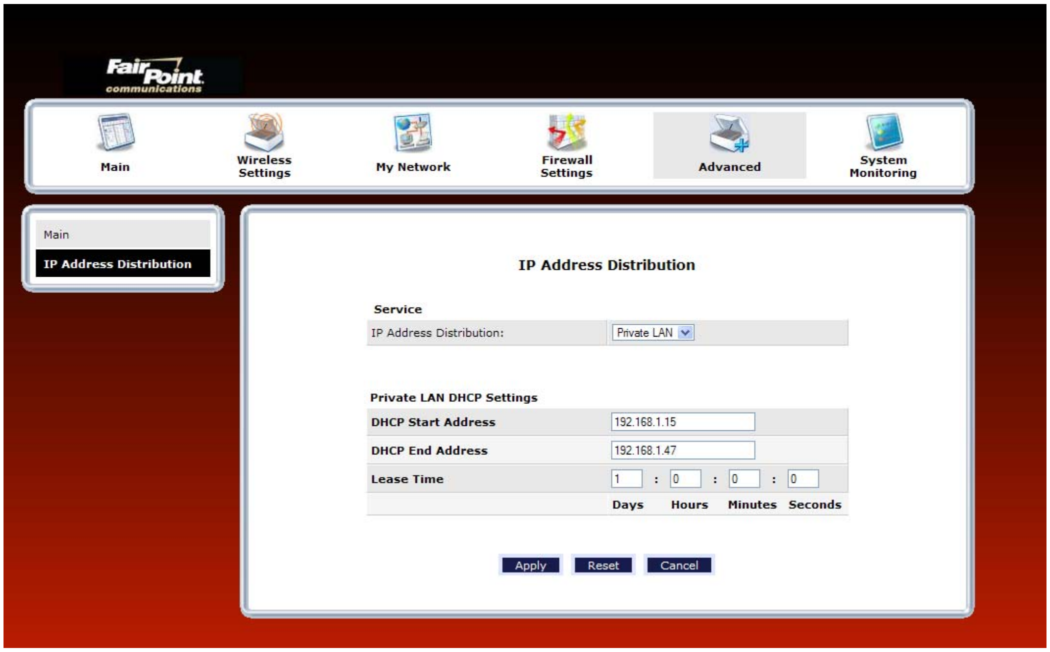


Route Settings

Gateway:	0.0.0.0 OR Select Interface
Destination Type:	Host
Destination:	0.0.0.0
Netmask:	255.255.255.255
Metric:	1
RIP Advertised:	□
Save To Flash:	□

16.16 IP Address Distribution

In the **Advanced** screen, click **IP Address Distribution.** The following screen will appear. IP Address Distribution allows you to configure the Router's DHCP server to automatically assign IP address to local devices connected to your LAN.



IP Address Distribution

Service

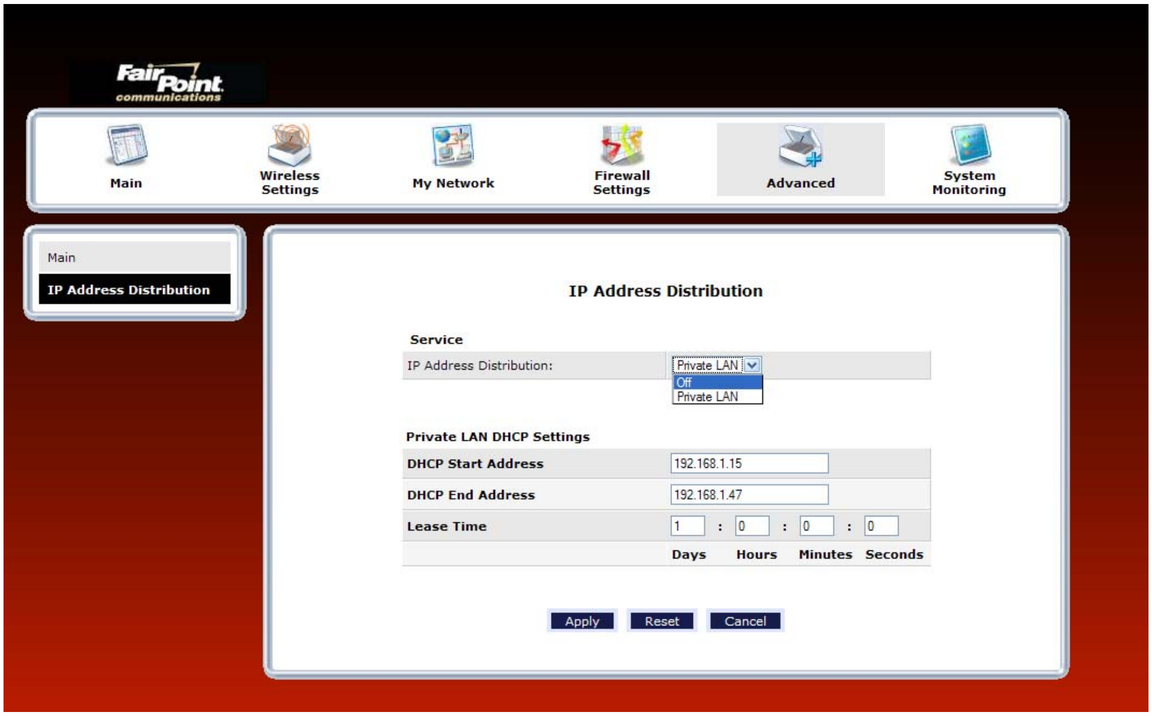
IP Address Distribution:	Private LAN

Private LAN DHCP Settings

DHCP Start Address	192.168.1.15			
DHCP End Address	192.168.1.47			
Lease Time	1 :	0 :	0 :	0
	Days	Hours	Minutes	Seconds

IP Address Distribution	
IP Address Distribution	Factory Default = Private LAN This setting allows VersaLink to automatically assign IP addresses to local devices connected to the LAN. Off = DHCP Server is disabled Private LAN = DHCP addresses will be issued from the Private LAN DHCP server.
Start IP Address	Factory Default = 192.168.1.15 This field displays the first IP address that the DHCP server will provide. The DHCP Start Address must be within the IP address and lower than the DHCP End Address. You can use any number from 0 to 254 in this address.
End IP Address	Factory Default = 192.168.1.47 This field displays the last IP address that the DHCP server will provide. The DHCP End Address must be within the IP address and higher than the DHCP Start Address. You can use any number from 0 to 254 in this address.
DHCP Lease Time	Factory Default = 01:00:00:00 Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually resubmit a request. Note: This value must be greater than 10 seconds. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.

By default Private LAN is already enabled. To disable the Private LAN DHCP server, select **Off** from the **IP Address Distribution** drop-down menu.



IP Address Distribution

Service

IP Address Distribution: Private LAN (Off / Private LAN)

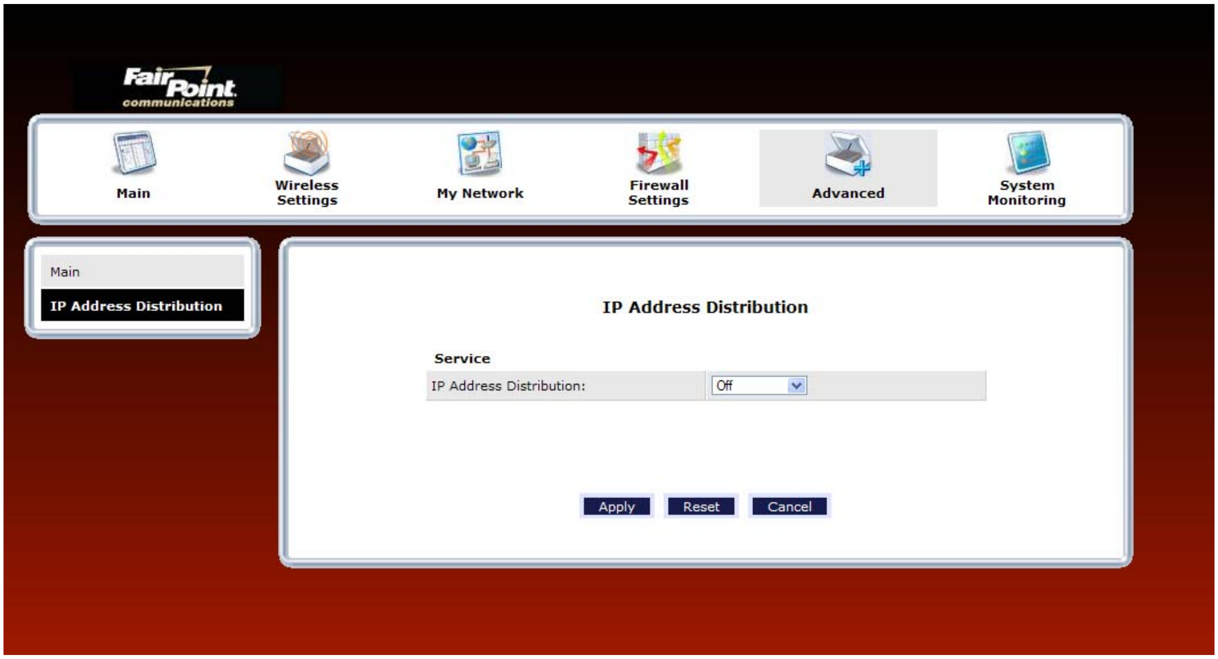
Private LAN DHCP Settings

DHCP Start Address	192.168.1.15
DHCP End Address	192.168.1.47
Lease Time	1 : 0 : 0 : 0 Days Hours Minutes Seconds

If you selected **Off**, the following screen will appear. Click **Apply** to save the settings. If you click **Reset**, the screen will refresh, and the previously saved settings will remain active.

IMPORTANT:

1. Whenever you change the settings in a screen, the screen will display the changes; however, you must click **Apply** to allow the changes to take effect in the Router. (**Private LAN** is the default for **DHCP Server.**)
2. After you disable the Private LAN DHCP server, reboot your computer to allow the changes to take effect.



IP Address Distribution

Service

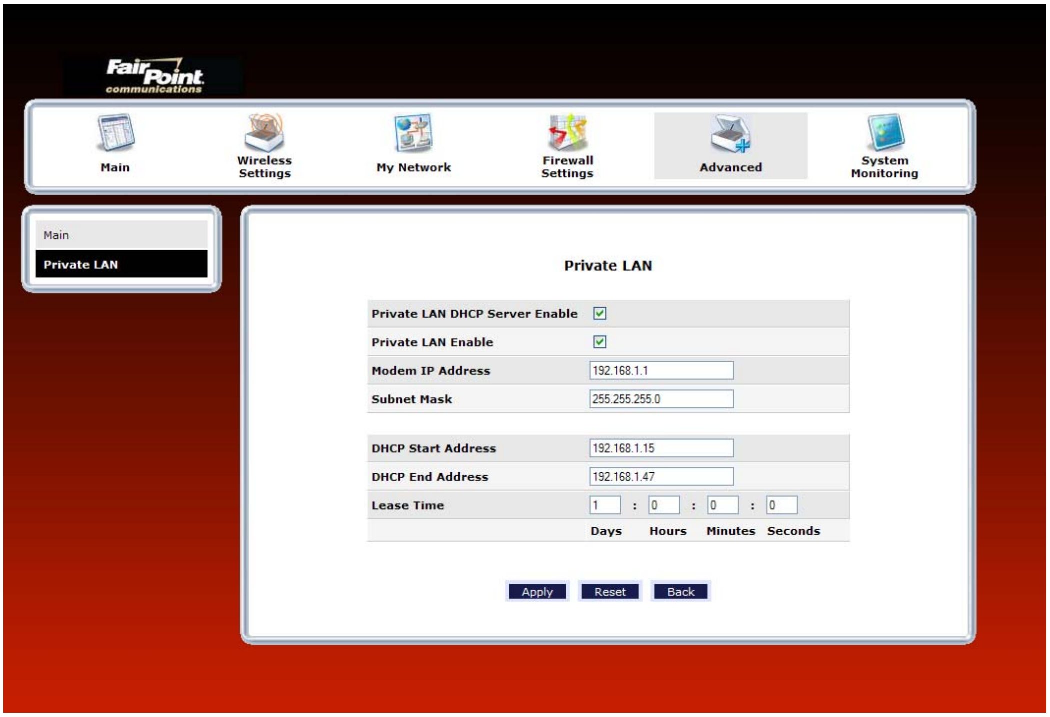
IP Address Distribution: Off

16.17 Private LAN—Configuring NAT

In the **Advanced** screen**,** click **Private LAN**. The following screen will appear. Private LAN allows you to set up a network behind your Router.

If you change the settings in this screen, click **Apply.** If you click **Reset**, the screen will refresh and the previously saved settings will remain active.

IMPORTANT: Whenever you change the settings in a screen, the screen will display the changes; however, you must click **Apply** to allow the changes to take effect in the Router. (**Private LAN** is the default setting for VersaLink.)



Private LAN

Private LAN DHCP Server Enable	☑
Private LAN Enable	☑
Modem IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Start Address	192.168.1.15
DHCP End Address	192.168.1.47
Lease Time	1 : 0 : 0 : 0 Days Hours Minutes Seconds

Private LAN	
Private LAN DHCP Server Enable	Default = Enabled If this box contains a check mark, this enables DHCP addresses to be served from the Private LAN pool.
Private LAN Enable	Default = Enabled If this box contains a check mark, this enables the addresses from the Private LAN to use the NAT interface.
Modem IP Address	Displays the Router's IP address.
Subnet Mask	Displays the Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host.
DHCP Start Address	Displays the first IP address that the DHCP server will provide.
DHCP End Address	Displays the last IP address that the DHCP server will provide.
DHCP Lease Time	Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually resubmit a request.
Note: The DHCP Lease Time value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.	

If the settings you have entered in the **Private LAN Configuration** screen are incorrect, the following warning messages may be displayed in pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

Warning Message	Check Private LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the **Seconds** value in the DHCP Lease Time field
Minutes must be between 0 and 59	Check the **Minutes** value in the DHCP Lease Time field
Hours must be between 0 and 23	Check the **Hours** value in the DHCP Lease Time field

16.18 Public LAN—Multiple IP Address Passthrough

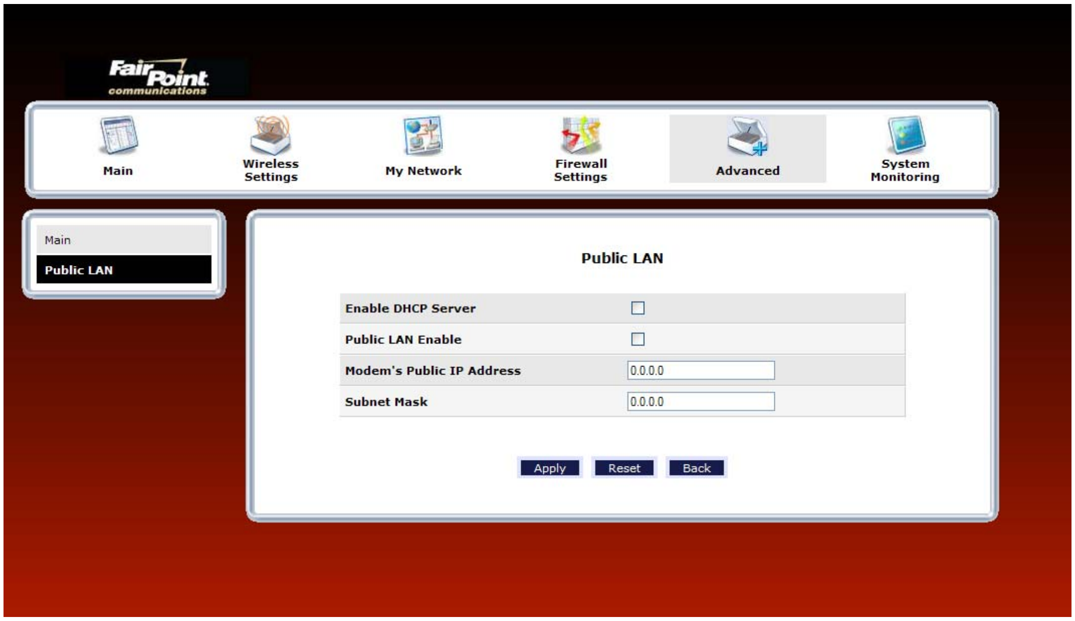
In the **Advanced** screen, click **Private LAN**. The following screen will appear. The Public LAN feature allows VersaLink to use LAN IP addresses that are accessible from the WAN. Public LAN allows your computer to have global address ability.

NOTE: To utilize the Public LAN feature in your VersaLink, must support Public LAN and Static IP. If you have questions about the feature, contact for details.

If you change the settings in this screen, click **Apply.** If you click **Reset**, the screen will refresh and the previously saved settings will remain active.

IMPORTANT: Whenever you change the Private LAN settings, the screen will display the changes; however, you must click **Apply** to allow the changes to take effect in the Router. (**Private LAN** is the default setting for VersaLink.)

To enable Public LAN, click the **Public LAN DHCP Server Enable** box (a check mark will appear in the box).



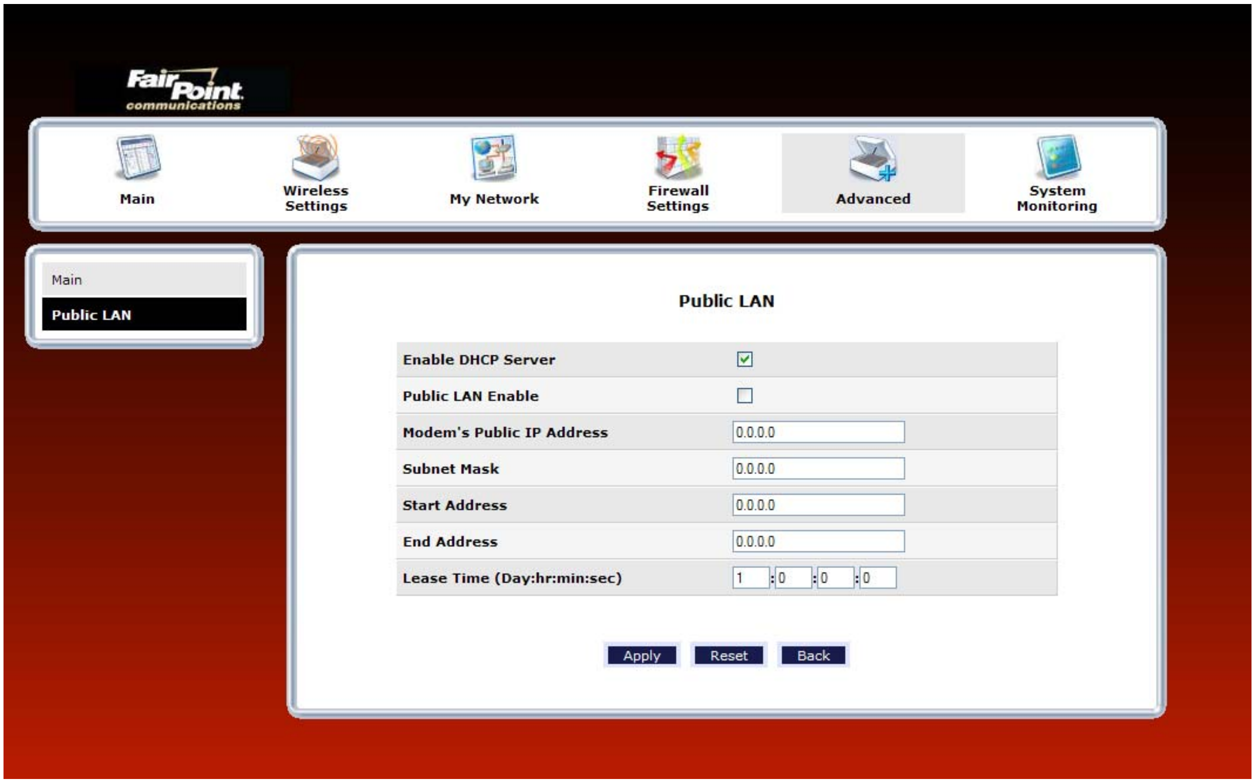
Public LAN

Enable DHCP Server	□
Public LAN Enable	□
Modem's Public IP Address	0.0.0.0
Subnet Mask	0.0.0.0

Public LAN	
Public LAN DHCP Server Enable	Default = Disabled (deselected) If this box contains a check mark, this enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = Disabled (deselected) If this box contains a check mark, this enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address	Provides a Public IP Address if the service provider does not automatically provide one.
Public LAN Subnet Mask	Provides a Public Subnet Mask if the service provider does not automatically provide one.

If you clicked the **Public LAN DHCP Server Enable** box, the following screen will appear. Click the **Public LAN Enable** box (a check mark will appear in the box).

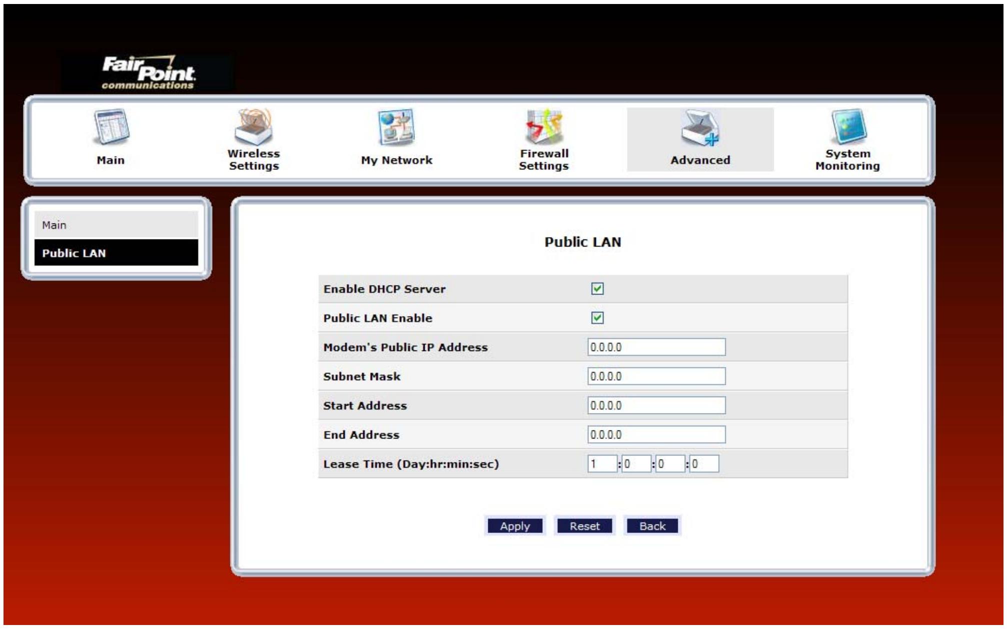
WARNING: By enabling the Public LAN DHCP Server, you automatically disable the Router's Private LAN DHCP Server. (**Private LAN DHCP** is the default setting for VersaLink.)



Public LAN

Enable DHCP Server	☑
Public LAN Enable	□
Modem's Public IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Start Address	0.0.0.0
End Address	0.0.0.0
Lease Time (Day:hr:min:sec)	1 : 0 : 0 : 0

If you clicked the **Public LAN Enable** box, the following screen will appear. After you have made changes to this screen, click **Apply** to allow the settings to take effect.



Public LAN

Enable DHCP Server	☑
Public LAN Enable	☑
Modem's Public IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Start Address	0.0.0.0
End Address	0.0.0.0
Lease Time (Day:hr:min:sec)	1 : 0 : 0 : 0

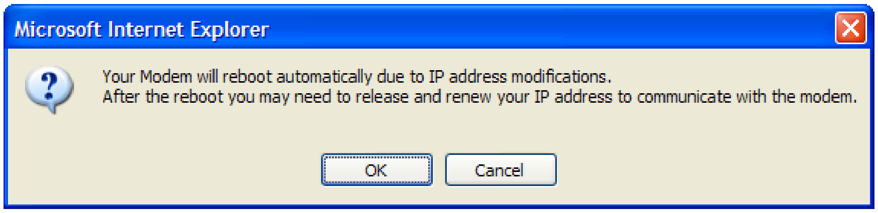
If the settings you have entered in the **Public LAN Configuration** screen are incorrect, the following warning messages may be appear in pop-up screens. If this occurs, check the **Public LAN Configuration** settings.

Warning Message	Check Public LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the **Seconds** field at DHCP Lease Time
Minutes must be between 0 and 59	Check the **Minutes** field at DHCP Lease Time
Hours must be between 0 and 23	Check the **Hours** field at DHCP Lease Time
Note: The DHCP Lease Time value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.	

If you clicked **Apply** in the **Public LAN** screen, a warning screen will display the following message:

> **Your Modem will reboot automatically due to IP address modifications.**
> **After the reboot, you may need to release and renew your IP address to communicate with the modem.**

Click **OK** to allow the modem to reboot. After the modem has rebooted, confirm that you have a DSL link and that your PPP Status displays **UP.**



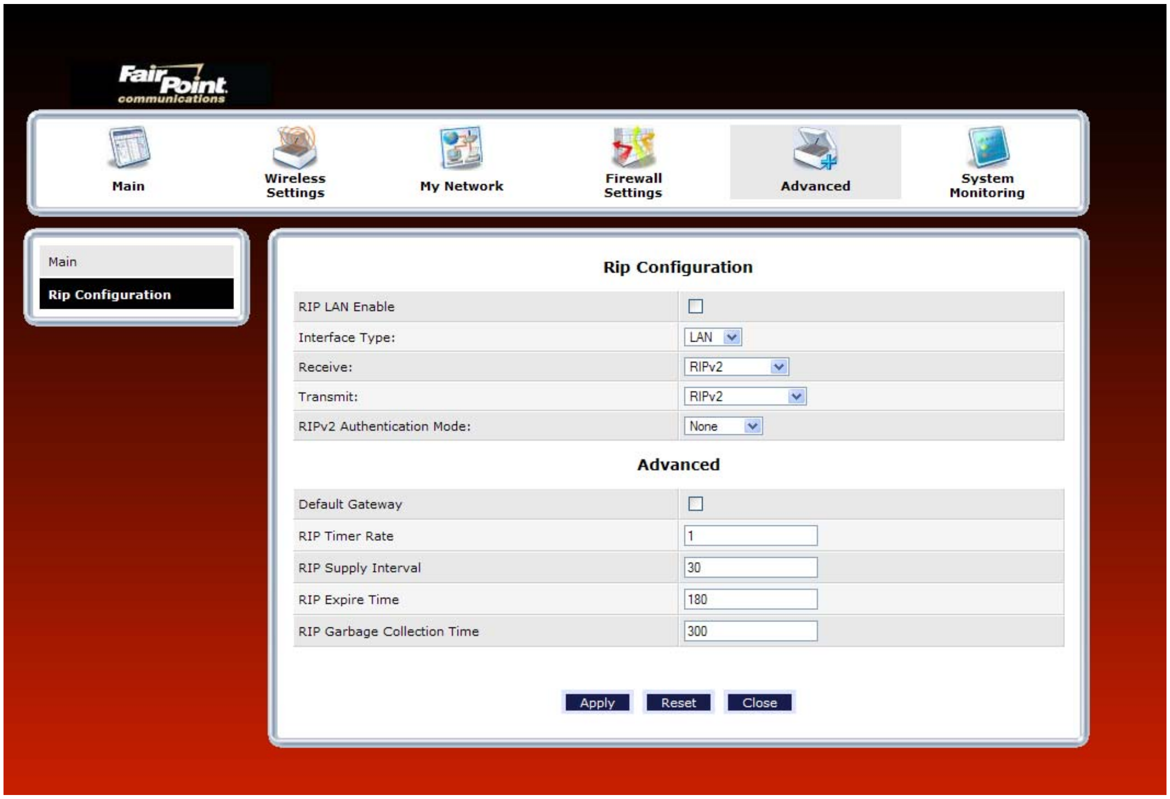
Your Modem will reboot automatically due to IP address modifications.
After the reboot you may need to release and renew your IP address to communicate with the modem.

16.19 RIP Configuration

In the **Advanced** screen, click **RIP Configuration**. The following screen will appear.

RIP (Routing Interface Protocol) is a dynamic inter-network routing protocol primarily used in interior routing environments. A dynamic routing protocol, as opposed to a static routing protocol, automatically discovers routes and builds routing tables.

If you change any settings in this screen, click **Save** to save the settings. If you click **Reset,** this screen will refresh and display the previously saved RIP settings.



Rip Configuration

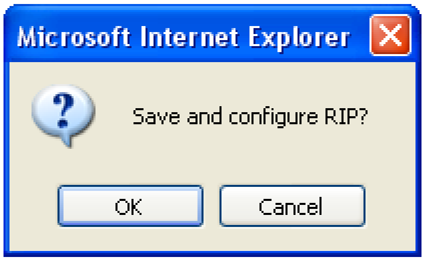
RIP LAN Enable	☐
Interface Type:	LAN
Receive:	RIPv2
Transmit:	RIPv2
RIPv2 Authentication Mode:	None

Advanced

Default Gateway	☐
RIP Timer Rate	1
RIP Supply Interval	30
RIP Expire Time	180
RIP Garbage Collection Time	300

RIP Configuration	
RIP Global Enable	Factory Default = Disabled If this box is checked, RIP will be Enabled (activated).
Interface Type	LAN: Select this if you are configuring RIP for the LAN side. WAN: Select this if you are configuring RIP for the WAN side. (WAN side is receive only.)
Receive	The version of RIP to be accepted. Possible Responses: None RIPv1 RIPv2 RIPv1 or RIPv2
Transmit	The version of RIP to be transmitted. (WAN side RIP never transmits) Possible Responses: None RIPv1 RIPv1 Compatible RIPv2
RIPv2 Authentication Mode	If using RIP V2, you must select the type of authentication to use. Possible Responses: None Clear Text MD5 (If MD5 authentication, the password)
Advanced	
Default Gateway	Factory Default = Disabled If this box is check (Enabled), this feature will determine whether the modem advertises itself as the default Gateway (i.e., the default route)
RIP Timer Rate	Indicates how often to update the local routing table.
RIP Supply Interval	Indicates how often to advertise routes to neighbors.
RIP Expire Time	Indicates how long routes received from neighbors become invalid, if no refresh of the route is received.
RIP Garbage Collection Time	Indicates how long to advertise invalid routes after they have expired.

After you have enabled RIP and clicked **Save**, the following pop-up screen will be displayed. Click **OK** to save and configure RIP.

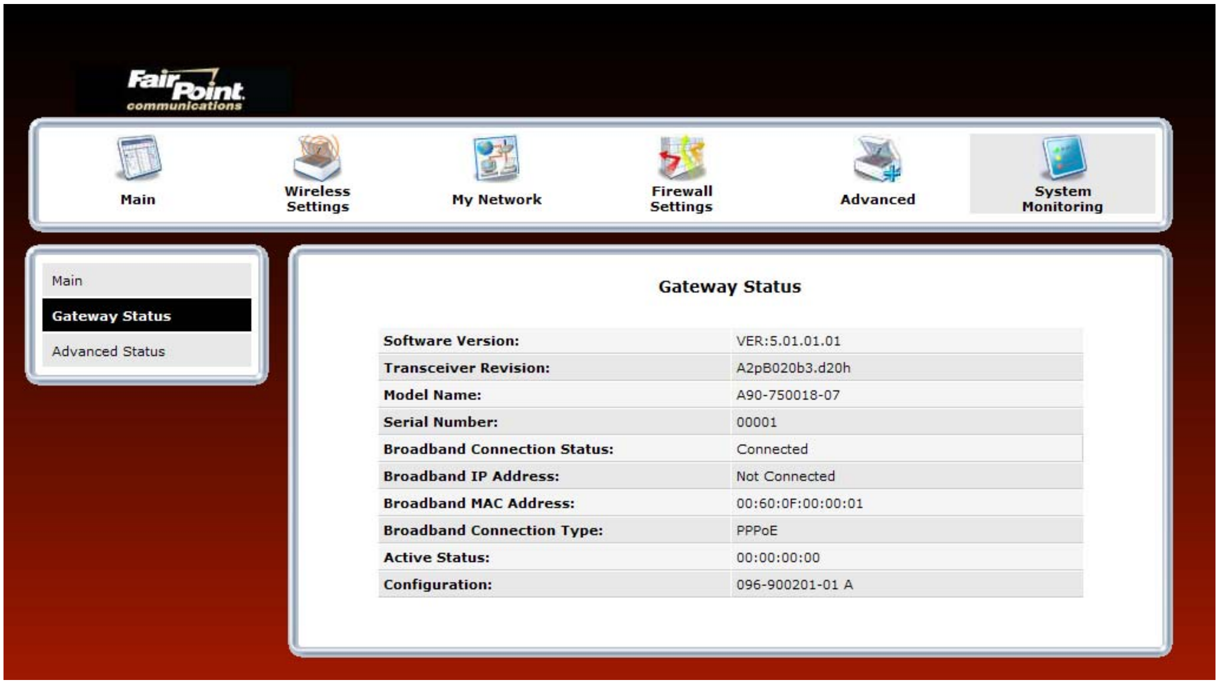


Save and configure RIP?

17. SYSTEM MONITORING

17.1 Gateway Status

If you clicked **Yes** in the warning screen, the following **Gateway Status** screen will appear. This screen allows you to view details about your Router.



Gateway Status

Software Version:	VER:5.01.01.01
Transceiver Revision:	A2pB020b3.d20h
Model Name:	A90-750018-07
Serial Number:	00001
Broadband Connection Status:	Connected
Broadband IP Address:	Not Connected
Broadband MAC Address:	00:60:0F:00:00:01
Broadband Connection Type:	PPPoE
Active Status:	00:00:00:00
Configuration:	096-900201-01 A

Gateway Status	
Software Version	VersaLink's software version.
Transceiver Revision	VersaLink's transceiver version.
Model Name	VersaLink manufacturer's model name.
Serial Number	VersaLink's serial number.

Broadband Connection Status	The status of your Internet connection.
	Up = Internet connection established
	Down = No Internet connection established

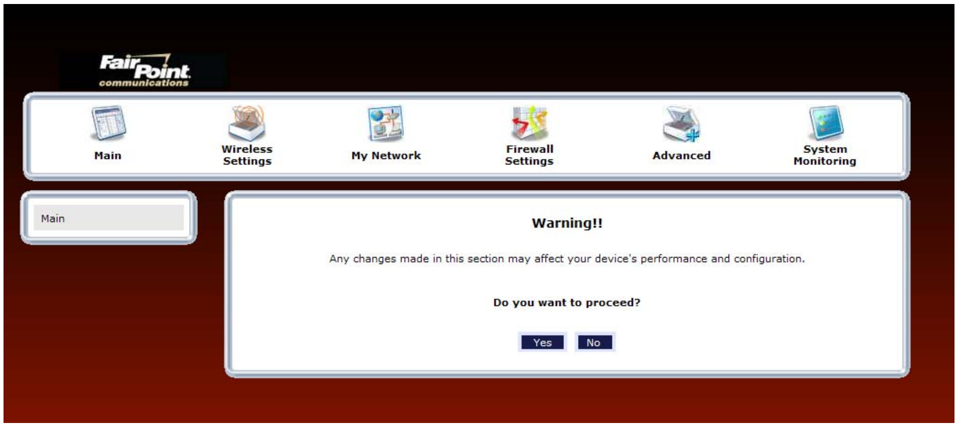
Broadband IP Address	VersaLink's WAN IP Address, assigned or provided by your Internet service provider.
Broadband MAC Address	Media Access Controller (MAC) i.e., hardware address of this device, assigned by the manufacturer.
Broadband Connection Type	The protocol used to establish an Internet connection with your Internet service provider.
Active Status	The duration that VersaLink has been in use (measured in hours: minutes: seconds).
Configuration	Proprietary configuration number for VersaLink.

17.2 Advanced Status

If you select **System Monitoring** in the top navigational menu, and then click **Advanced Status** in the menu options at the left of the screen, a warning screen will display the following message:

> **Any changes made in this section may affect your device's performance and configuration.**
> **Do you want to proceed?**

Click **Yes** to proceed.



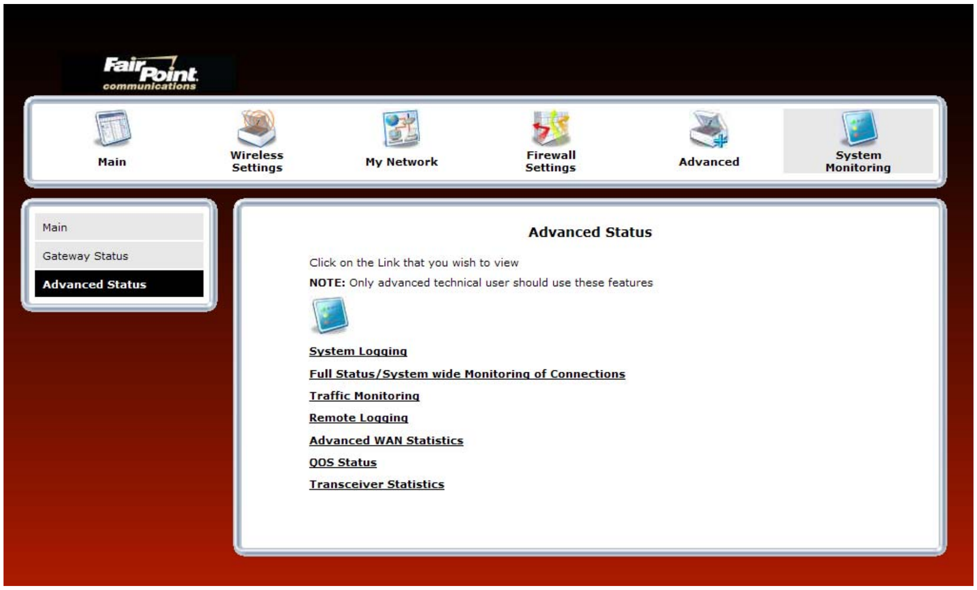
Warning!!

Any changes made in this section may affect your device's performance and configuration.

Do you want to proceed?

If you clicked **Yes**, in the **Warning** screen, the following screen will appear. From this screen, you can access various logging and monitoring information recorded by your Router. Click the desired link to go to that screen.

NOTE: Only advanced users should use these features. If you need to reset the Router to factory default settings, press the reset button on the rear of the Router. Or follow the instructions in section 16.2, "Restore Defaults," to restore the Router to factory default settings.



Advanced Status

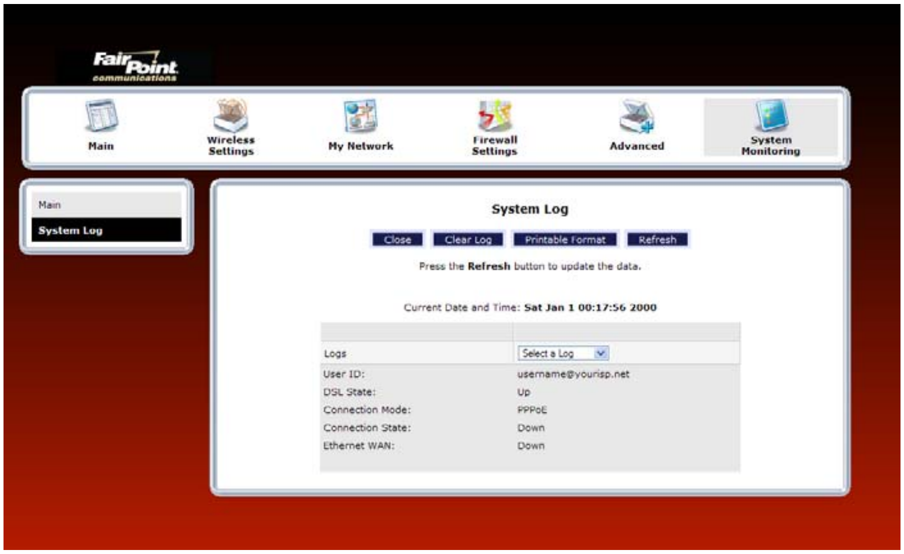
Click on the Link that you wish to view

NOTE: Only advanced technical user should use these features

System Logging
Full Status/System wide Monitoring of Connections
Traffic Monitoring
Remote Logging
Advanced WAN Statistics
QOS Status
Transceiver Statistics

17.2.1 System Logging

In the **Advanced Status** screen, click **System Logging**. The following screen will be displayed.



System Log

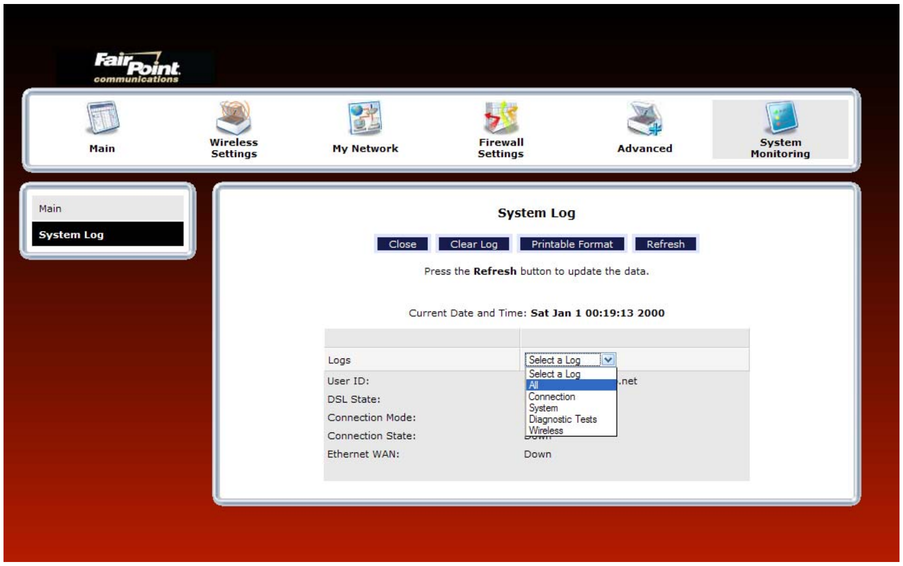
Press the **Refresh** button to update the data.

Current Date and Time: **Sat Jan 1 00:17:56 2000**

Logs	Select a Log
User ID:	username@yourisp.net
DSL State:	Up
Connection Mode:	PPPoE
Connection State:	Down
Ethernet WAN:	Down

At the **Logs** drop-down menu, do any of the following:

- Select **All** to list both Connection and System logs.
- Select **Connection** to list all events related to connection activity (any traffic on the USB, Ethernet, or DSL ports).
- Select **System** to list all events related to system activity (Time, Errors, Boot Information, etc.)
- Select **Diagnostic Tests** to list all events related to the diagnostic logs
- Select **Wireless** to list all events related to the voice event logs



System Log

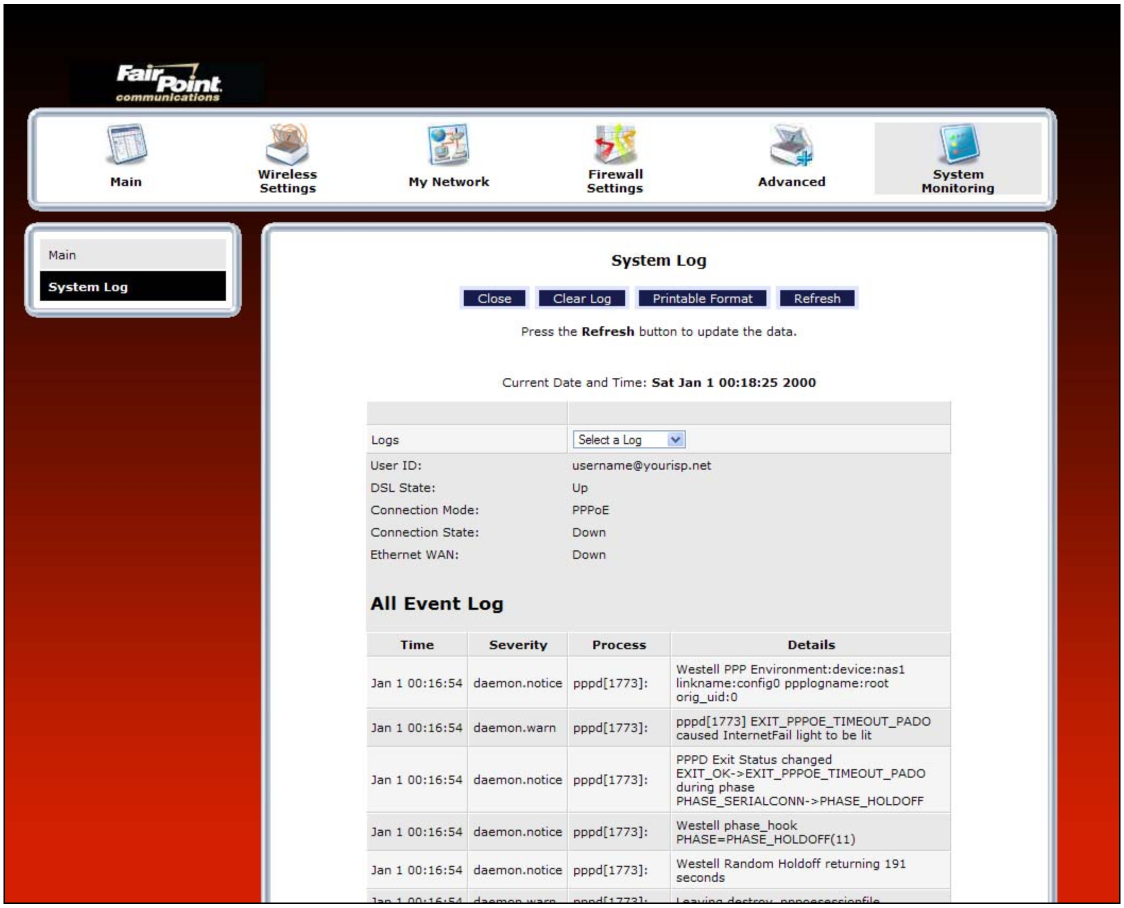
Press the **Refresh** button to update the data.

Current Date and Time: **Sat Jan 1 00:19:13 2000**

Logs	Select a Log
User ID:	.net
DSL State:	
Connection Mode:	
Connection State:	Down
Ethernet WAN:	Down

If you selected **All** from the **Logs** drop-down menu, the following screen will appear. You may need to scroll down to the bottom of the logs screen to view all the logged events. After you have viewed the logs, do any of the following:

- Click **Close** to close the logs page and to return to the Advanced Status screen.
- Click **Clear Log** to clear the logs screen.
- Click **Printable Format** to save a copy of the logs to a location on your computer.
- Click **Refresh** to update the logs screen so that it displays the most current information.



System Log

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

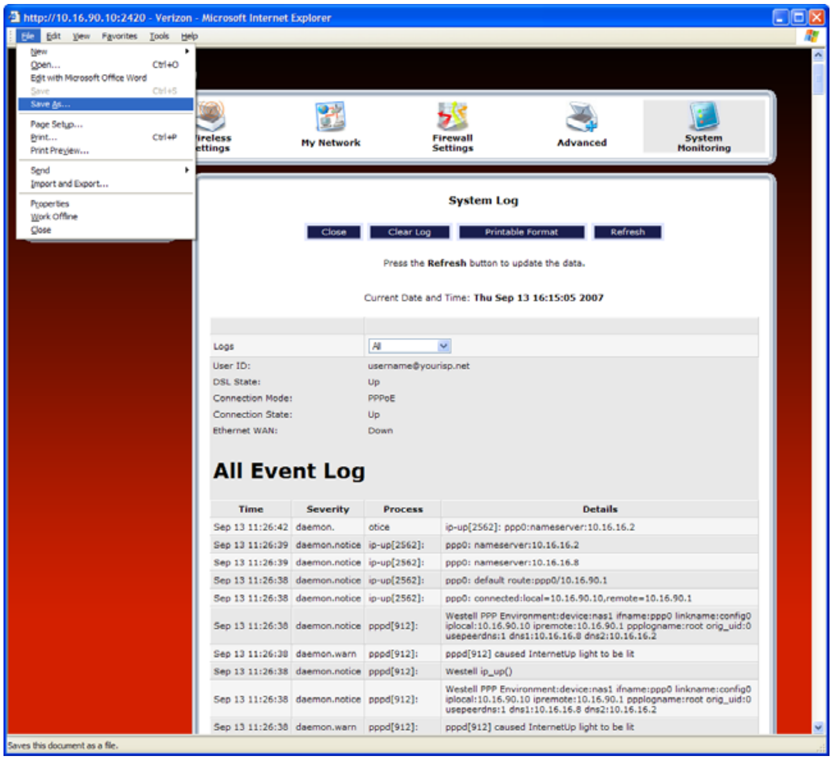
Current Date and Time: **Sat Jan 1 00:18:25 2000**

Logs	Select a Log
User ID:	username@yourisp.net
DSL State:	Up
Connection Mode:	PPPoE
Connection State:	Down
Ethernet WAN:	Down

All Event Log

Time	Severity	Process	Details
Jan 1 00:16:54	daemon.notice	pppd[1773]:	Westell PPP Environment:device:nas1 linkname:config0 ppplogname:root orig_uid:0
Jan 1 00:16:54	daemon.warn	pppd[1773]:	pppd[1773] EXIT_PPPOE_TIMEOUT_PADO caused InternetFail light to be lit
Jan 1 00:16:54	daemon.notice	pppd[1773]:	PPPD Exit Status changed EXIT_OK->EXIT_PPPOE_TIMEOUT_PADO during phase PHASE_SERIALCONN->PHASE_HOLDOFF
Jan 1 00:16:54	daemon.notice	pppd[1773]:	Westell phase_hook PHASE=PHASE_HOLDOFF(11)
Jan 1 00:16:54	daemon.notice	pppd[1773]:	Westell Random Holdoff returning 191 seconds
Jan 1 00:16:54	daemon.warn	pppd[1773]:	Leaving destroy_pppoesessionfile

To save a copy of the logs to a location on your computer, in the **System Log** page, click **Printable Format.** The following screen will appear. From the **File** menu, select the “Save As” option to save the file to the desired location.



System Log

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

Current Date and Time: **Thu Sep 13 16:15:05 2007**

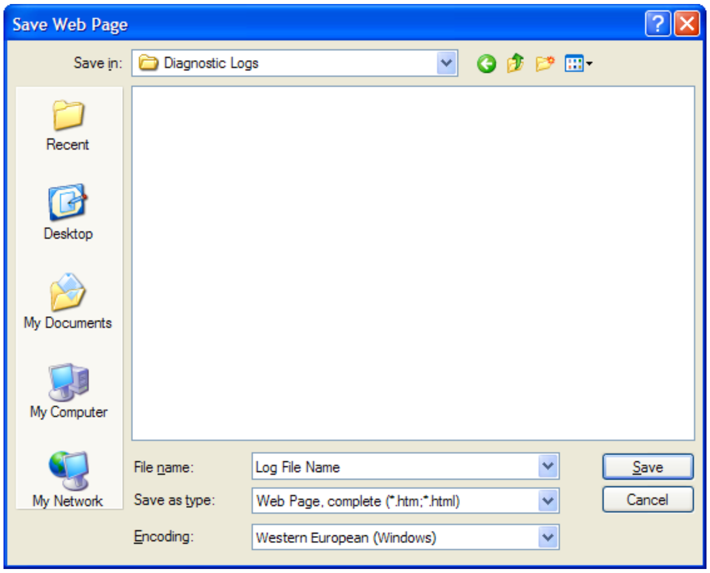
Logs: All

User ID:	username@yourisp.net
DSL State:	Up
Connection Mode:	PPPoE
Connection State:	Up
Ethernet WAN:	Down

All Event Log

Time	Severity	Process	Details
Sep 13 11:26:42	daemon.	otice	ip-up[2562]: ppp0:nameserver:10.16.16.2
Sep 13 11:26:39	daemon.notice	ip-up[2562]:	ppp0: nameserver:10.16.16.2
Sep 13 11:26:39	daemon.notice	ip-up[2562]:	ppp0: nameserver:10.16.16.8
Sep 13 11:26:38	daemon.notice	ip-up[2562]:	ppp0: default route:ppp0/10.16.90.1
Sep 13 11:26:38	daemon.notice	ip-up[2562]:	ppp0: connected:local=10.16.90.10,remote=10.16.90.1
Sep 13 11:26:38	daemon.notice	pppd[912]:	Westell PPP Environment:device:nas1 ifname:ppp0 linkname:config0 iplocal:10.16.90.10 ipremote:10.16.90.1 pppIogname:root orig_uid:0 usepeerdns:1 dns1:10.16.16.8 dns2:10.16.16.2
Sep 13 11:26:38	daemon.warn	pppd[912]:	pppd[912] caused InternetUp light to be lit
Sep 13 11:26:38	daemon.notice	pppd[912]:	Westell ip_up()
Sep 13 11:26:38	daemon.notice	pppd[912]:	Westell PPP Environment:device:nas1 ifname:ppp0 linkname:config0 iplocal:10.16.90.10 ipremote:10.16.90.1 pppIogname:root orig_uid:0 usepeerdns:1 dns1:10.16.16.8 dns2:10.16.16.2
Sep 13 11:26:38	daemon.warn	pppd[912]:	pppd[912] caused InternetUp light to be lit

At the **Save Web Page** dialog box, select a destination for your log file from the **Save in** drop-down menu. Next, enter a name for your log file in the field labeled **File name,** and then click **Save** to save the log file.



Save in: Diagnostic Logs

File name: Log File Name

Save as type: Web Page, complete (*.htm;*.html)

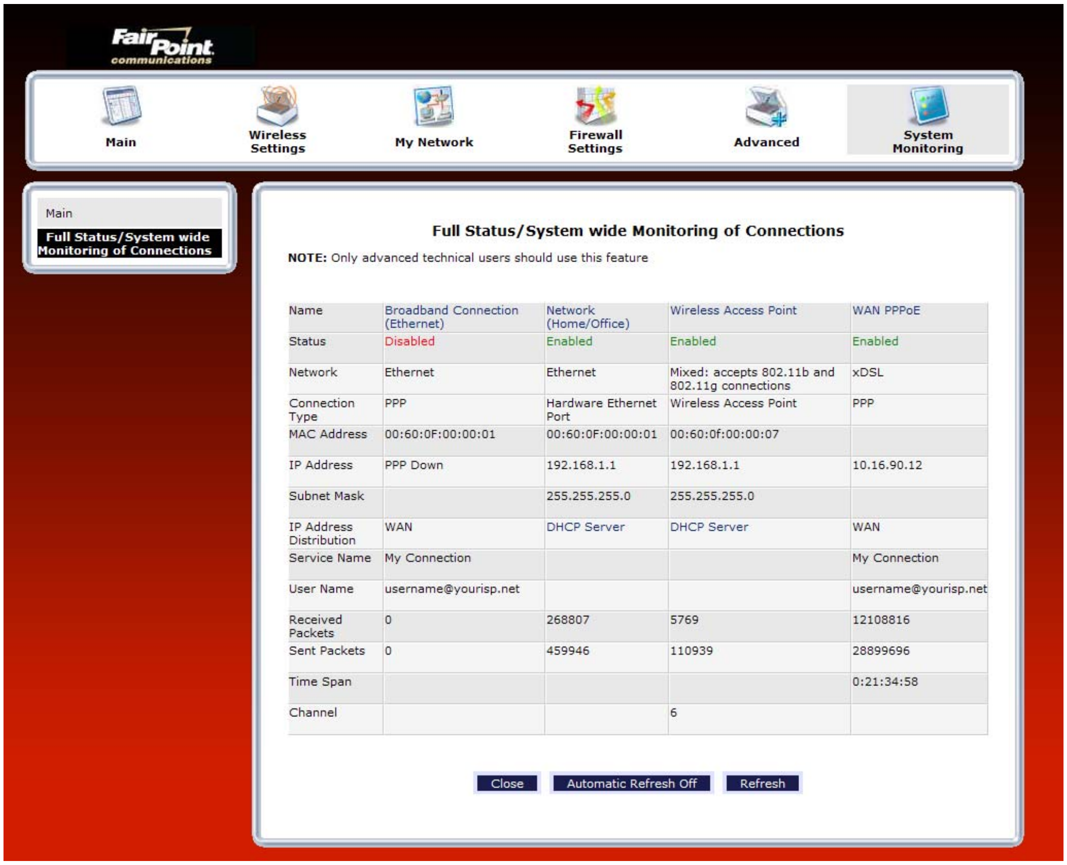
Encoding: Western European (Windows)

17.2.2 Full Status/System-wide Monitoring of Connections

In the **Advanced Status** screen, click **Full Status/System-wide Monitoring of Connection.** The following screen will be displayed. After viewing the details of your Router’s connection, you can do any of the following:

- Click the **Broadband Connection** link to go to the VersaPort page and edit your broadband settings. Refer to section 14.2.3 for additional details on this feature.
- Click the **Network (Home/Office)** link to go to the Private LAN DHCP page and edit your Private LAN DHCP settings. Refer to section 16.17 for additional details on this feature.
- Click **Wireless Access Point** link to go to the Basic Security Settings page and edit your wireless settings. Refer to section 13.3 for additional details on this feature.
- Click the **WAN PPPoE** link to go to the Advanced DSL Configuration page and edit your connection settings. Refer to section 14.2.2 for additional details on this feature.
- Click the **DHCP Server** link to go to the Private LAN page and edit your Private LAN DHCP Server settings. Refer to section 16.16 for additional details on this feature.
- Click the **Close** button to return to the **Advanced Status** screen.
- Click the **Automatic Refresh Off/On** button to turn on or turn off the screen’s automatic refresh feature.
- Click the **Refresh** button to manually refresh the screen.

NOTE: When the Automatic Refresh button displays **Automatic Refresh Off,** this means that the auto-refresh feature is turned Off. Click the Automatic Refresh button to turn on automatic refresh. When the button displays **Automatic Refresh On**, the page will refresh automatically.



Full Status/System wide Monitoring of Connections

NOTE: Only advanced technical users should use this feature

Name	Broadband Connection (Ethernet)	Network (Home/Office)	Wireless Access Point	WAN PPPoE
Status	Disabled	Enabled	Enabled	Enabled
Network	Ethernet	Ethernet	Mixed: accepts 802.11b and 802.11g connections	xDSL
Connection Type	PPP	Hardware Ethernet Port	Wireless Access Point	PPP
MAC Address	00:60:0F:00:00:01	00:60:0F:00:00:01	00:60:0f:00:00:07	
IP Address	PPP Down	192.168.1.1	192.168.1.1	10.16.90.12
Subnet Mask		255.255.255.0	255.255.255.0	
IP Address Distribution	WAN	DHCP Server	DHCP Server	WAN
Service Name	My Connection			My Connection
User Name	username@yourisp.net			username@yourisp.net
Received Packets	0	268807	5769	12108816
Sent Packets	0	459946	110939	28899696
Time Span				0:21:34:58
Channel			6	

Full Status/System-wide Monitoring of Connections	
Name	A descriptor used to identify the Router's connection type Network (Home/Office)-Displays information about the Routers LAN connection WAN PPPoE-Displays information about the Router's WAN/Braodband connection
Status	The status of the connection (Enabled/Disabled)
Network	Ethernet- The the interface used to connect the Router to your LAN xDSL - The interface used to connect to the Router to the WAN
Connection Type	Hardware Ethernet Port- The physical connection type; the hardware used for the LAN connection PPP the virtual connection type; the protocol use for WAN/Braodband connection
MAC Address	The Media Access Controller; the hardware address assigned to the deviced by the manufacturer
IP Address	The Router's LAN and WAN/Braodband IP Addresses
Subnet Mask	Displays the Router's Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host
IP Address Distribution	The method by which IP address are allocated to devices on your LAN
Service Name	The connection profile name to used to establish your Internet connection
User Name	The user name (Account ID) used to identify you to and to establish your Internet connection, provided by your Internet service provider.
Received Packets	The number of packets received in to the Router's LAN and WAN interfaces
Sent Packets	The number of packets sent out from the Router's LAN and WAN interfaces
Time Span	The duration your PPP session has been connected (measured in hours: minutes: seconds)
Channel	The channel of the wireless access point.

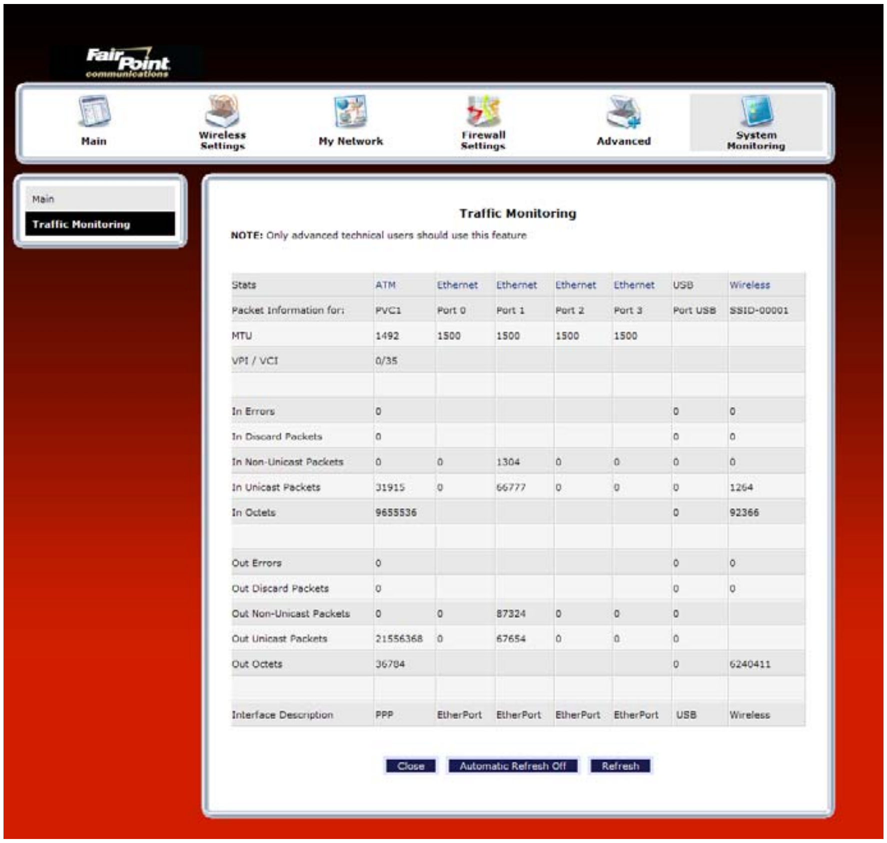
17.2.3 Traffic Monitoring

In the **Advanced Status** screen, click **Traffic Monitoring.** The following screen will be displayed. After viewing your Router's traffic details, you can do any of the following:

NOTE: Only advanced technical users should use this feature.

- Click the **ATM** link to go to the Advanced DSL Configuration page and edit your connection settings. Refer to section 14.2.2 for additional details on this feature.
- Click the **Ethernet** link to go to the Private LAN DHCP page and edit your Private LAN DHCP settings. Refer to section 16.17 for additional details on this feature.
- Click the **Wireless** link to go to the Basic Security Settings page and edit your wireless settings. Refer to section 13.3 for additional details on this feature.
- Click the **Close** button to return to the **Advanced Status** screen.
- Click the **Automatic Refresh Off/On** button to turn on or turn off the screen's automatic refresh feature.
- Click the **Refresh** button to manually refresh the screen.

NOTE: When the Automatic Refresh button displays **Automatic Refresh Off,** this means that the auto-refresh feature is turned off. Click the Automatic Refresh button to turn on automatic refresh. When the button displays **Automatic Refresh On**, the page will refresh automatically.



Traffic Monitoring

NOTE: Only advanced technical users should use this feature

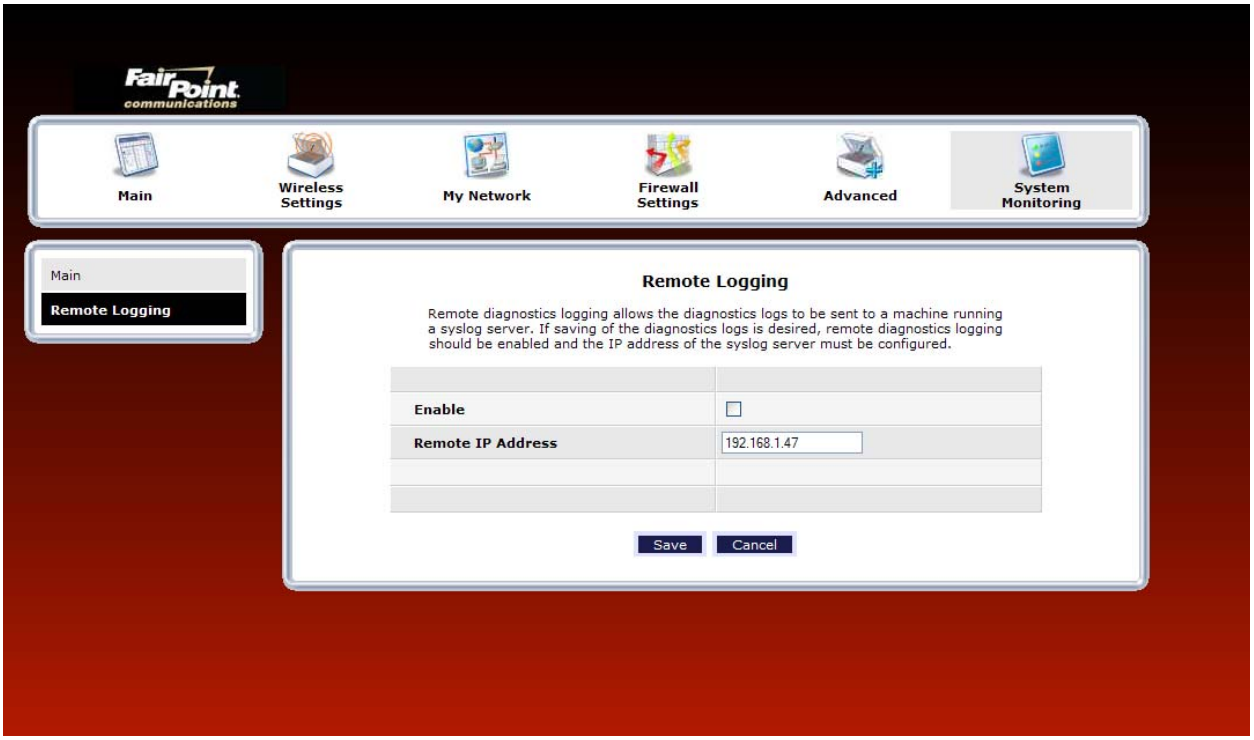
Stats	ATM	Ethernet	Ethernet	Ethernet	Ethernet	USB	Wireless
Packet Information for:	PVC1	Port 0	Port 1	Port 2	Port 3	Port USB	SSID-00001
MTU	1492	1500	1500	1500	1500		
VPI / VCI	0/35						
In Errors	0					0	0
In Discard Packets	0					0	0
In Non-Unicast Packets	0	0	1304	0	0	0	0
In Unicast Packets	31915	0	66777	0	0	0	1264
In Octets	9655536					0	92366
Out Errors	0					0	0
Out Discard Packets	0					0	0
Out Non-Unicast Packets	0	0	87324	0	0	0	
Out Unicast Packets	21556368	0	67654	0	0	0	
Out Octets	36784					0	6240411
Interface Description	PPP	EtherPort	EtherPort	EtherPort	EtherPort	USB	Wireless

Traffic Monitoring	
Stats	Represents the statistics for each interface type: ATM, Ethernet, or USB
Packet Information for	The packet information for the interface.
VPI/VCI	The VPI/VCI values obtained from .
In Errors	The number of error packets received on the interface.
In Discard Packets	The number of discarded packets received on the interface.
In Non Unicast Packets	The number of non-Unicast packets received on the interface.
In Unicast Packets	The number of Unicast packets received on the interface.
In Octets	The number of bytes received on the interface.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the interface.
Out Unicast Packets	The number of Unicast packets transmitted on the interface.
Out Octets	The number of bytes transmitted on the interface.
Interface Description	A description field that refers to the interface type.

17.2.4 Remote Logging

In the **Advanced Status** screen, click **Remote Logging.** The following screen will be displayed. Remote diagnostics logging allows the diagnostics logs to be sent to a machine running a syslog server.

To save the diagnostics logs, click the **Enable** box (a check mark will appear in the box). Next, type the IP address of the syslog server in the **Remote IP Address** field. Click **Save** to save the settings.



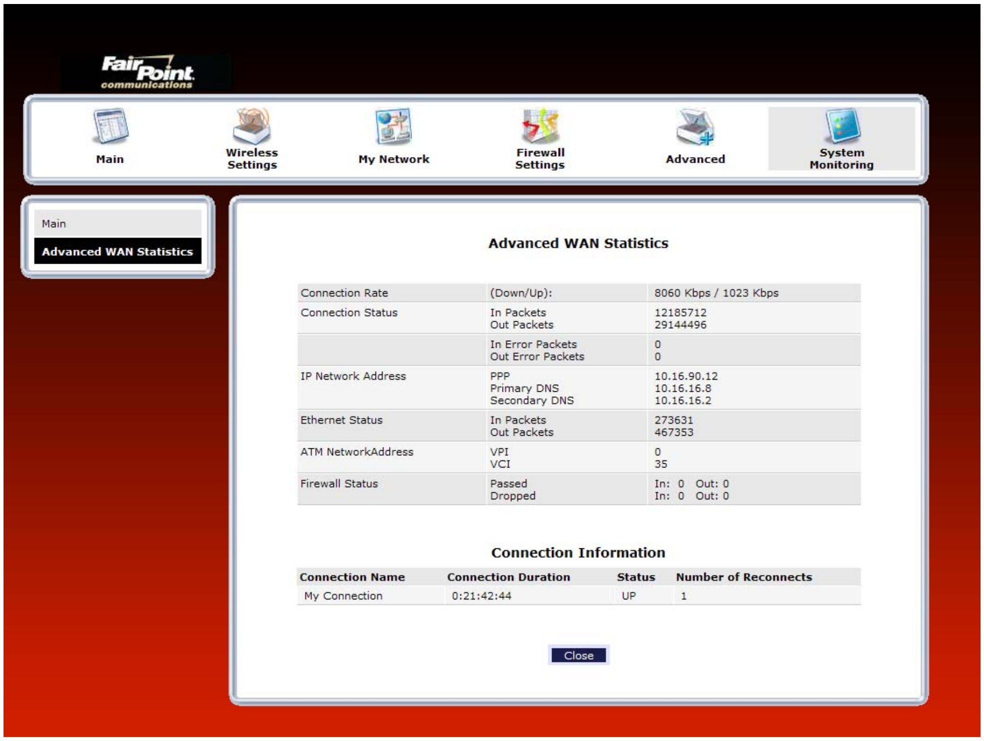
Remote Logging

Remote diagnostics logging allows the diagnostics logs to be sent to a machine running a syslog server. If saving of the diagnostics logs is desired, remote diagnostics logging should be enabled and the IP address of the syslog server must be configured.

Enable	□
Remote IP Address	192.168.1.47

17.2.5 Advanced WAN Statistics

In the **Advanced Status** screen, click **Advanced WAN Statistics.** The following screen will be displayed. After you have viewed the details in this page, click **Close** to return to the **Advanced Status** screen.



Advanced WAN Statistics

Connection Rate	(Down/Up):	8060 Kbps / 1023 Kbps
Connection Status	In Packets Out Packets	12185712 29144496
	In Error Packets Out Error Packets	0 0
IP Network Address	PPP Primary DNS Secondary DNS	10.16.90.12 10.16.16.8 10.16.16.2
Ethernet Status	In Packets Out Packets	273631 467353
ATM NetworkAddress	VPI VCI	0 35
Firewall Status	Passed Dropped	In: 0 Out: 0 In: 0 Out: 0

Connection Information

Connection Name	Connection Duration	Status	Number of Reconnects
My Connection	0:21:42:44	UP	1

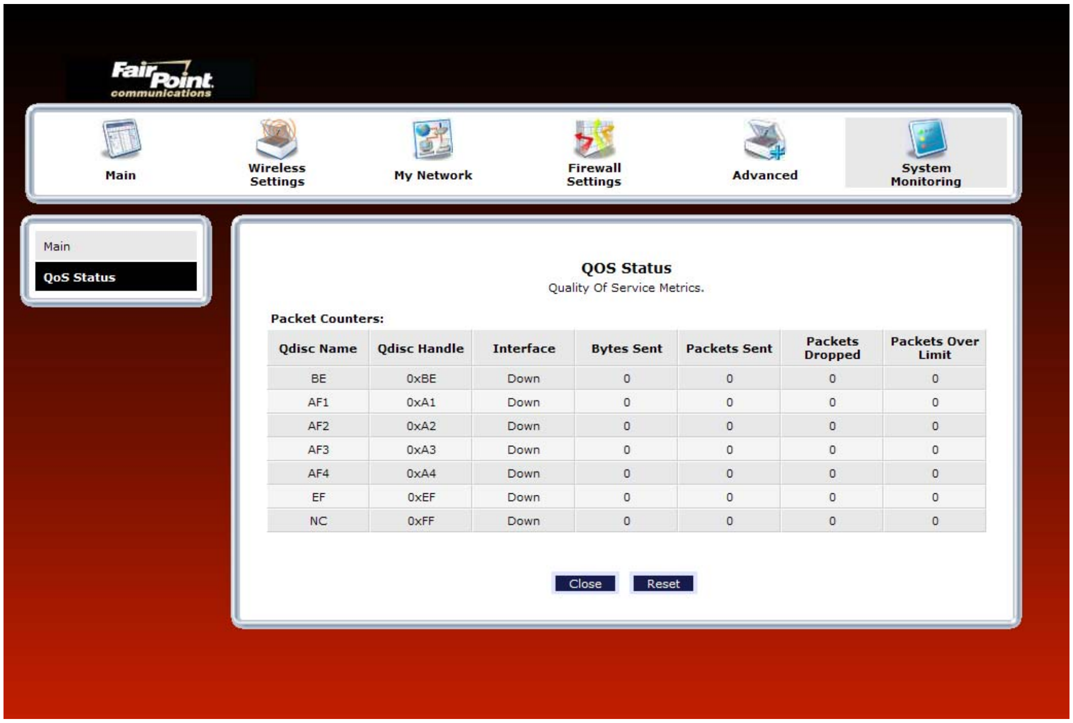
DSL Connection Information	
Connection Rate	This field will let you know if you have a DSL signal and the DSL rate at which you are connected.
Connection Status	This field will show how much information was received (IN) or sent (OUT) in packets.
IP Network Address	PPP = An IP address identifies your device on the Internet Primary DNS = Provided by your Internet service provider. Secondary DNS = Provided by your Internet service provider.
Ethernet Status	This field will display your Ethernet information that was received (IN) or sent (OUT) in packets on your Ethernet port.
ATM Network Address	This field will display your VPI and VCI values, which are provided by your Internet service provider.
Firewall Status	This field will display your firewall traffic in packets. Passed: Monitors information traffic that was successfully received (IN) or transmitted (OUT) in packets. Dropped: Monitors information traffic that was not successfully received (IN) or transmitted (OUT) due to your firewall settings.
PPP Connection Information	
Connection Name	This is from the connection profile that you established in section 8.
Connection Duration	This field will display how long your PPP session has been connected.

Status	This field will display the status of your PPP session.
	UP=Connected
	DOWN=Disconnected

Number of Reconnects	This field will display the number of attempts that were made to establish a PPP session.

17.2.6 QOS Status

In the **Advanced Status** screen, click **QOS Status**. The following screen will be displayed. Click the **Clear** button to clear all counts and statistics (not just latency counts). Clicking **Clear** does not affect the Router's configuration. (QOS must be enabled on the Router for this table to be populated.) After you have viewed the details in this page, click **Close** to return to the **Advanced Status** screen.



QOS Status

Quality Of Service Metrics.

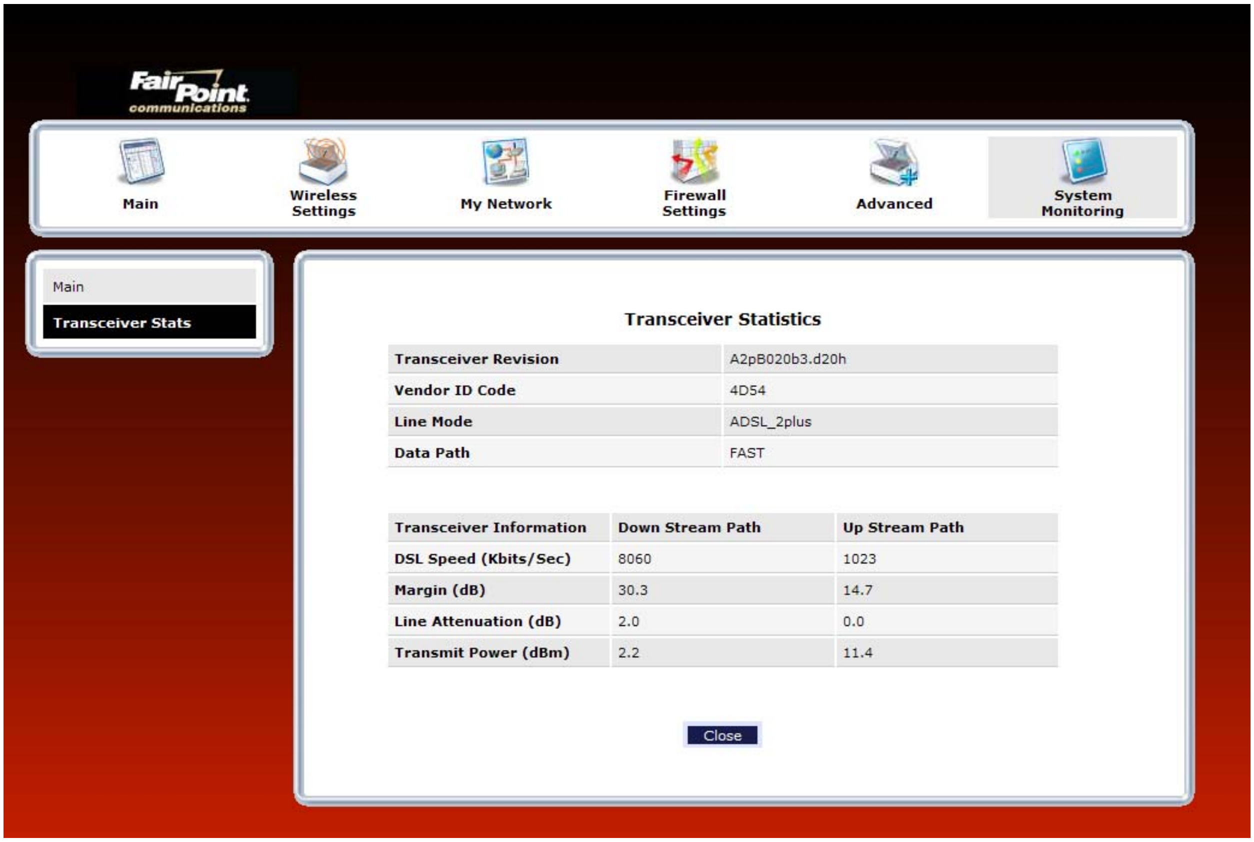
Packet Counters:

Qdisc Name	Qdisc Handle	Interface	Bytes Sent	Packets Sent	Packets Dropped	Packets Over Limit
BE	0xBE	Down	0	0	0	0
AF1	0xA1	Down	0	0	0	0
AF2	0xA2	Down	0	0	0	0
AF3	0xA3	Down	0	0	0	0
AF4	0xA4	Down	0	0	0	0
EF	0xEF	Down	0	0	0	0
NC	0xFF	Down	0	0	0	0

QOS Status	
Queue Number	Indicates the DiffServ Queue. Queue Number Descriptions: 0 = Best Effort (BE) 1 = Assured Forwarding 1 (AF1) 2 = Assured Forwarding 2 (AF2) 3 = Assured Forwarding 2 (AF3) 4 = Assured Forwarding 2 (AF4) 5 = Expedited Forwarding (EF) 6 = Routing Protocols (DiffServ priorities 6 and 7)
Max Queue Size	The maximum number of packets that can be queued for this priority.
Total Dropped Packets	Indicates how many packets of this priority have been dropped by QOS due to lack of buffer space or filtering rules.
Total Sent Packets	Displays the number of packets, destined for the WAN, that have been received.
Total Overlimit Packets	Displays the current number of overlimit packets.
Total Requeued Packets	Displays the most number of packets that have been requeued for this priority.

17.2.7 Transceiver Statistics

In the **Advanced Status** screen, click **Transceiver Statistics.** The following screen will be displayed. After you have viewed the details in this page, click **Close** to return to the **Advanced Status** screen.



Transceiver Statistics

Transceiver Revision	A2pB020b3.d20h
Vendor ID Code	4D54
Line Mode	ADSL_2plus
Data Path	FAST

Transceiver Information	Down Stream Path	Up Stream Path
DSL Speed (Kbits/Sec)	8060	1023
Margin (dB)	30.3	14.7
Line Attenuation (dB)	2.0	0.0
Transmit Power (dBm)	2.2	11.4

Transceiver Statistics	
Transceiver Revision	The transceiver software version number.
Vendor ID Code	The CPE Vendor's ID code for their chipset.
Line Mode	The operational mode. Modes supported are No Mode, Multi Mode, T1.413 Mode, G.DMT Mode, and G.LITE Mode.
Data Path	The data path used (either Fast or Interleaved).
Transceiver Information-Down Stream/Up Stream Path	
DSL Speed (Kbits/Sec)	The transmission rate that is provided by your Internet service provider.
SNR Margin (dB)	The Signal-to-Noise Ratio (S/N) where 0 db = 1x10^{-7}, which inhibits your DSL speed.
Line Attenuation (dB)	The DSL line loss.
Transmit Power (dBm)	The transmitted signal strength.

18. PORT FORWARDING SERVICES

For your convenience, VersaLink supports protocols for Applications, Games, and VPN-specific programs. The following chart provides port/protocol information for the supported services.

NOTE: To configure the Router for a service or application, follow the steps in section 15.3.3, "Configuring Port Forwarding Services," of this User Guide.

Applications/Games/VPN Support	
Application/Game	**Port/Protocol**
Aliens vs. Predator	80 UDP, 2300 UDP, 8000-8999 UDP
Age of Empires II: The Conquerors	6073 UDP, 47624 TCP, 2300-2400 TCP/UDP This service will open up ports for both traffic directions.
Americas Army	TCP – 20045 UDP – 1716 to 1718, 8777, 27900
America Online	5190 TCP/UDP
Anarchy Online	TCP/UDP – 7012,7013, 7500 -7505
AOL Instant Messenger	4099 TCP, 5190 TCP
Asheron's Call	9000-9013 UDP, 28800-29000 TCP
Battlecom	2300-2400 TCP/UDP, 47624 TCP/UDP
Battlefield 1942	UDP - 14567, 22000, 23000 to 23009, 27900, 28900
Black and White	2611-2612 TCP, 6667 TCP, 6500 UDP, 27900 UDP
Blizzard Battle.net (Diablo II)	4000 TCP, 6112 TCP/UDP
Buddy Phone	700, 701 UDP
Bungie.net, Myth, Myth II Server	3453 TCP
Calista IP Phone	3000 UDP, 5190 TCP
Citrix Metaframe	1494 TCP
Client POP/IMAP	110 TCP
Client SMTP	25 TCP
Counter Strike	27015 TCP/UDP, 27016 TCP/UDP
Dark Reign 2	26214 TCP/UDP
Delta Force (Client and Server)	3568 UDP, 3100-3999 TCP/UDP
Delta Force 2	3568-3569 UDP
DeltaForce: Land Warrior	UDP 53 TCP 21 TCP 7430 TCP 80 UDP 1029 UDP 1144 UDP 65436 UDP 17478
DNS 53	UDP
Elite Force	2600 UDP, 27500 UDP, 27910 UDP, 27960 UDP
Everquest 1	024-7000 TCP/UDP
F-16, Mig 29	3863 UDP
F-22 Lightning 3	4660-4670 TCP/UDP, 3875 UDP, 4533-4534 UDP, 4660-4670 UDP
F-22 Raptor	3874-3875 UDP
Fighter Ace II	50000-50100 TCP/UDP
Fighter Ace II for DX play	50000-50100 TCP/UDP, 47624 TCP, 2300-2400 TCP/UDP
FTP	20 TCP, 21 TCP
GameSpy Online	UDP 3783 UDP 6515

	TCP 6667 UDP 12203 TCP/UDP 13139 UDP 27900 UDP 28900 UDP 29900 UDP 29901
Ghost Recon	TCP 80 UDP 1038 UDP 1032 UDP 53 UDP 2347 UDP 2346
GNUtella	6346 TCP/UDP, 1214 TCP
Half Life Server	27005 UDP(client only) 27015 UDP
Heretic II Server	28910 TCP
Hexen II	26900 (+1) each player needs their own port. Increment by one for each person.
Hotline Server	5500, 5503 TCP 5499 UDP
HTTPS 443	TCP/UDP
ICMP Echo	4 ICMP
ICQ OLD	4000 UDP, 20000-20019 TCP
ICQ 2001b	4099 TCP, 5190 TCP
ICUII Client	2000-2038 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP
ICUII Client Version 4.xx	1024-5000 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP, 2000-2038 TCP6700-6702 TCP, 6880 TCP, 1200-16090 TCP
IMAP 11	9 TCP/UDP
IMAP v.3	220 TCP/UDP
Internet Phone	22555 UDP
IPSEC ALG	IPSEC ALG
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
JKII:JO (Jedi Knight II: Jedi Outcast)	UDP - 28070 (default) UDP- 27000 to 29000
KALI, Doom & Doom II	2213 UDP, 6666 UDP (EACH PC USING KALI MUST USE A DIFFERENT PORT NUMBER STARTING WITH 2213 + 1)
KaZaA 12	14 TCP/UDP
Limewire	6346 TCP/UDP, 1214 TCP
Medal Of Honor: Allied Assault	TCP 80 UDP 53 UDP 2093 UDP 12201 TCP 12300 UDP 2135 UDP 2139 TCP/UDP 28900
mIRC Chat	6660-6669 TCP
Motorhead Server	16000 TCP/UDP, 16010-16030 TCP/UDP
MSN Game Zone	6667 TCP, 28800-29000 TCP
MSN Game Zone (DX 7 & 8 play)	6667 TCP, 6073 TCP, 28800-29000 TCP, 47624 TCP, 2300-2400 TCP/UDP This service will open up ports for both traffic directions.
MSN Messenger	6891-6900 TCP, 1863 TCP/UDP, 5190 UDP, 6901 TCP/UDP

Napster 66	99 TCP
Need for Speed 3, Hot Pursuit	1030 TCP
Need for Speed, Porsche 9442	UDP
Net2Phone 68	01 UDP
NNTP 11	9 TCP/UDP
Operation FlashPoint	47624 UDP, 6073 UDP, 2300-2400 TCP/UDP, 2234 TCP
Outlaws 53	10 TCP/UDP
Pal Talk	2090-2091 TCP/UDP, 2095 TCP, 5001 TCP, 8200-8700 TCP/UDP, 1025-2500 UDP
pcAnywhere host	5631 TCP, 5632 UDP, 22 UDP
Phone Free	1034-1035 TCP/UDP, 9900-9901 UDP, 2644 TCP, 8000 TCP
Quake 2	27910 UDP
Quake 3	27660 UDP Each computer playing QuakeIII must use a different port number, starting at 27660 and incrementing by 1. You'll also need to do the following: 1. Right click on the QIII icon 2. Choose "Properties" 3. In the Target field you'll see a line like "C:\Program Files\Quake III Arena\quake3.exe" 4. Add the Quake III net_port command to specify a unique communication port for each system. The complete field should look like this: "C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660 5. Click OK. 6. Repeat for each system behind the NAT, adding one to the net_port selected (27660,27661,27662)
Quicktime 4/Real Audio	6970-32000 UDP, 554 TCP/UDP
Rainbow Six & Rogue Spear	2346 TCP
RealOne Player	TCP - 554, 7070 to 7071 UDP - 6970 to 7170
Real Audio	6970-7170 UDP
Return To Castle Wolfenstein	Default -27960 TCP/UDP UDP - 27950 to 27980
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
SIP ALG	SIP ALG
ShoutCast Server	8000-8005 TCP
Spinner Radio/Netscape Music	TCP - 554
SSH Secure Shell	22 TCP/UDP
Starcraft 2346	TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
SOF/SOFII (Soldier of Fortune / Soldier of Fortune II)	UDP - 28910 to 28915
Telnet 23	TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Tribes2	TCP - 15104, 15204, 15206, 6660 to 6699 UDP - 27999 to 28002
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port) 7779,7779+ are allocated dynamically for each helper UdpLink objects, including UdpServerUplin objects. Try starting with 7779-7781 and add ports if needed.

	27900 server query, if master server uplink is enabled. Home master servers use other ports like 27500. Port 8080 is for UT Server Admin. In the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 and ServerName to the IP assigned to the Gateway from .
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 or 8080 TCP (PROXY)
Xbox Live	88 TCP/UDP, 3074 TCP/UDP
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
NAT/VPN Support	
IPSec Encryption	IPSec using AH can not be supported through NAT. IPSec using ESP and L2TP can be supported via an ALG
L2TP	IPSec using ESP and L2TP can be supported via an ALG.
PPTP	Works through NAT.

19. TECHNICAL SUPPORT INFORMATION

Contact your Internet service provider for technical support.

20. PRODUCT SPECIFICATIONS

System Requirements for and 10/100 Base-T/Ethernet

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

System Requirements for USB

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (Vista™, XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- USB Version 1.1 or higher compliant bus
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer operating system CD-ROM

System Requirements for Wireless

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (Vista™, XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- USB Version 1.1 or higher compliant bus
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer operating system CD-ROM
- IEEE 802.11b/g/n PC adapter

LEDs

- Power
- E1, E2, E3, E4
- Wireless
- USB
- DSL
- Internet

Connectors

- DSL: 6-pin RJ-11 modular jack-DSL
- Ethernet: 8-pin RJ-45 modular jack
- Power: Barrel connector

Power

- Power Supply: External 120 VAC (10%) to 12 VDC wall-mount power supply, small form factor
- Energy Star® qualified
- Power Consumption: Less than 8 watts typical, from 120 VAC

Dimensions

- Height: 1.3 in. (3.30 cm)
- Width: 7.0 in (17.78 cm)
- Depth: 4.9 in. (12.44 cm)

Weight

- Approx. 1 lb (0.45 kg)

Environmental

- Ambient Operating Temperature: +32 to +104 °F (0 to +40 °C)
- Relative Humidity: 5 to 95%, non-condensing

EMC/Safety/Regulatory Certifications

- FCC Part 15
- FCC Part 68
- ANSI/UL Standard 60950-1

21. SOFTWARE LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

22. PUBLICATION INFORMATION

Westell VersaLink Wireless Gateway (Model 7550)
Document Part Number 030-300629 Rev. A