technicolor

WIRELESS ADSL2+GATEWAY
TD5130

User's Manual

Table of Contents

Chapter 1: Product Overview

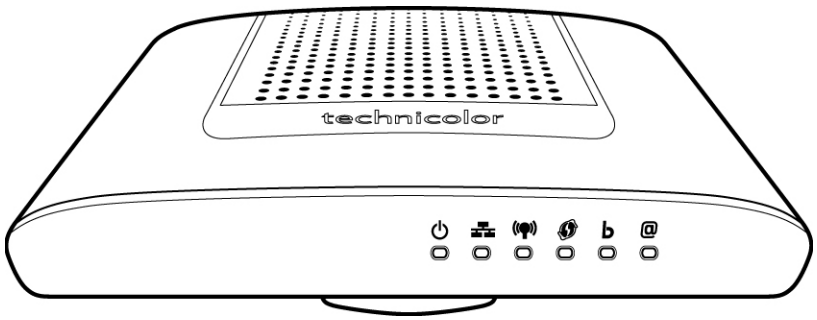
Thank you for choosing Technicolor® Wireless ADSL2+ Gateway. This Wireless Gateway combines the functionality of an ADSL modem and Internet gateway in one. You can access the Internet and share resources such as printers, scanners, and files, via a wireless connection or through one of the Ethernet ports. The various security features, such as WPS, WPA2, SPI, and NAT, protect your data and privacy online. The web-based utility allows you to configure your Wireless Gateway easily.

1.1 Features

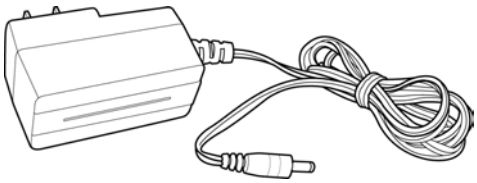
- Compliant with ADSL G.dmt (G.992.1), G.lite (G.992.2) standards
- Compliant with ADSL2 G.dmt.bis (G.992.3) and ADSL2 + G.992.5 standards
- Up to Up to 24Mbps downstream, 1.2Mbps upstream with ADSL2+ service
- IEEE 802.11b/g/n infrastructure operating modes
- Supports IPv4 and IPv6 protocols
- Supports web-based configuration
- Supports Command Line Interface (CLI) via Telnet
- Supports NAT, DHCP
- Supports VLAN and QoS
- Supports firewall protection
- Supports up to 8 permanent virtual circuits (PVC)
- Supports Wi-Fi Multimedia (WMM)
- Supports Wi-Fi Protected Setup (WPS) for easy connection
- Supports wireless data encryption with 64/128-bit WEP standard
- Supports enhance security for WPA-TKIP, WPA2-AES, WPA, and WPA2

1.2 Package Contents

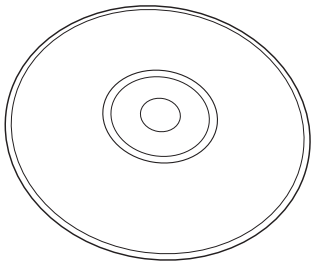
Check if the package contains the following items. If any item is missing or appears damaged, contact your dealer.



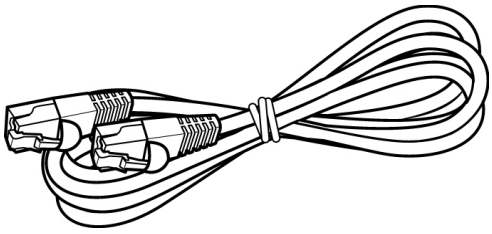
Wireless Gateway



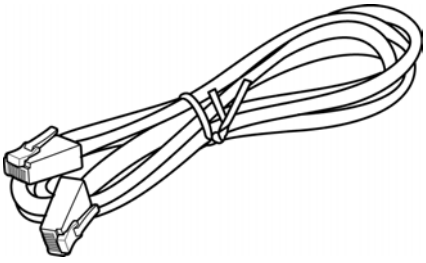
Power adapter



CD-ROM with User's Guide



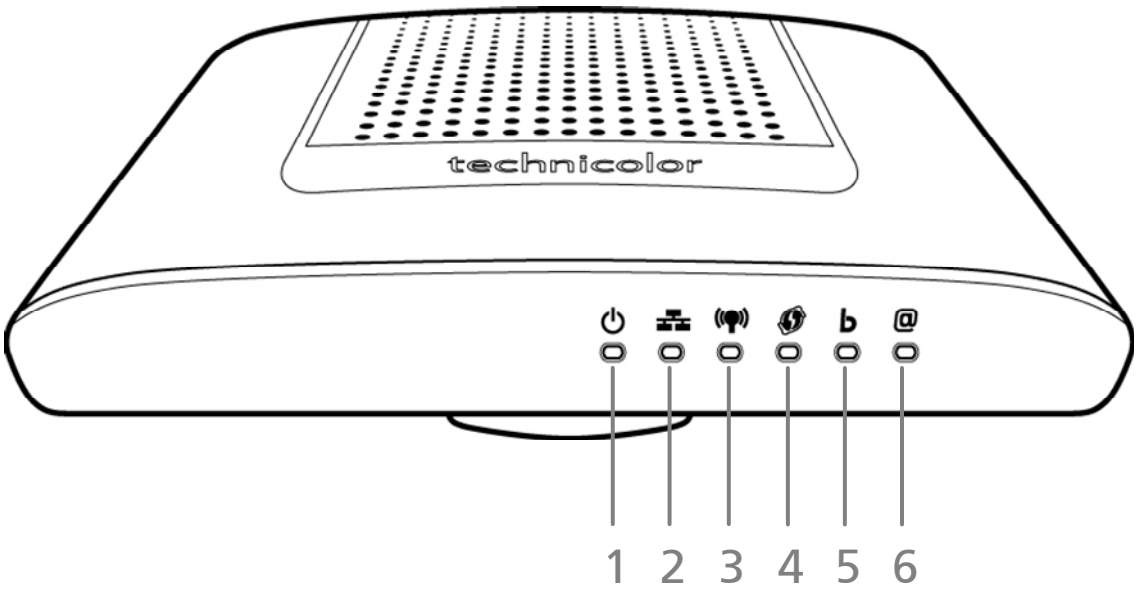
RJ-45 Ethernet cable



RJ-11 telephone cable

1.3 Hardware Overview

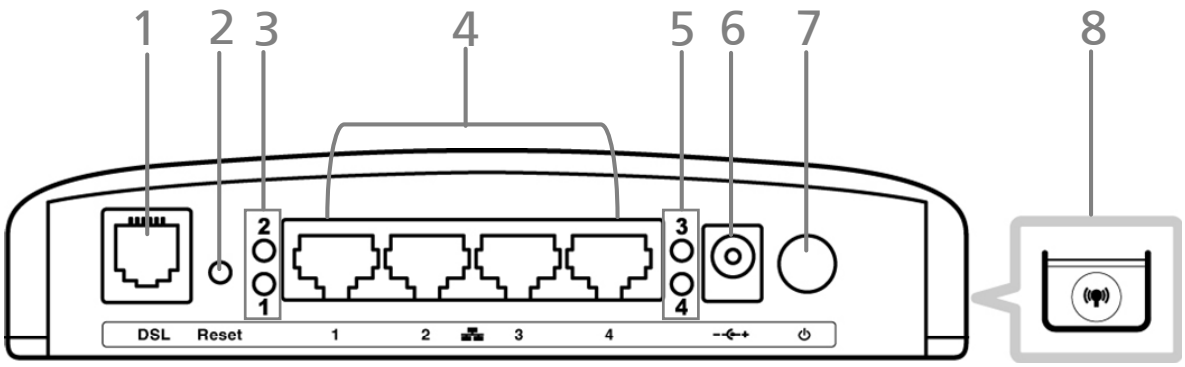
1.3.1 Front Panel



No.	LED	Description
1	**Power LED**	Lights up when the device is powered on. • Solid GREEN – Indicates normal operation. • Flashing GREEN – Firmware upgrade in progress. • Solid RED – Indicates malfunction. • Off – The device is powered off.
2	**Ethernet LED**	• Solid GREEN – A wired connection is established. • Flashing GREEN – Data transmission is in progress. • Off – No wired connection detected.
3	**WLAN LED**	Lights up to indicate wireless connection. • Solid GREEN – Wireless connection is established. • Flashing GREEN – Data transmission is in progress. • Off – Wireless connection is disabled.

No.	LED	Description
4	**WPS LED**	Lights up to indicate the Wi-Fi Protected Setup (WPS) connection status. • Solid GREEN – WPS-enabled device is connected. • Flashing GREEN – Data transmission is in progress. • Flashing RED – WPS connection failed. • Off – WPS is disabled.
5	**Broadband (DSL) LED**	Lights up to indicate DSL connection status. • Flashing GREEN – Attempts to synchronize with DSL line. • Solid GREEN – DSL connection is established. • Off – DSL connection is not present.
6	**Internet LED**	Lights up to indicate Internet connection status. • Solid GREEN – Internet is connected but no activity. • Flashing GREEN – Data transmission is in progress. • Solid RED – Internet connection failed. • Off – No internet connection.

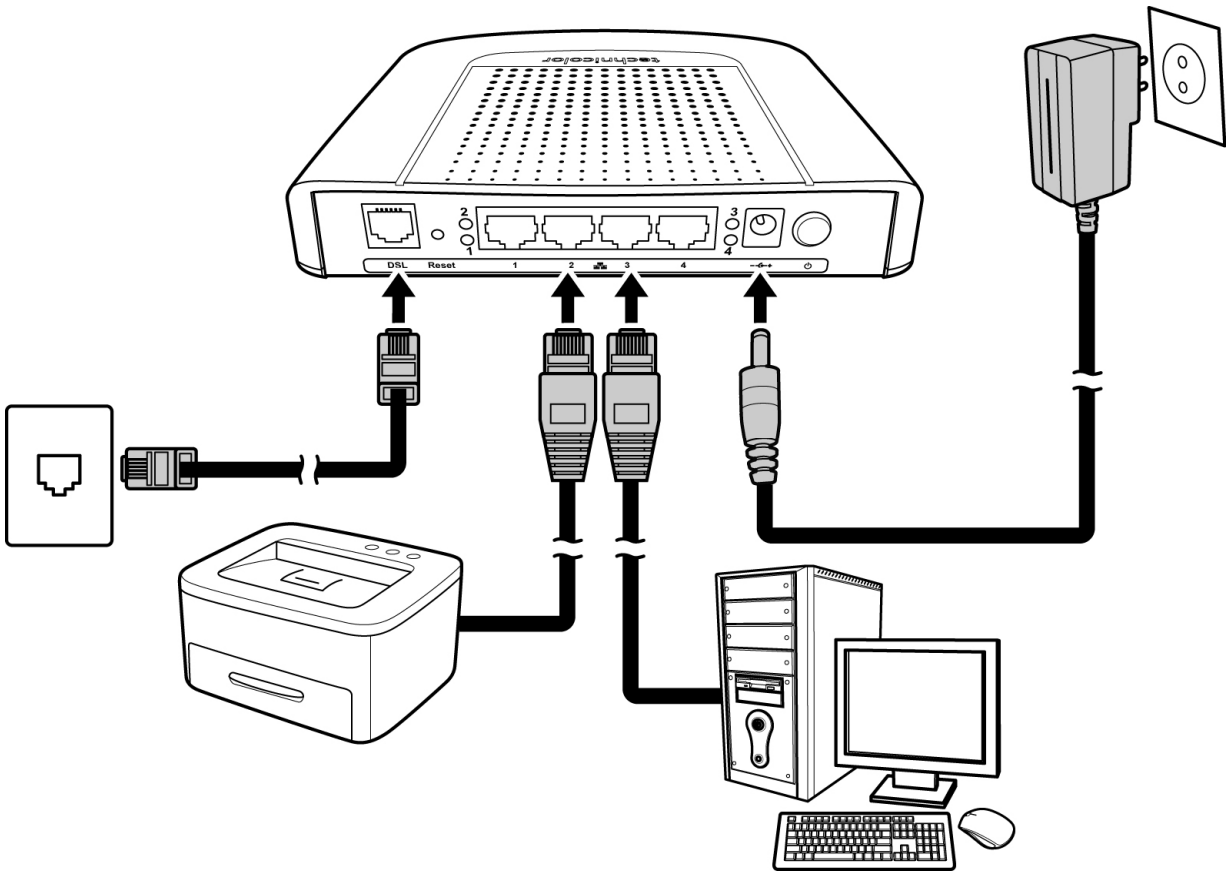
1.3.2 Rear Panel



No.	Ports / Buttons	Description
1	**DSL port**	Connects to the DSL line using the RJ-11 cable.
2	**Reset button**	Press and hold this button for at least 10 seconds to restore your device to its original factory default setting.
3	**LAN LED 1, 2**	The LAN LED (1, 2) lights up when a device is connected to the Ethernet port (1, 2).
4	**Ethernet port 1, 2, 3, 4**	Connects a computer and other Ethernet network devices to the Wireless Gateway using RJ-45 cables.
5	**LAN LED 3, 4**	The LAN LED (3, 4) lights up when a device is connected to the Ethernet port (3, 4).
6	**DC In jack**	Connects to the power adapter.
7	**Power button**	Press to turn your device on or off.
8	**WPS button**	Press to enable the WLAN. Press and hold to enable WPS.

Chapter 2: Installation

Make sure that all devices are powered off before starting installation.



Installation Diagram

2.1 Connect the Power

1. Connect the power adapter to the DC In jack of your Wireless Gateway.
2. Plug the power adapter to a wall outlet or a power strip.

NOTE:

- Use only the supplied power adapter. Using other power adapters may cause damage to the device.
- Connect all devices to your Wireless Gateway before connecting the power adapter to a wall outlet.

2.2 Connect Wired Devices

Connect devices such as computers, printers, and other Ethernet-enabled devices to the LAN port of the Wireless Gateway.

NOTE:

When setting up the Wireless Gateway for the first time, connect the host computer via Ethernet connection.

1. Connect one end of the RJ-45 cable to one of the Ethernet (1, 2, 3, 4) ports of your Wireless Gateway.
2. Connect the other end of the RJ-45 cable to the Ethernet port of the computer.
3. Repeat the above steps to connect other computers to the Wireless Gateway via Ethernet connection.
4. To connect more than four computers, use a hub or switch. Connect one end of an RJ-45 cable to the hub or switch and the other end to the computer.

2.3 Connect Wireless Devices

Before connecting wireless devices to the Wireless Gateway, configure the wireless security settings of your Wireless Gateway (see “Security Setting” on page 32). Take note of the SSID and the password you have set, you need the SSID and the password to connect devices to your Wireless Gateway.

2.3.1 WLAN

From the wireless device end, search for the Wireless Gateway network name (SSID), and enter the passphrase to connect.

NOTE:

The SSID and passphrase are the ones you have set in the Wireless Security Settings (see “Security Setting” on page 32).

2.3.2 Wi-Fi Protected Setup (WPS)

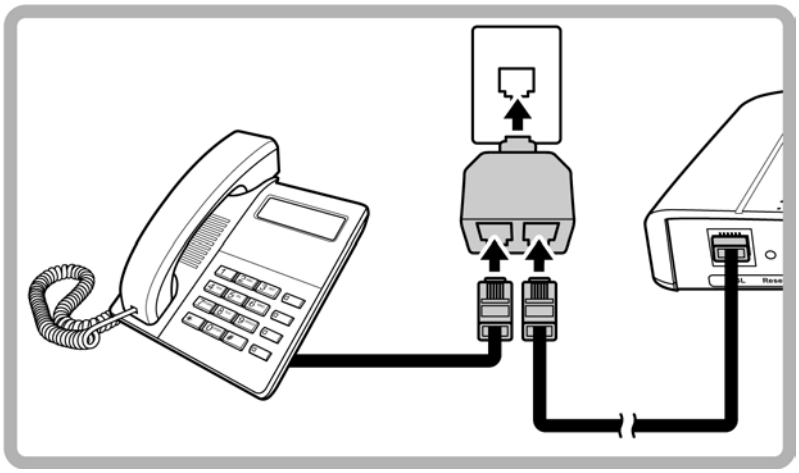
Press the **WPS button** of the Wireless Gateway and the WPS button on the WPS-enabled device to start pairing.

2.4 Connect the Broadband (DSL)

1. Connect one end of the RJ-11 cable to the DSL port of your Wireless Gateway.
2. Connect the other end of the RJ-11 cable to a wall jack with DSL service.

2.4.1 Use a Splitter

You need a splitter when connecting the Wireless Gateway to the wall jack that also connects to a telephone.



1. Plug the splitter to the wall jack with DSL service.
2. Connect one end of the RJ-11 cable to the DSL port of your Wireless Gateway.
3. Connect the other end of the RJ-11 cable to the MODEM port of the splitter.
4. Connect the telephone to the LINE port of the splitter using another RJ-11 cable.

2.5 Check the Installation

To ensure that all devices are properly connected, check the LED indicators on the front of your Wireless Gateway. For basic installation, the following LEDs must be lit:

- √ Power LED
- √ Ethernet LED
- √ DSL LED

The lighted LED indicators vary depending on the type of connection that you make. See “Front Panel” on page 8 for more information about the LED indicators.

Chapter 3: Configure the Computer

This chapter will guide you on how to configure your computer according to the operating system you are using.

Windows® XP, see below.

Windows® Vista, see page 16.

Windows® 7, see page 16.

3.1 Windows XP

If you are using Windows® XP, follow the instructions below to configure your computer.

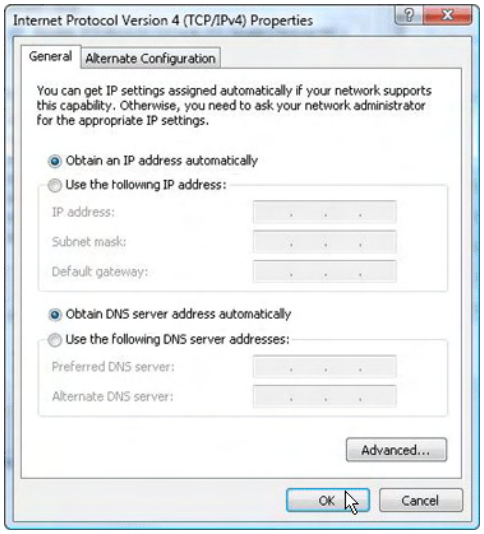
1. Click Start > Control Panel > Network Connections.
2. Right-click Local Area Connection, then click Properties.
3. On the network components list, make sure that **Internet Protocol (TCP/IP)** is checked. If not, check it to enable the **Properties** button.
4. Select Internet Protocol (TCP/IP), and then click Properties.
5. On the General tab, select Obtain an IP Address automatically and Obtain DNS server address automatically.
6. Click **OK**.

General Page

3.2 Windows Vista

If you are using Windows® Vista, follow the instructions below to configure your computer.

1. Click Start > Control Panel > Network and Internet Connections > Network Connections.
2. Right-click Local Area Connection, then click Properties.
3. On the General tab, make sure that **Internet Protocol (TCP/IP)** is checked. If not, check it to enable the **Properties** button.
4. Select Internet Protocol (TCP/IP), and then click Properties.
5. Select Obtain an IP Address automatically and Obtain DNS server address automatically.
6. Click **OK**.

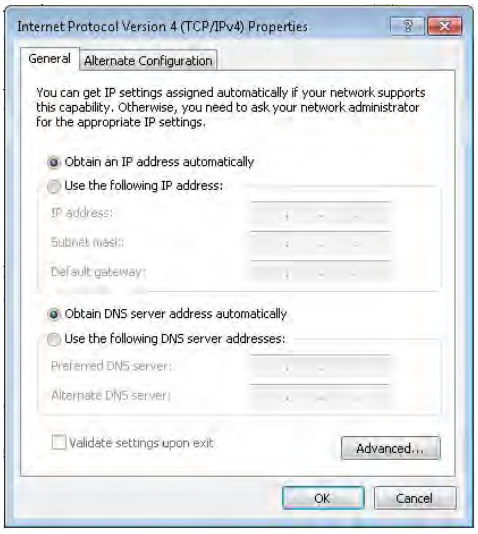


General Page

3.3 Windows 7

If you are using Windows® 7, follow the instructions below to configure your computer.

1. Click Start > Control Panel > Network & Sharing Center.
2. Click Local Area Connection.
3. Click Properties.
4. On the network components list, make sure that **Internet Protocol (TCP/IP)** is checked. If not, check it to enable the **Properties** button.
5. Select Internet Protocol (TCP/IP), and then click Properties.
6. On the General tab, select Obtain an IP Address automatically and Obtain DNS server address automatically.
7. Click **OK**.



General Page

Chapter 4: Access the Wireless Gateway

Use the Web Configurations utility to configure your Wireless Gateway.

1. Launch the web browser.
2. On the address bar, enter http://192.168.1.1, then press **Enter**.

NOTE:

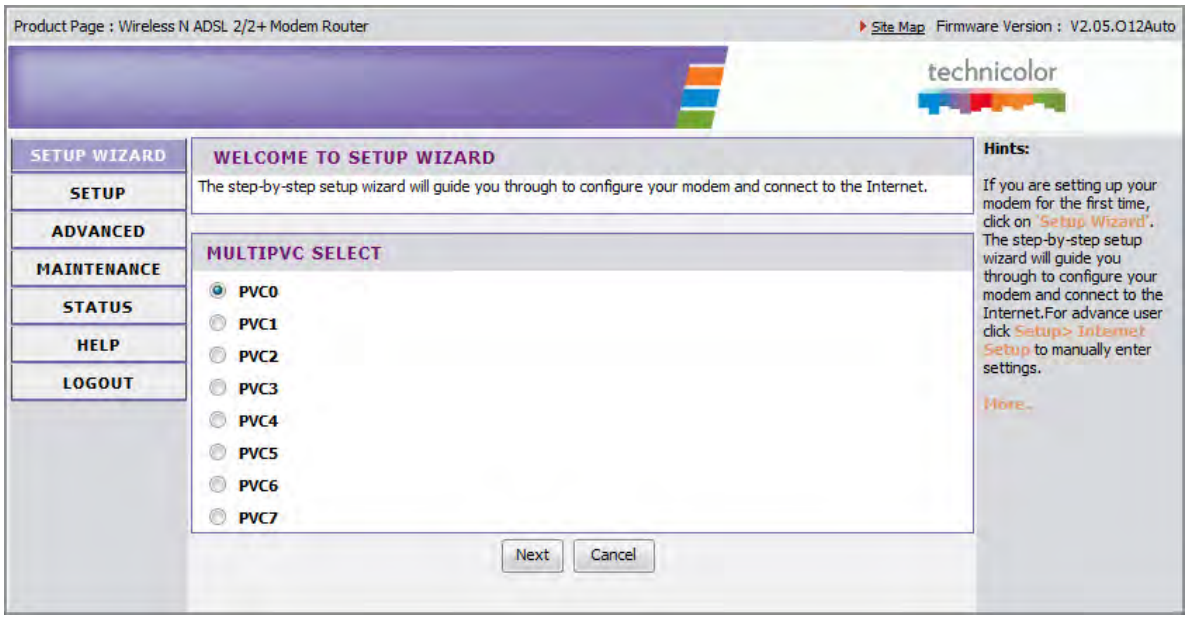
- For first time access, the **Setup Wizard** appears. See below.
- If the Web Configurations utility has been left idle for some minutes, the system may prompt you to login; enter the **User name** and **Password**. The default user name is "root" and the password is empty. It is advised to change the password, see "Password" on page 84.

4.1 Setup Wizard

It is recommended to follow the wizard if you are setting up the network and configuring the Wireless Gateway for the first time.

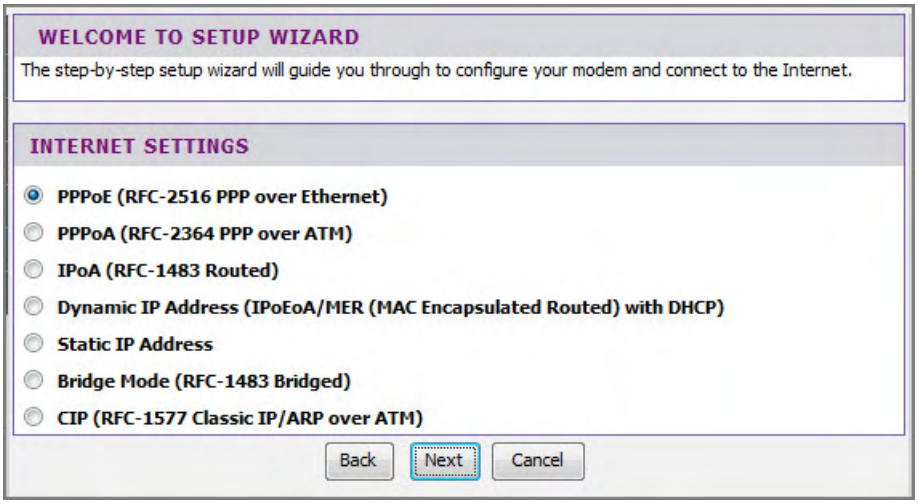
1. Select a **PVC** (Permanent Virtual Circuit), then click **Next**.

   It is recommended to use the default setting, PVC0, when setting up the Wireless Gateway for the first time.



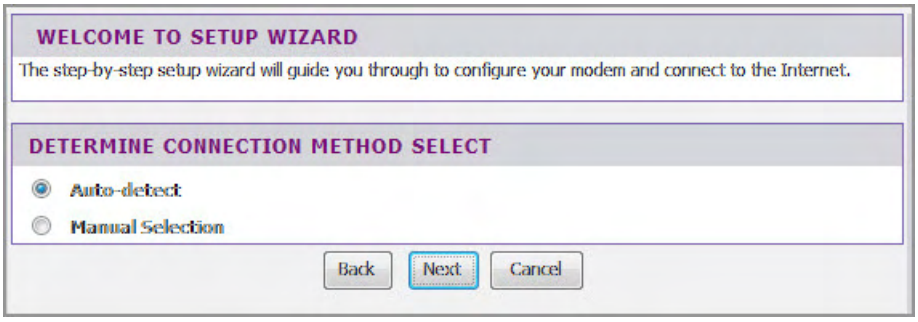
   The information on the succeeding pages can be obtained from your Internet service provider (ISP). Consult your ISP.

2. Select a network protocol. Click **Next** to continue.



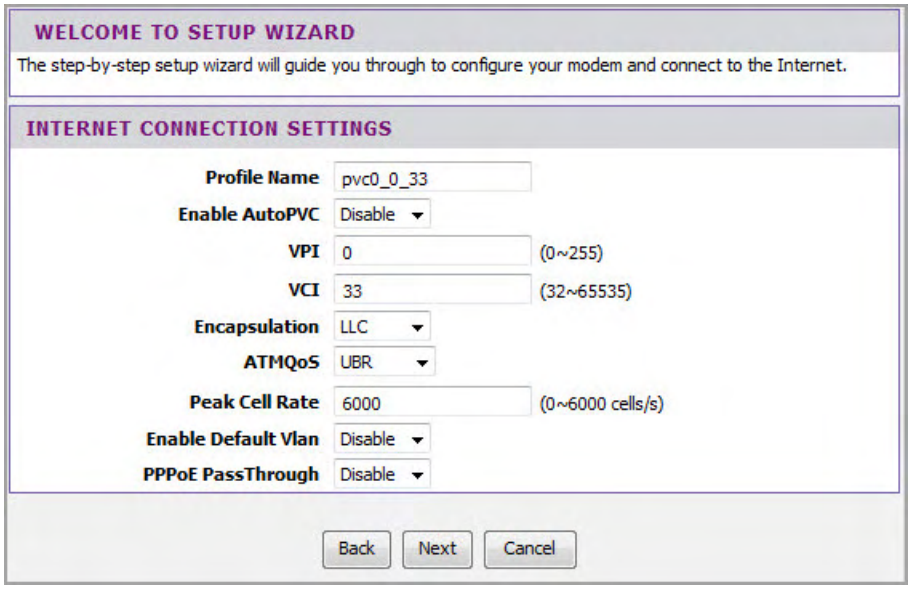
The information required on the succeeding pages varies depending on the network protocol you select here.

3. Select a scanning method, and then click **Next** to continue.



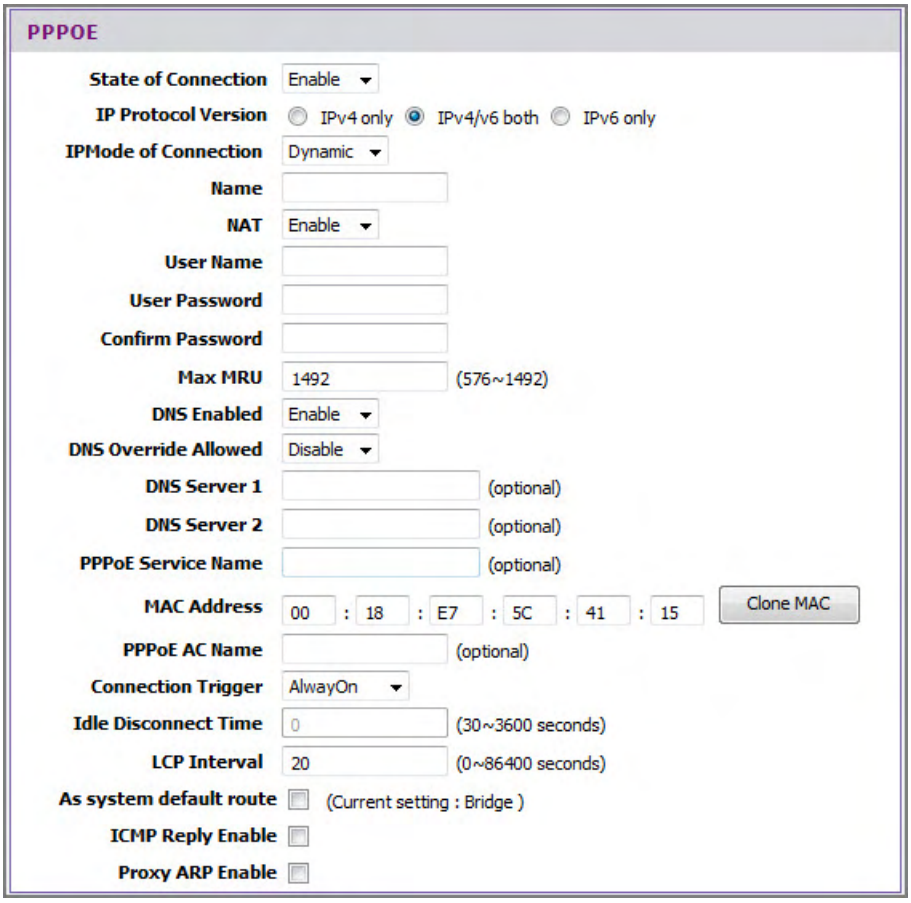
- **Auto Scan**: The Wireless Gateway automatically scans for Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).
- **Manual Scan**: To allow you to configure the VPI and VCI manually.

4. If **Auto Scan is selected**, skip to step 5.
   If **Manual Scan** is selected, do the following:



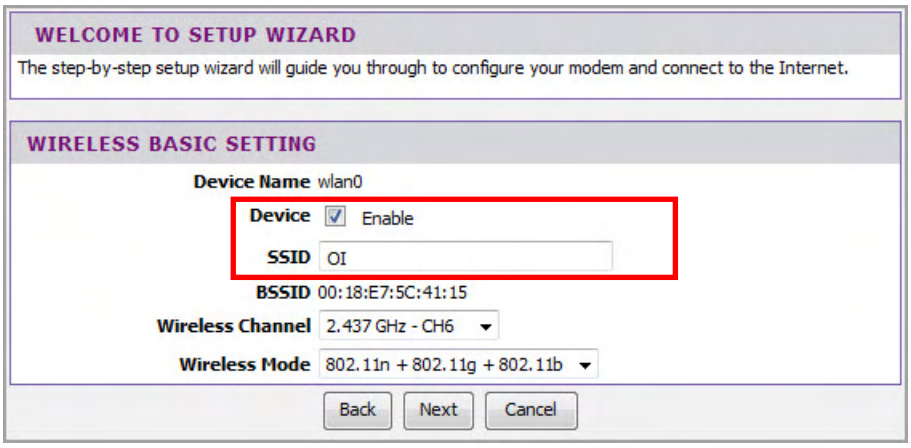
a. Enter desired **Profile Name**.
b. Enter the Virtual Path Identifier (**VPI**) and Virtual Channel Identifier (**VCI**).
c. Select an **Encapsulation** mode: LLC, VCMUX.
d. Select the **ATMQoS** option.
e. Enter a **Peak Cell Rate**.
f. Enable or disable **Default VLAN** and **PPPoE PassThrough**.
g. Click **Next** to continue.

5. The displayed screen varies depending on the network protocol you selected on step 2. Obtain the required information from your ISP.
The following is a PPPoE example.



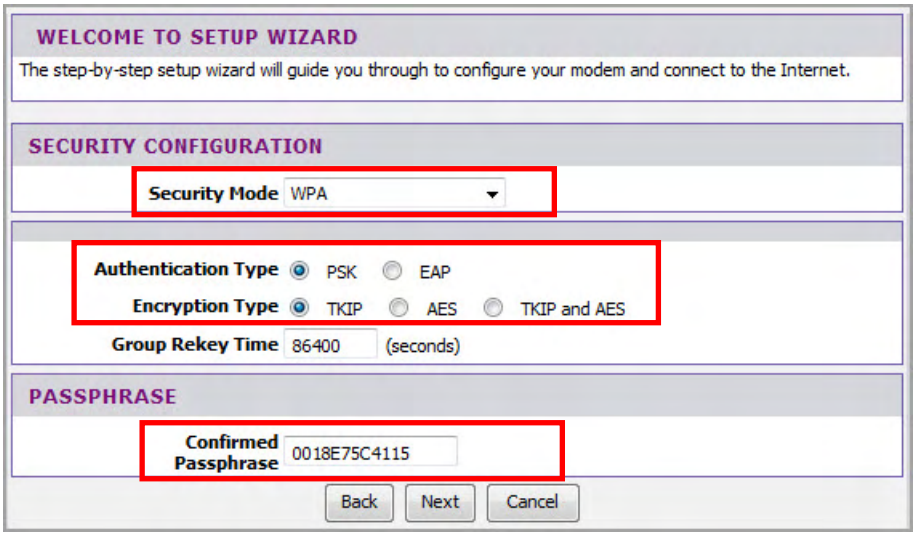
a. On **State of Connection**, select **Enable**.
b. Select an **IP Protocol Version**.
c. Select the
d. Enter the connection **Name**, **User Name**, and **User Password**. Re-type the password in the **Confirm Password** field.
e. Select whether to enable or disable features such as **NAT** (Network Address Translation), **DNS** (Domain Name System), and **DNS Override**.
f. Leave the remaining fields to their default settings.
g. Click **Next** to continue.

6. Select whether to enable or disable wireless connection. From this point, you can also change the **SSID** with a name that you can easily remember. Click **Next** to continue.

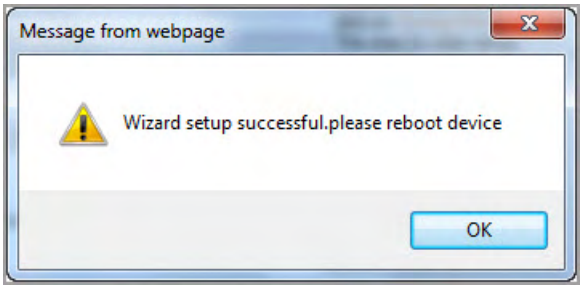


7. Select the **Security Mode**, **Authentication Type**, and **Encryption**, and enter a passphrase. Click **Next** to continue.

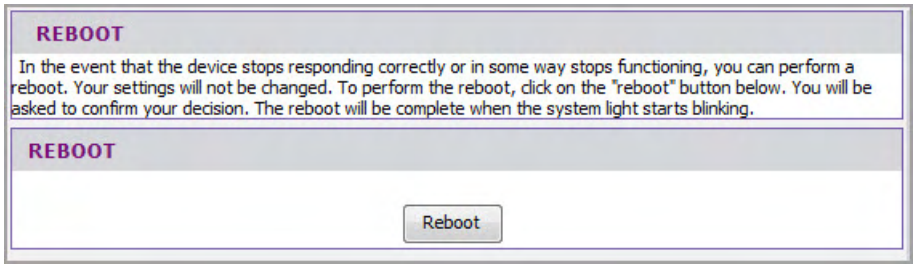
   The screen below varies depending on the security mode you selected, below is an example of a WPA security screen.



8. When prompted to reboot, click **OK**.



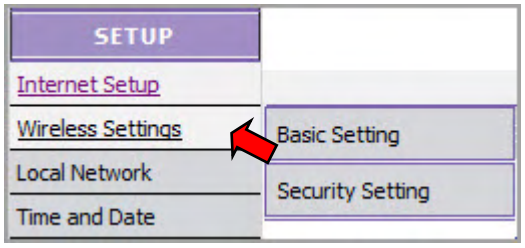
9. To reboot the Wireless Gateway, click **Reboot**.



4.2 Menu

Use the main menu, located on the left panel of the screen, to manually configure your Wireless Gateway. Click a menu item, then a submenu to display the page on the screen.

For submenus with more options, move the mouse cursor over the submenu to view the options.



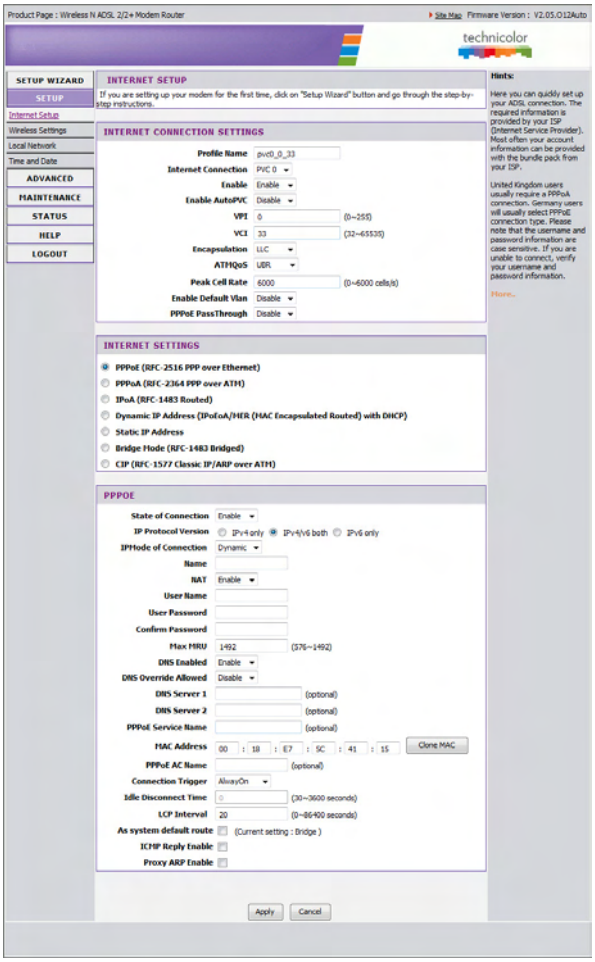
Chapter 5: Setup

The Setup menu allows you to configure the Internet connection of your Wireless Gateway manually.

5.1 Internet Setup

The Internet Setup page is divided into three sections: **Internet Connection Settings**, **Internet Settings**, and **Protocol**.

To access the Internet Setup page, click **SETUP** > **Internet Setup**.



5.1.1 Internet Connection Settings

This setting configures the Wireless Gateway to your Internet connection. The required settings should be obtained from your ISP.

Profile Name — Enter desired profile name.

Internet Connection — Select the Permanent Virtual Circuit (PVC). The Wireless Gateway supports up to 8 PVCs.

Enable — Select whether to enable or disable this Internet connection.

Enable AutoPVC — Select whether to automatically enable this Internet connection whenever needed.

VPI — Enter the Virtual Path Identifier (VPI) provided by your ISP. The default VPI is 0.

VCI — Enter the Virtual Channel Identifier (VCI)) setting provided by your ISP. The default VCI is 33.

Encapsulation — Select **LLC** (Logical Link Control) or **VCMUX** (Virtual Circuit Multiplexing), according to your ISP.

ATMQoS — Select the type of ATM Queue of Service (ATMQoS) specified by your ISP. Options are: **UBR** (Unspecified Bit Rate), **CBR** (Constant Bit Rate), **VBR-nrt** (Variable Bit Rate non-real-time), and **VBR+rt** (Variable Bit Rate real-time).

Peak Cell Rate — This is the maximum rate of cells that you can send. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.

Enable Default Vlan — Select whether to enable or disable VLAN tagging.

PPPoE PassThrough — Select whether to enable or disable PPPoE passthrough.

5.1.2 Internet Settings

DSL lines use different network protocols to establish Internet connection. Ask your ISP and select the protocol used by your DSL line, options are:

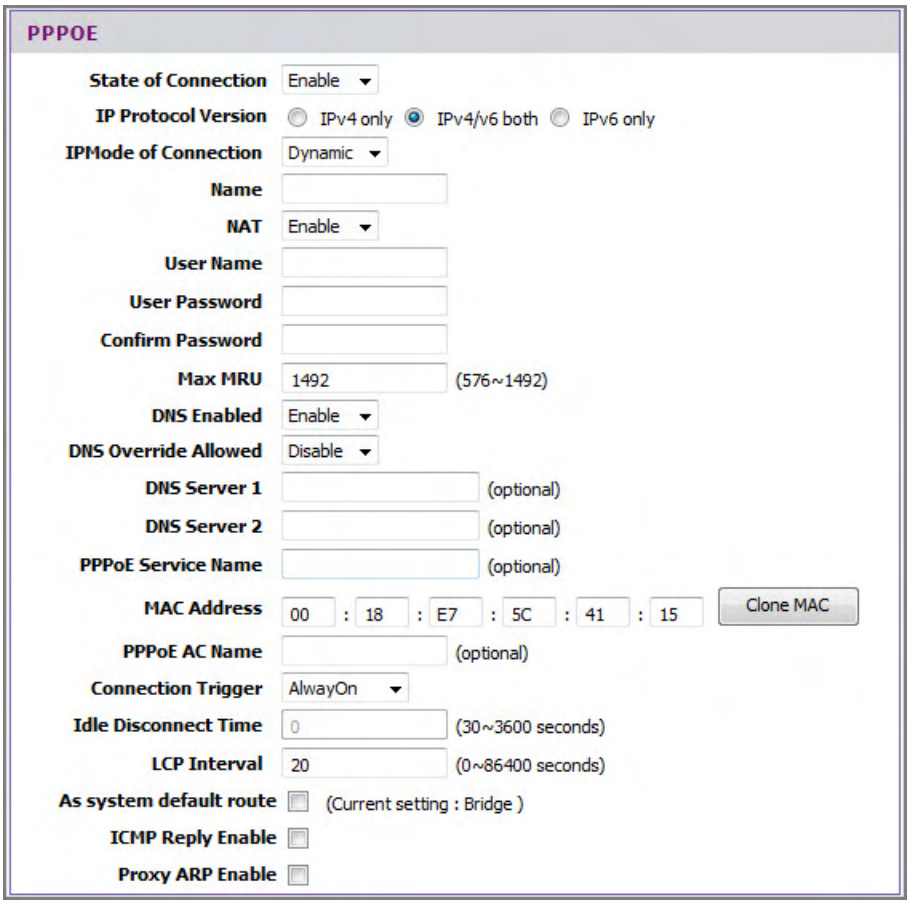
- PPPoE (RFC-2516 PPP over Ethernet)
- PPPoA (RFC-2364 PPP over ATM)
- IPoA (RFC-1483 Routed)
- Dynamic IP Address (IPoEoA/MER (MAC Encapsulated Routed) with DHCP)
- Static IP Address
- Bridge Mode (RFC-1483 Bridged)
- CIP (RFC-1577 Classic IP/ARP over ATM)

5.1.3 Protocol

This section varies depending on the selected network protocol.

PPPoE (RFC-2516 PPP over Ethernet)

If you select PPPoE (Point-to-Point Protocol over Ethernet), the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

IPMode of Connection — Select the connection mode, options are:

- **Dynamic**: Select Dynamic if the IP address can be automatically obtained from your ISP.
- **Static**: Select Static if you are required to use a permanent IP address to connect to the Internet. You must enter the **IP Address** and **Subnet Mask** provided by your ISP.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

User Name — Enter the user name provided by your ISP.

User Password — Enter the password provided by your ISP. Re-enter the password in the **Confirm Password** field.

Max MRU — This is the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

PPPoE Service Name — Enter a PPPoE service name.

MAC Address — Displays the cloned MAC address. Click the **Clone Mac** button to clone the MAC address of your computer.

PPPoE AC Name — Enter the PPPoE account name provided by your ISP.

Connection Trigger — You can configure how you want your Wireless Gateway to connect and terminate the Internet connection. Options are:

- **OnDemand**: Enables the Wireless Gateway to cut off the Internet connection after being idle for a specified period of time. The Wireless Gateway automatically re-establishes the connection when you try to access the Internet again. On the **Idle Disconnect Time** field, enter the number of seconds that you want to elapse before your Wireless Gateway terminates the Internet connection.
- **AlwaysOn**: Enables the Wireless Gateway to be connected to the Internet at all times. If you are disconnected, the Wireless Gateway will automatically re-establish the connection.
- **Manual**: With this setting, you have to enter the user name and password to establish the Internet connection.

LCP Interval — Enter the number of seconds that you want to be the interval in sending LCP (Link Control Protocol) packets.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

Proxy ARP Enable — Check this box to enable proxy ARP function.

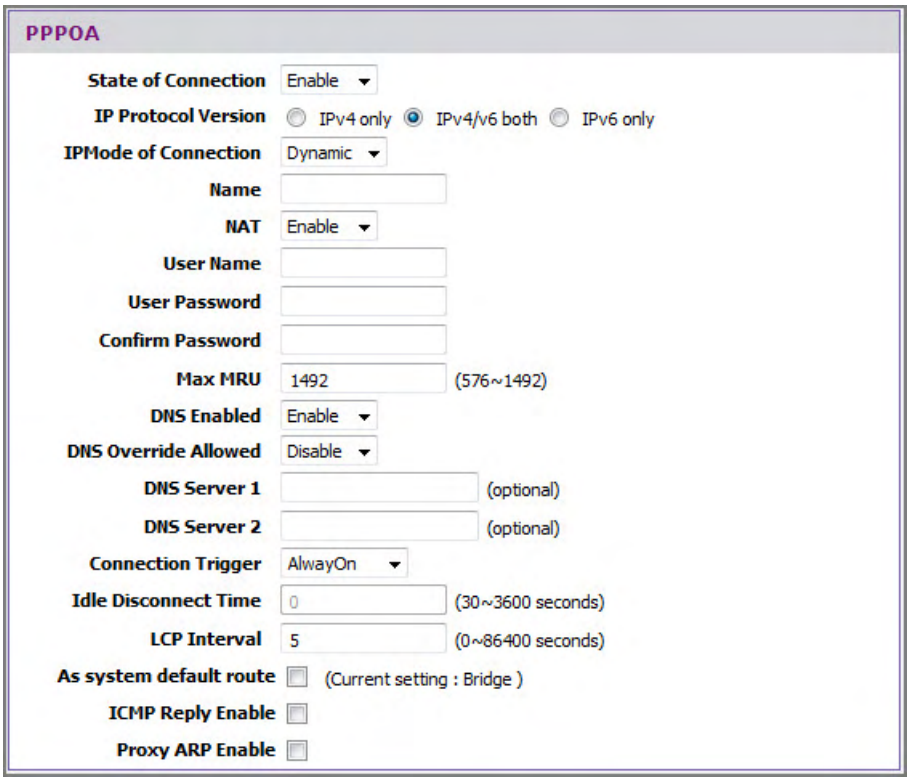
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

NOTE:

If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

PPPoA (RFC-2364 PPP over ATM)

If you select **PPPoA** (Point-to-Point Protocol over ATM), the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

IPMode of Connection — Select the connection mode, options are:

- **Dynamic**: Select Dynamic if the IP address can be automatically obtained from your ISP.
- **Static**: Select Static if you are required to use a permanent IP address to connect to the Internet. You must enter the **IP Address** and **Subnet Mask** provided by your ISP.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

User Name — Enter the user name provided by your ISP.

User Password — Enter the password provided by your ISP. Re-enter the password in the **Confirm Password** field.

Max MRU — This is the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

Connection Trigger — You can configure how you want your Wireless Gateway to connect and terminate the Internet connection. Options are:

- **OnDemand**: Enables the Wireless Gateway to cut off the Internet connection after being idle for a specified period of time. The Wireless Gateway automatically re-establishes the connection when you try to access the Internet again. On the **Idle Disconnect Time** field, enter the number of seconds that you want to elapse before your Wireless Gateway terminates the Internet connection.
- **AlwaysOn**: Enables the Wireless Gateway to be connected to the Internet at all times. If you are disconnected, the Wireless Gateway will automatically re-establish the connection.
- **Manual**: With this setting, you have to manually restore the connection if you are disconnected.

LCP Interval — Enter the number of seconds that you want to be the interval in sending LCP (Link Control Protocol) packets.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

Proxy ARP Enable — Check this box to enable proxy ARP function.

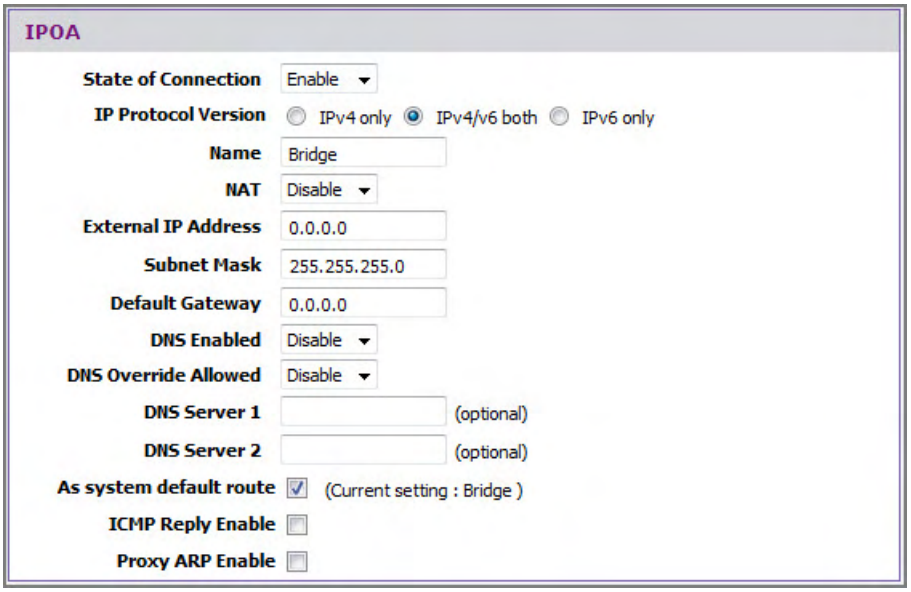
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

NOTE:

If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

IPoA (RFC-1483 Routed)

If you select **IPoA** (IP over ATM), the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

External IP Address — Enter the IP address provided by your ISP.

Subnet Mask — Enter the subnet mask provided by your ISP.

Default Gateway — Enter the default gateway provided by your ISP.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

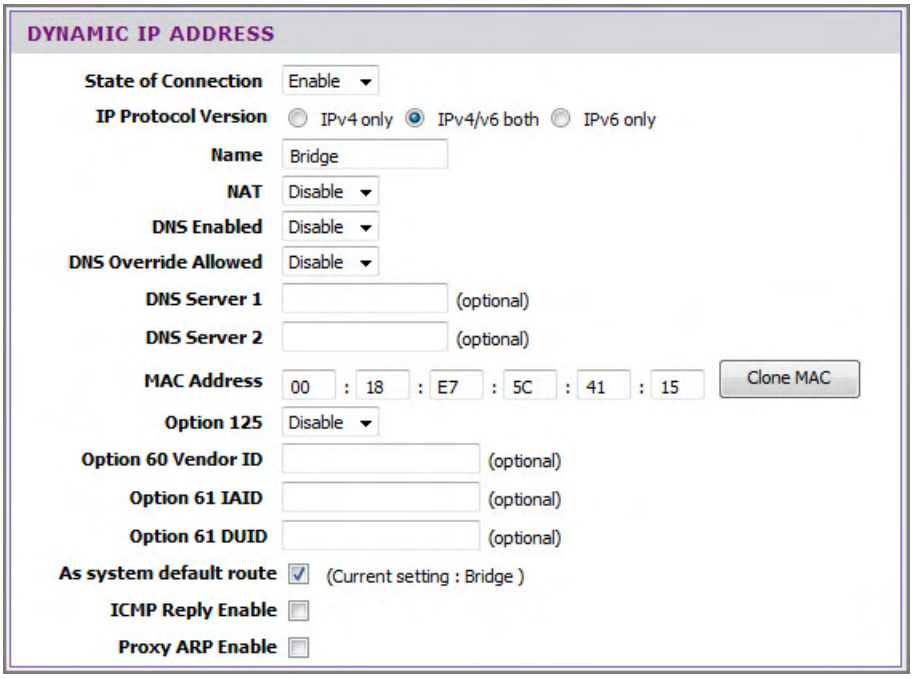
Proxy ARP Enable — Check this box to enable proxy ARP function.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

> **NOTE:**
>
> If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

Dynamic IP Address

If you select **Dynamic IP Address (IPoEoA/MER (MAC Encapsulated Routed) with DHCP)**, the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

MAC Address — Displays the cloned MAC address. Click the **Clone Mac** button to clone the MAC address of your computer.

Option 125 — Select whether to enable or disable Option 125.

Option 60 Vendor ID — Enter option 60 vendor ID.

Option 61 IAID — Enter option 61 IAID.

Option 61 DUID — Enter option 61 DUID.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

Proxy ARP Enable — Check this box to enable proxy ARP function.

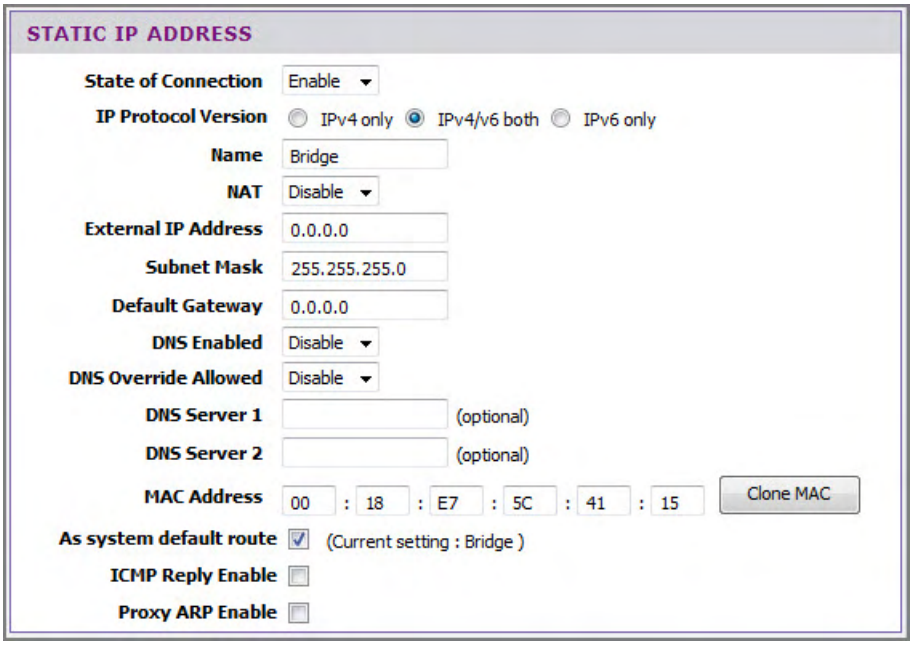
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

NOTE:

If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

Static IP Address

If you select **Static IP Address**, the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.

- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

External IP Address — Enter the IP address provided by your ISP.

Subnet Mask — Enter the subnet mask provided by your ISP.

Default Gateway — Enter the default gateway provided by your ISP.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

MAC Address — Displays the cloned MAC address. Click the **Clone Mac** button to clone the MAC address of your computer.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

Proxy ARP Enable — Check this box to enable proxy ARP function.

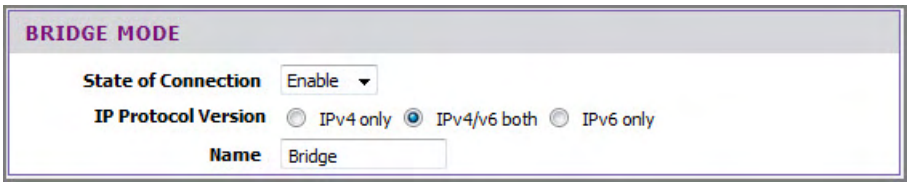
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

NOTE:

If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

Bridge Mode

If you select **Bridge mode (RFC-1483 Bridged)**, the screen below is displayed.



State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

Name — Enter your desired connection name.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

> **NOTE:**
>
> If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

CIP (RFC-1577)

If you select **CIP (RFC-1577 Classic RP/ARP over ATM)**, the screen below is displayed.

State of Connection — Select whether to enable or disable this connection.

IP Protocol Version — Select the type of IP protocol to use with this connection:

- **IPv4 only**: Select to use IPv4 protocol.
- **IPv4/v6 both**: Select to use this connection in both IPv4 and IPv6 protocols.
- **IPv6 only**: Select to use IPv6 protocol.

Name — Enter your desired connection name.

NAT — Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.

External IP Address — Enter the IP address provided by your ISP.

Subnet Mask — Enter the subnet mask provided by your ISP.

Default Gateway — Enter the default gateway provided by your ISP.

DNS Enabled — Select whether to enable or disable DNS (Domain Name System).

DNS Override Allowed — Select whether to enable or disable DNS override.

DNS Server 1 and **DNS Server 2** — If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

As system default route — Check this box to set the current setting as the default route.

ICMP Reply Enable — Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.

Proxy ARP Enable — Check this box to enable proxy ARP function.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

> **NOTE:**
>
> If the IPv6 protocol is selected, the web utility may prompt for you to configure the IPv6 connection settings. See "IPv6 WAN" on page 48.

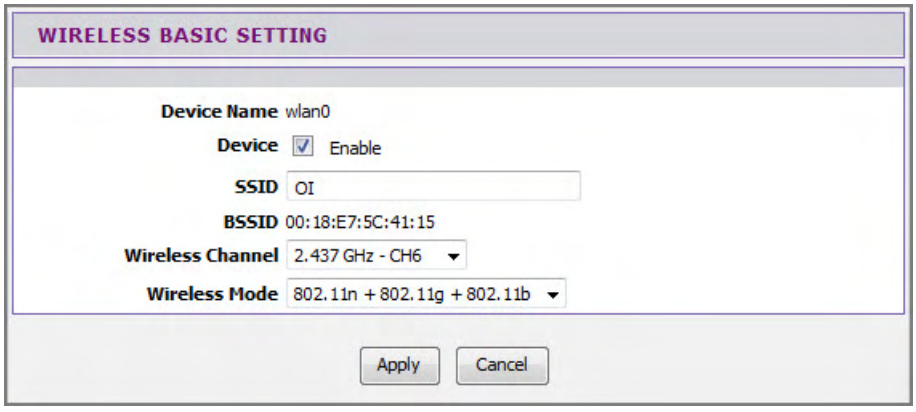
5.2 Wireless Settings

The Wireless Settings page allows you to enable and configure wireless connections.

5.2.1 Basic Setting

The Basic Settings page allows you to enable the wireless function of your Wireless Gateway and set its SSID.

To access the Basics Settings page, click **SETUP** > **Wireless Settings** > **Basic Setting** or click the **Wireless Setting** button.



Device — Check this box to enable the wireless function of your Wireless Gateway.

SSID – Enter the service set identifier (SSID) or the name of your wireless network. The SSID is case-sensitive and must not exceed 32 alphanumeric characters.

BSSID — (Basic Service Set Identifier) Displays the MAC address of your Wireless Gateway.

Wireless Channel — Select the appropriate channel that corresponds to your network settings. You should assign different channels for each access point to avoid signal interference.

TIP:

Select **Auto** for Wireless Channel to allow your Wireless Gateway to select the best possible channel for your wireless network.

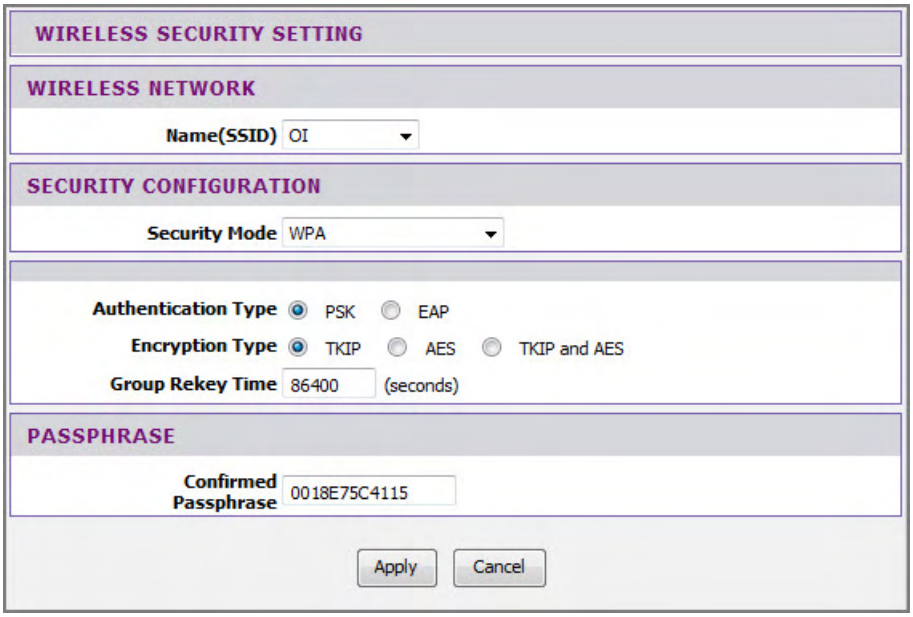
Wireless Mode — Select the wireless mode to limit the type of wireless devices that can connect to the network. Options are:

- **802.11b only**: Only 802.11b wireless devices can connect to the network.
- **802.11g + 802.11b**: Only 802.11g and 802.11b wireless devices can connect to the network.
- **802.11g only**: Only 802.11g wireless devices can connect to the network.
- **802.11n + 802.11g + 802.11b**: All 802.11n, 802.11g, and 802.11b wireless devices can connect to the network.
- **802.11n only**: Only 802.11n wireless devices can connect to the network.

5.2.2 Security Setting

It is strongly recommended to enable the security settings to secure your network from unauthorized access. Use the Security Setting page to configure the type of security and encryption of your wireless network.

To access the Security Setting page, click **SETUP** > **Wireless Settings** > **Security Setting** or click the **Security Setting** button.

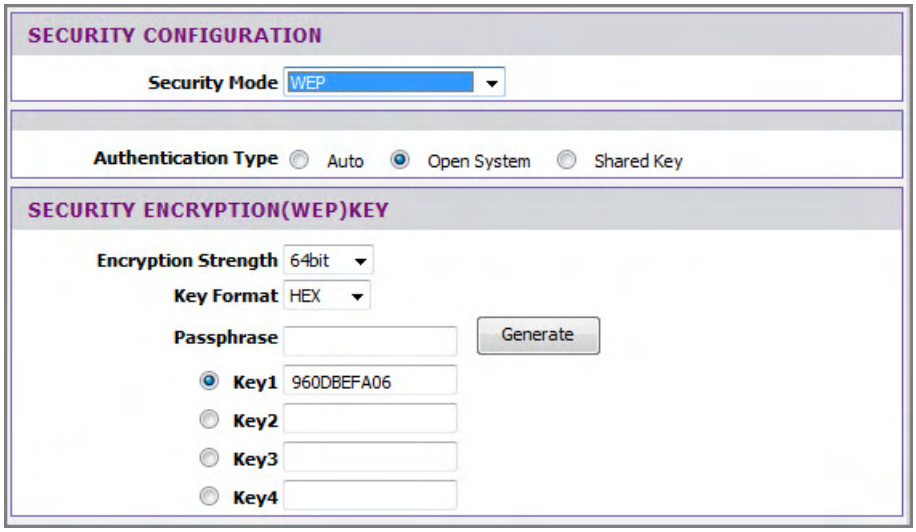


Name (SSID) — Select the wireless network that you want to configure. Aside from the main SSID, there are four virtual access points (VAP) that you can set the security separately (see “MBSSID Settings” on page 43).

Security Mode — Select the security and the encryption type to use. Select **None** if you do not want to use any security mode.

WEP

WEP (Wired Equivalent Privacy) is the basic security method. With WEP security, all wireless devices must enter the same key to connect to the network.



Authentication Type — Select an authentication type. Options are:

- **Auto**: Select Auto if you are unsure which authentication is suitable for your wireless devices.
- **Open System** — Open System allows public access to the Wireless Gateway via wireless communications.
- **Shared Key** — Requires users to enter the same WEP key to exchange data with other wireless devices.

Encryption Strength — Select **64bit** to enter or generate a 10-character key or select **128bit** to enter or generate a 26-character key.

Key Format — Select **HEX** to generate hexadecimal characters only or **ASCII** to generate ASCII characters.

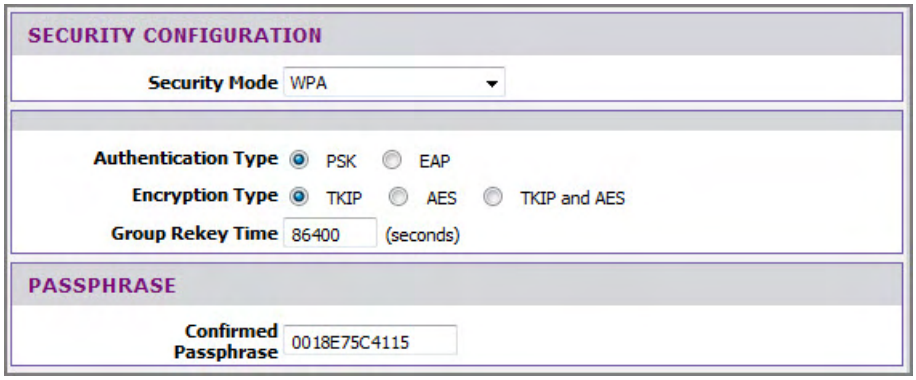
Passphrase — Enter a passphrase, then click the **Generate** button to automatically generate WEP keys.

Key 1, 2, 3, 4 — When you enter a passphrase and click the **Generate** button, these fields display the auto-generated keys. Otherwise, enter the WEP key(s) manually.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

WPA / WPA2

Select **WPA** (Wi-Fi Protected Access) or **WPA2** for better encryption.



Authentication Type — Select an authentication type. Options are:

- **PSK**: Select to use a passphrase for authentication.

  If you select **PSK**, enter a passphrase in the **Confirmed Passphrase** field.

- **EAP** — Select to use Extensible Authentication Protocol (EAP). This should only be used when a Radius server is connected to your Wireless Gateway.

  If you select EAP, enter the following information:

  - **Radius Server IP**: The IP address of the authentication server.
  - **Radius Server Port**: The port number used to connect to the authentication server.
  - **Radius Server Key**: Enter the passphrase that matches the authentication server.

Encryption Type — Select an encryption protocol:

- **TKIP**: Select to use the Temporal Key Integrity Protocol (TKIP).
- **AES**: Select to use Advanced Encryption Standard (AES).
- **TKIP and AES**: Select if you are unsure which protocol to use.

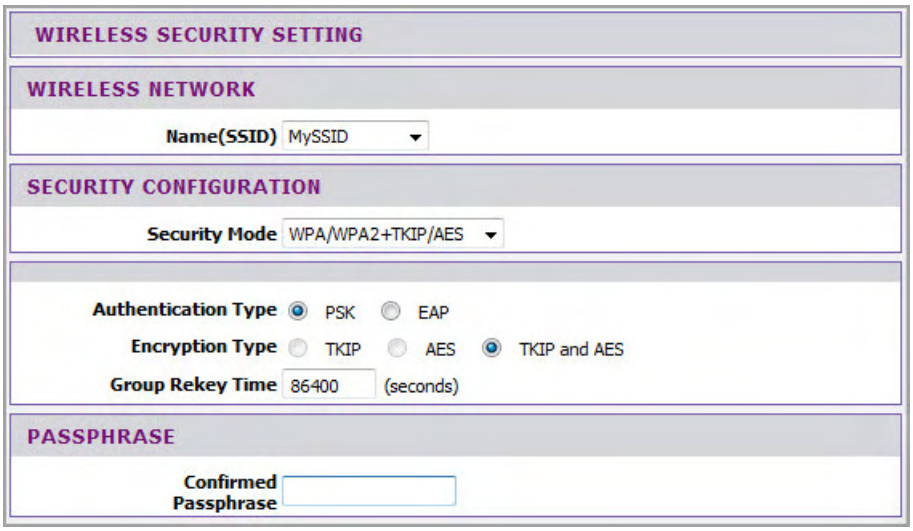
Group Rekey Time — Enter the number of seconds to elapse until the Wireless Gateway prompts for the key again.

Confirmed Passphrase — Enter the desired passphrase.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

WPA/WPA2+TKIP/AES

Select this security mode if you are unsure which mode is suitable for your wireless devices.



Authentication Type — Select an authentication type. Options are:

- **PSK**: Select to use a passphrase for authentication.

  If you select **PSK**, enter a passphrase in the **Confirmed Passphrase** field.

- **EAP**: Select to use Extensible Authentication Protocol (EAP). This should only be used when a Radius server is connected to your Wireless Gateway.

  If you select EAP, enter the following information:

  - **Radius Server IP**: The IP address of the authentication server.
  - **Radius Server Port**: The port number used to connect to the authentication server.
  - **Radius Server Key**: Enter the passphrase that matches the authentication server.

Encryption Type — **TKIP and AES** is automatically selected.

Group Rekey Time — Enter the number of seconds to elapse until the Wireless Gateway requires the wireless devices to re-authenticate.

Confirmed Passphrase — Enter the desired passphrase.

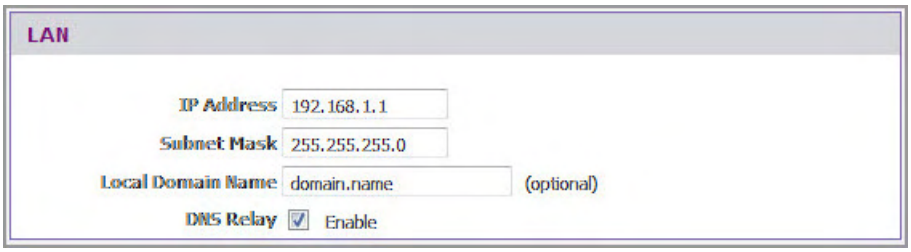
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

5.3 Local Network

To access the Local Network page, click **SETUP** > **Local Network**.

5.3.1 LAN

This section contains the local settings of your network. These settings are private to your internal network and cannot be seen on the Internet. It is recommended to keep the default values.



IP Address — The default value is 192.168.1.1.

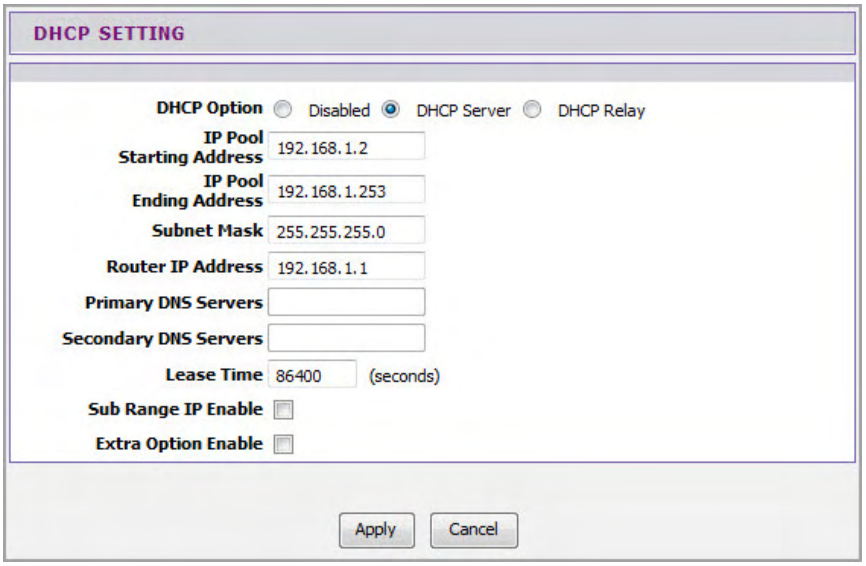
Subnet Mask — The default value is 255.255.255.0.

Local Domain Name — Enter a name to refer to the group of devices that will be assigned addresses from this pool.

DNS Relay — Select whether to enable or disable the DNS relay function. Check this box to request automatic assignment of a DNS, then enter the **Primary DNS Server** and the **Secondary DNS Server** in the DHCP Setting screen below.

5.3.2 DHCP Setting

This section allows you to configure your Wireless Gateway to use the Dynamic Host Configuration Protocol (DHCP). You can set your Wireless Gateway as a DHCP server or a DHCP relay agent of your network.



The information required on the DHCP Setting screen vary depending on the selected DHCP option.

DHCP Option — Select the DHCP mode of your Wireless Gateway. Options are:

- **Disabled**: Select this setting if there is already a DHCP server on your network and all devices on your network use static IP addresses.
- **DHCP Server**: By default, your Wireless Gateway is set as a DHCP server. See more details below.
- **DHCP Relay**: Select this setting to set your Wireless Gateway as a DHCP Relay agent. See description on the next page.

NOTE:

If you want to set your Wireless Gateway as a DHCP server, make sure there is no other DHCP server on your network.

DHCP Server

If you set your Wireless Gateway as the DHCP server, your Wireless Gateway will automatically assign an IP address to each computer on your network. By default, the fields for DHCP settings have predefined values. It is recommended to retain these values unless specified by your ISP.

IP Pool Starting Address — Enter the lowest range of IP address to assign. The default value is 192.168.1.2.

IP Pool Ending Address — Enter the highest range of IP address to assign. The default value is 192.168.1.253.

Subnet Mask — Enter the subnet mask. The default value is 255.255.255.0.

Router IP Address — Enter the IP address of your Wireless Gateway. The default value is 192.168.1.1.

Primary DNS Server and **Secondary DNS Server** — Enter a primary and a secondary DNS server if the **DNS Relay** option is disabled.

Lease Time — Enter the lease time in seconds. The lease time is the amount of time a device is allowed connection to your Wireless Gateway using its current dynamic IP address. At the end of the lease time, the lease is either renewed or a new IP address is assigned. The default value is 86400 seconds (1 day).

Sub Range IP Enable — Check this box to set another range of IP address.

- **Vendor Class (Option 60)**: Enter a vendor class name.
- **Sub-String Match**: Check to enable the sub-string match function.
- **IP Pool Starting Address** — Enter the lowest sub range of IP address to assign.
- **IP Pool Ending Address** — Enter the highest sub range of IP address to assign.
- **Subnet Mask** — Enter the subnet mask.
- **IPRouters** — Enter the IP address of your Wireless Gateway.

- **Primary DNS Server** and **Secondary DNS Server** — Enter a primary and a secondary DNS server of the sub range.

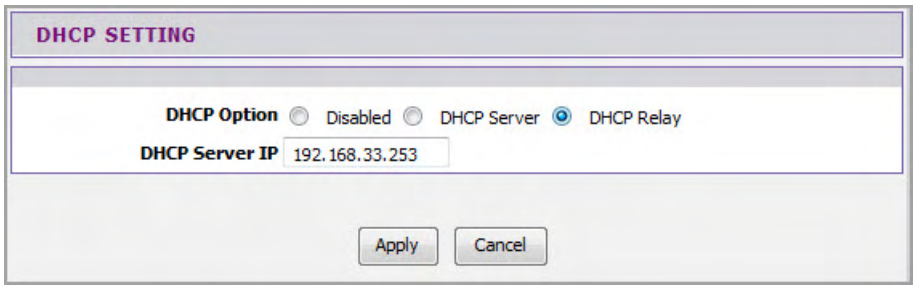
Extra Option Enable — Check this box to enable extra options.

- **Option 240**, **Option 241**, **Option 242**, **Option 243**, **Option 244**, and **Option 245**: Enter a name for the corresponding option.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

DHCP Relay

Some ISPs function as the DHCP server for their clients' small office network. In this case, you can set your Wireless Gateway to act as a DHCP relay agent. When a device on your network requests Internet access, your Wireless Gateway contacts the ISP to obtain the IP configuration, and then forwards the information to that device.

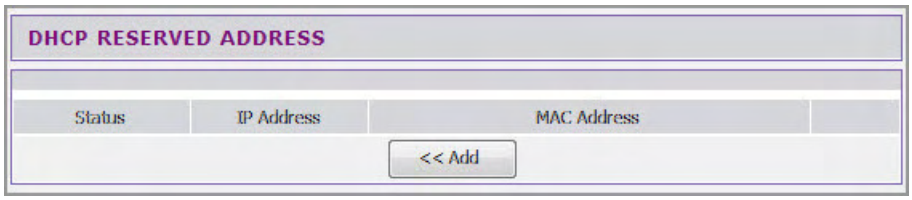


DHCP Server IP — Enter the IP address of the DHCP server.

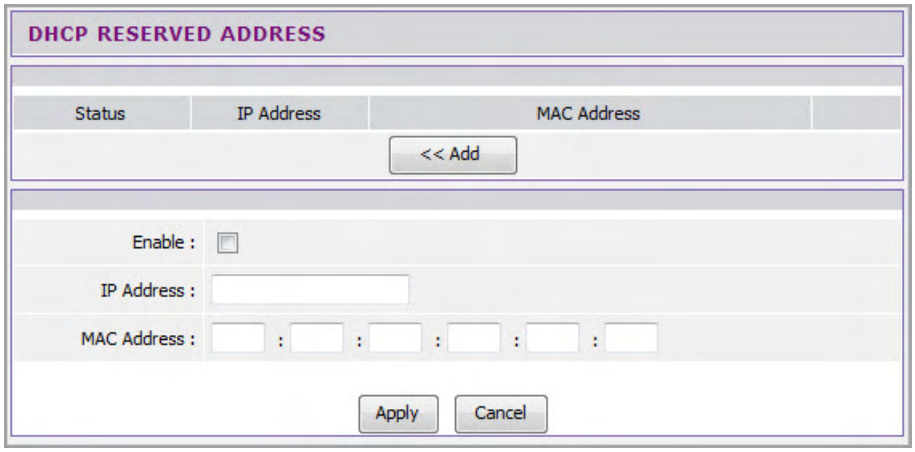
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

5.3.3 DHCP Reserved Address

This section lists the DHCP reserved addresses on your network. If your Wireless Gateway is set as the DHCP server, your Wireless Gateway can reserve a particular IP address to a specific device. To reserve an IP address, click the **Add** button.



Enable — Check this box to enable this function.



IP Address — Enter the IP address to reserve.

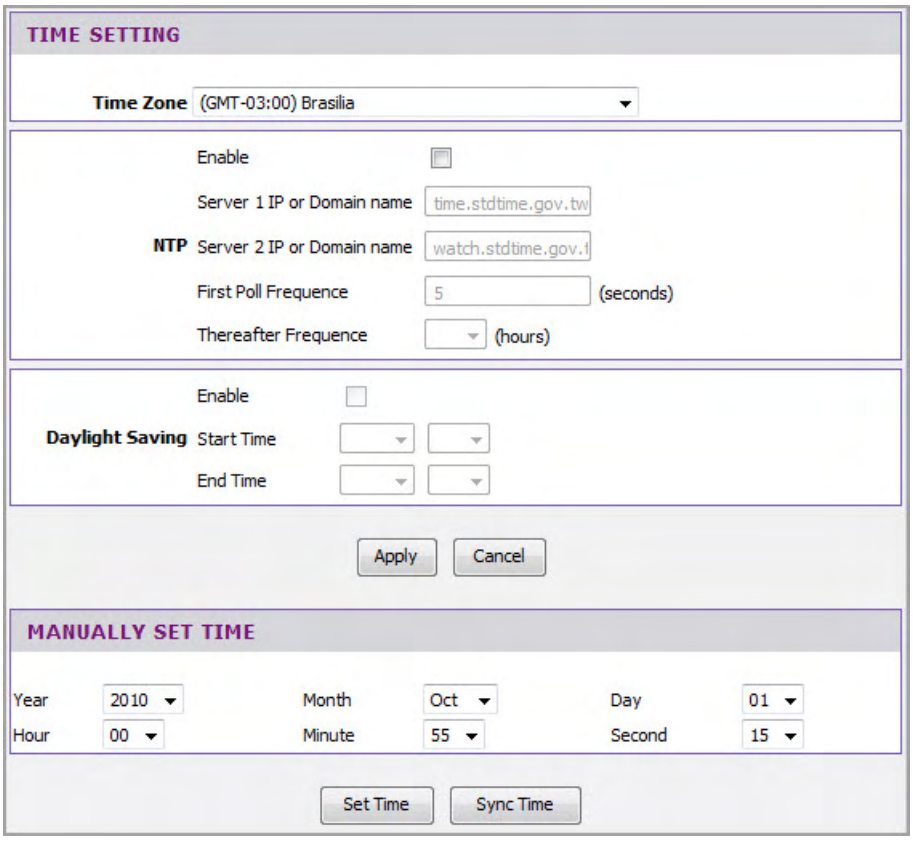
MAC Address — Enter the MAC address of the device to reserve the IP address to.

Click the **Apply** button to save your changes; the reserved IP address is listed on the DHCP Reserved Address table. Or, to discard changes, click the **Cancel** button.

5.4 Time and Date

The Time and Date page allows you to configure the time and date of your network by setting the time zone, synchronizing with a Network Time Protocol (NTP) server or manually set the time and date.

To access the Time and Date page, click **SETUP** > **Time and Date**.



Sync By Time Zone

Time Zone — Select the time zone in your location. To set the network time and date according to the selected time zone, click the **Sync Time** button at the bottom of the screen.

Sync With NTP Server

NTP (Network Time Protocol) — Check the **Enable** box to synchronize the network time and date with an NTP server.

- **Server 1 IP or Domain name**: Enter the IP address or the domain name of the NTP server to synchronize your network with.
- **Server 2 IP or Domain name**: Enter the IP address or the domain name of another NTP server to synchronize your network with in case Server 1 is not available.
- **First Poll Frequency**: Enter the number in seconds of the first poll.
- **Thereafter Frequency**: Select the succeeding frequency from the drop-down list.

Daylight Saving — Check the **Enable** box to enable daylight saving time.

- **Start Time**: Select the month and the day to start the daylight saving time.
- **End Time**: Select the month and the day to end the daylight saving time.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

Manual Setup

To manually set the time and date of your network, select the **Year**, **Month**, **Day**, **Hour**, **Minute**, and **Second** from their corresponding drop-down lists. Click the **Set Time** button to apply the changes.

Chapter 6: Advanced

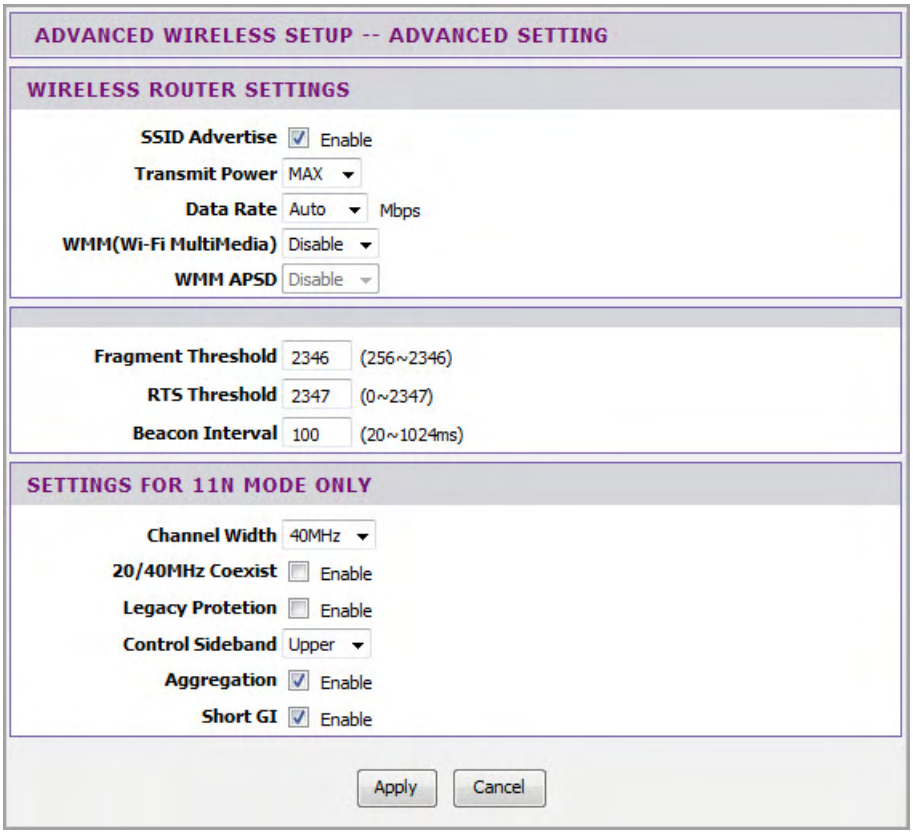
The Advanced menu configurations greatly affect the operating performance of your Wireless Gateway. This menu is intended for advance users. It is recommended to retain the default settings if you are unsure about them.

6.1 6.1 Advanced Wireless

6.1.1 Wireless Router Settings

This page allows you to configure advanced wireless router settings.

Click **Advanced** > **Advanced Wireless** > **Advanced Wireless** or click the **Advanced Setting** button.



SSID Advertise —Check this box to allow wireless devices scanning the area for wireless networks to detect your Wireless Gateway.

Transmit Power — Select the output power of the wireless LAN.

Data Rate — Select the data transmission rate.

WMM (Wi-Fi Multimedia) — Select whether to enable or disable WMM. The WMM feature enhances the Quality of Service (QoS) of a network that is used by multimedia applications such as Voice-over-IP (VoIP) and video. If WMM is enabled, multimedia applications on your network have priority over regular data packets, allowing multimedia applications to run smoother and with fewer errors.

WMM APSD — If WMM is enabled, you can also select whether to enable or disable WMM APSD (Automatic Power Save Delivery). APSD manages radio usage for battery-powered devices to allow longer battery life in certain conditions.

Fragment Threshold — Fragment threshold refers to the maximum size of a packet before data is fragmented into multiple packets. The default and recommended value is 2346 bytes. If you experience a high packet error rate, you may slightly adjust the value. Setting the fragment threshold too low may result in poor network performance.

RTS Threshold — The default and recommended value is 2347. Should you encounter inconsistent data flow, only slight modifications should be made.

Beacon Interval — Enter a value in milliseconds. A beacon is a packet that is sent out by the Wireless Gateway to synchronize the wireless network. The beacon interval value indicates the frequency interval of the beacon. The default value is 100.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

Settings for 11n Mode Only

The following settings are applicable only to wireless devices in the 802.11n mode.

Channel Width — Select the channel bandwidth: **20MHz** or **40MHz**.

20/40MHz Coexit — Check this box to enable both 20MHz and 40MHz channel bandwidth.

Legacy Protection — Check to enable legacy protection.

Control Sideband — Select to control **Upper** or **Lower** sideband.

Aggregation — Check to enable aggregation

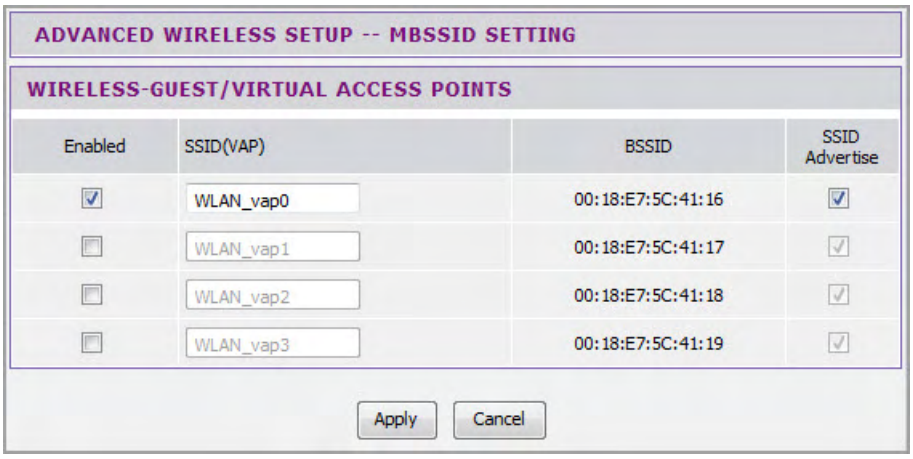
Short GI — Check to enable short guard interval (GI) function. Short GUI makes guard interval sending time shorter and thereby increases throughput.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.1.2 MBSSID Settings

This page allows you to configure up to four virtual access points (VAP).

Click **Advanced** > **Advanced Wireless** > **MBSSID Setting** or click the **MBSSID Setting** button.



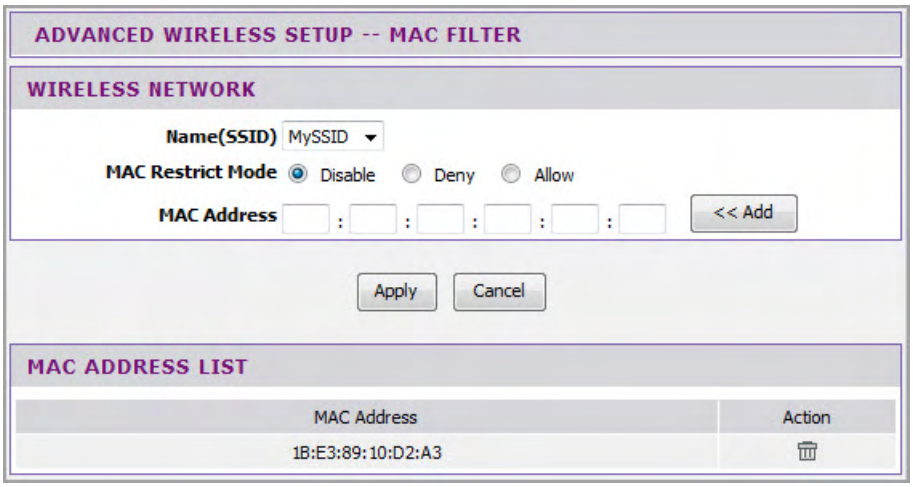
Check the corresponding **Enabled** box of the VAP to enable it. If you enable a VAP, you can modify its **SSID** and check its **SSID Advertise** box to allow wireless devices scanning for a wireless network to detect the VAP.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.1.3 Wireless MAC Filter

This page allows you to deny or allow devices to access the wireless network by filtering their MAC addresses.

Click **Advanced** > **Advanced Wireless** > **Wireless MAC Filter** or click the **MAC Filter** button.



Name (SSID) — Select the SSID from the drop-down list.

To Set MAC Filter

Do the following to deny or allow a device to access to the wireless network.

1. On the **MAC Address** field, enter the MAC address of the device that you want to deny or allow access.
2. Click the **Add** button to add the MAC address to the MAC ADDRESS LIST.
3. Select the **MAC Restrict Mode**. Options are:
   - **Disable**: No restriction or disable a previously set restriction.
   - **Deny**: To deny device to access to the wireless network.
   - **Allow**: To allow device to access to the wireless network.
4. Click the **Apply** button to apply the MAC filter or click the **Cancel** button to discard your changes.

To Remove MAC Filter

1. On the MAC ADDRESS LIST, click the icon to remove the device from the list of MAC addresses with restriction.
2. When prompted, click **OK** to confirm.

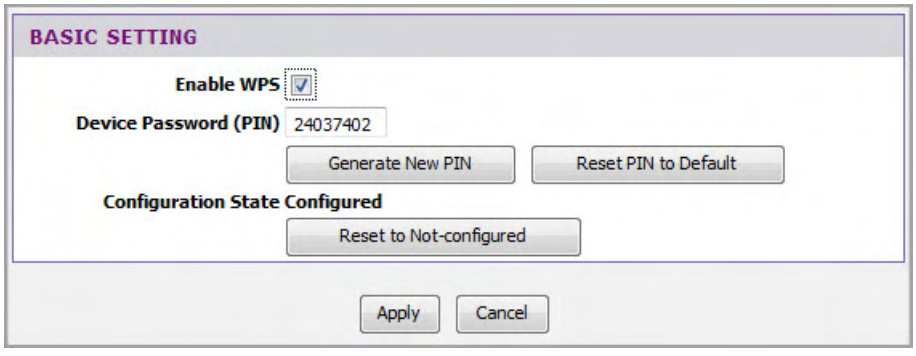
6.1.4 WPS Setting

Wi-Fi Protected Setup (WPS) is designed to make wireless setup easy and yet secure. Users do not need to know the network SSID and passphrases to use WPS to join the wireless network.

This page allows you to enable WPS-supported devices to connect to your Wireless Gateway.

> **NOTE:**
>
> This feature is available only WPA-PSK, WPA2PSK.

Click **Advanced** > **Advanced Wireless** > **WPS Setting** or click the **WPS Setting** button.



Enable WPS — Check this box to prompt WPS-enabled devices to enter the PIN before allowing access to the wireless network.

Device Password (PIN) — Displays the PIN password. To generate a new PIN, click the **Generate New PIN button**. To reset the PIN to default, click the **Reset PIN to Default** button. This PIN must be entered by wireless devices to connect to the wireless network.

To reset the WPS setting to not configured, click the **Reset to Not-configured** button.

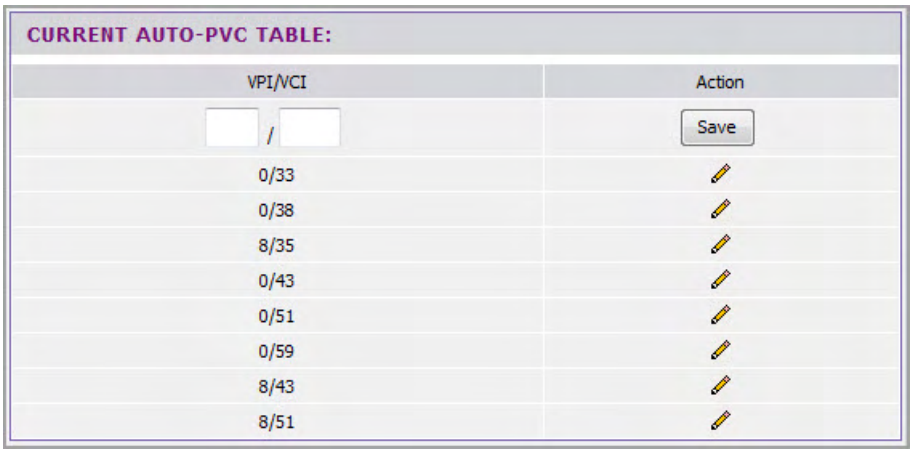
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.2 Multi-WAN

6.2.1 DSL Auto Scan

This page allows you to view and edit the VPI/VCI of the DSL line.

To access the DSL Auto Scan page, click **Advanced** > **Multi-WAN** > **DSL Auto Scan List** or click the **DSL Auto Scan List** button.



The CURRENT AUTO-PVC TABLE displays the current PVCs. Your Wireless Gateway supports up to 8 PVCs.

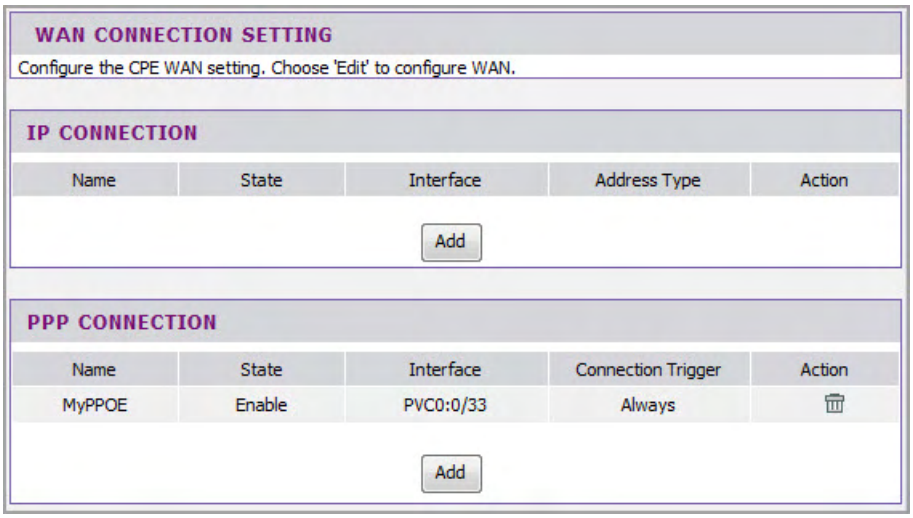
To modify an entry, do the following:

1. Click the icon. The selected entry is displayed on the editable field.
2. Enter the new VPI/VCI values.
3. Click the **Save** button.

6.2.2 IP/PPP Config

This page allows you to create multiple Wide Are Networks (WAN) and manually add an IP or a PPP connection.

To access the IP/PPP Config page, click **Advanced** > **Multi-WAN** > **IP/PPP Config** or click the **WAN Config** button.



To add an IP or PPP connection, do the following:

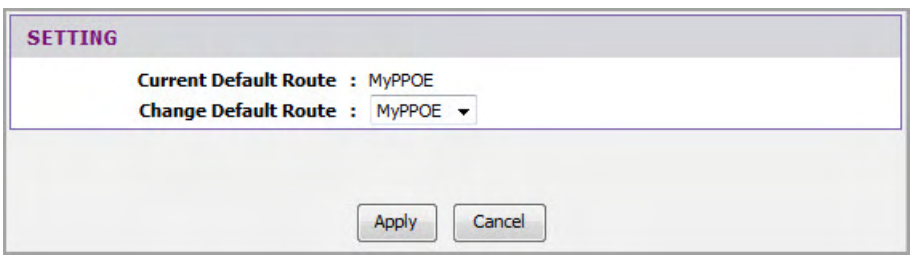
1. Click the **Add** button of the corresponding connection that you want to add. The connection screen appears; required settings vary depending on the type of connection that you want to add.
2. On the **Interface** field, select the PVC.
3. Enter the necessary connection settings. See “Protocol” on page 22 for connection configuration details.
4. Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

To delete an IP or PPP connection, click the corresponding icon.

6.2.3 Default Route

This page allows you to change the default route of your Wireless Gateway.

To access the Default Route page, click **Advanced** > **Multi-WAN** > **Default Route** or click the **Default Route** button.



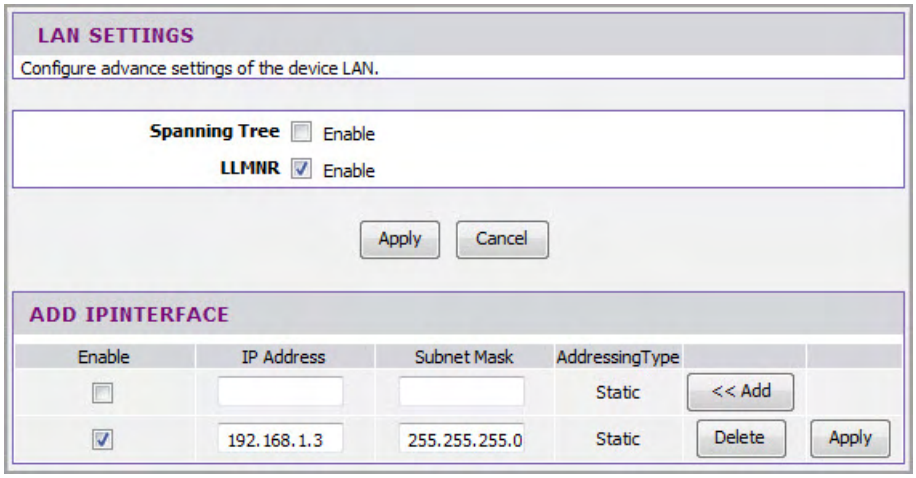
Change Default Route — Select the connection to set as the default route from the drop-down list.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.3 Advanced-LAN

This page allows you to add multiple LAN IP addresses of the Wireless Gateway.

To access the Advanced-LAN page, click **Advanced** > **Advanced-LAN**.



Spanning Tree Enable — Check this box to enable spanning tree.

LLMNR — Check this box to enable Link Local Multicast Name Resolution (LLMNR). When enabled, this allows both IPv4 and IPv6 hosts to perform name resolution for the names of neighboring computers without using a DNS server or DNS client configuration.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

Add IP Interface

To add an IP interface, do the following:

1. On the first record on the table, enter the **IP Address** and **Subnet Mask**.
2. Check the **Enable** box to enable the IP interface.
3. Click the **Add** button. The new entry is listed on the bottom of the list.

To apply the IP interface, click the corresponding **Apply** button.

To delete the IP interface, click the corresponding **Delete** button.

6.4 IPv6 WAN

This page allows you to configure IPv6 settings.

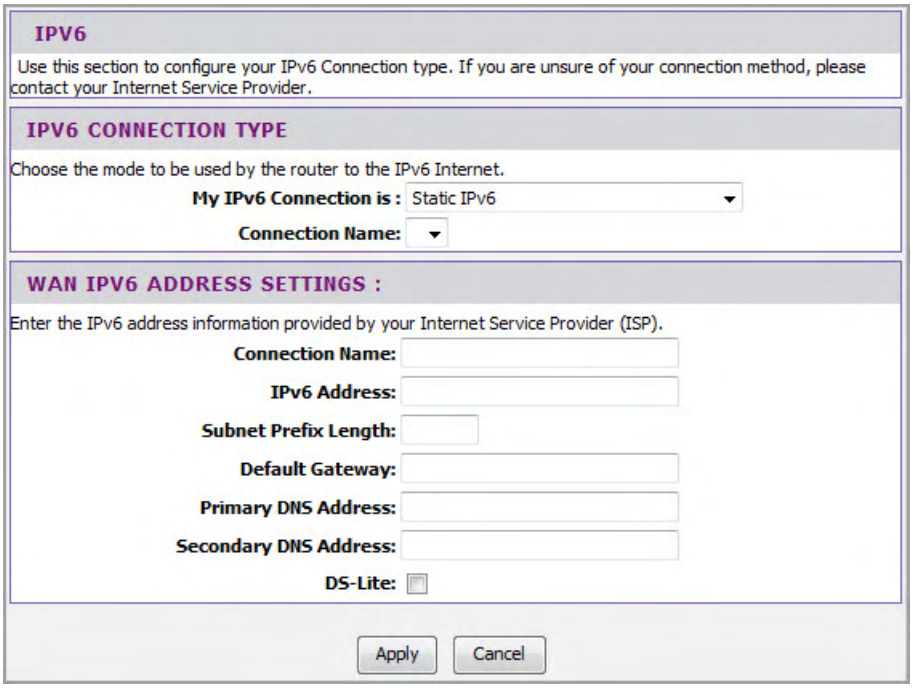
To access the IPv6 WAN page, click **Advanced** > **IPv6 WAN**.

The table lists the existing IPv6 connection settings. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding button.

To add a new connection, click the **Add** button. All required information must be obtained from your Internet Service Provider (ISP).

6.4.1 Static IPv6

On **My IPv6 Connection is**, select **Static IPv6**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

WAN IPv6 Address Settings

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

IPv6 Address — Enter the IPv6 IP address provided by your ISP.

Subnet Prefix Length — Enter the subnet prefix length provided by your ISP.

Default Gateway — Enter the gateway provided by your ISP.

Primary DNS Address and **Secondary DNS Address** — If provided by your ISP, enter the DNS server address. Otherwise, leave the fields blank.

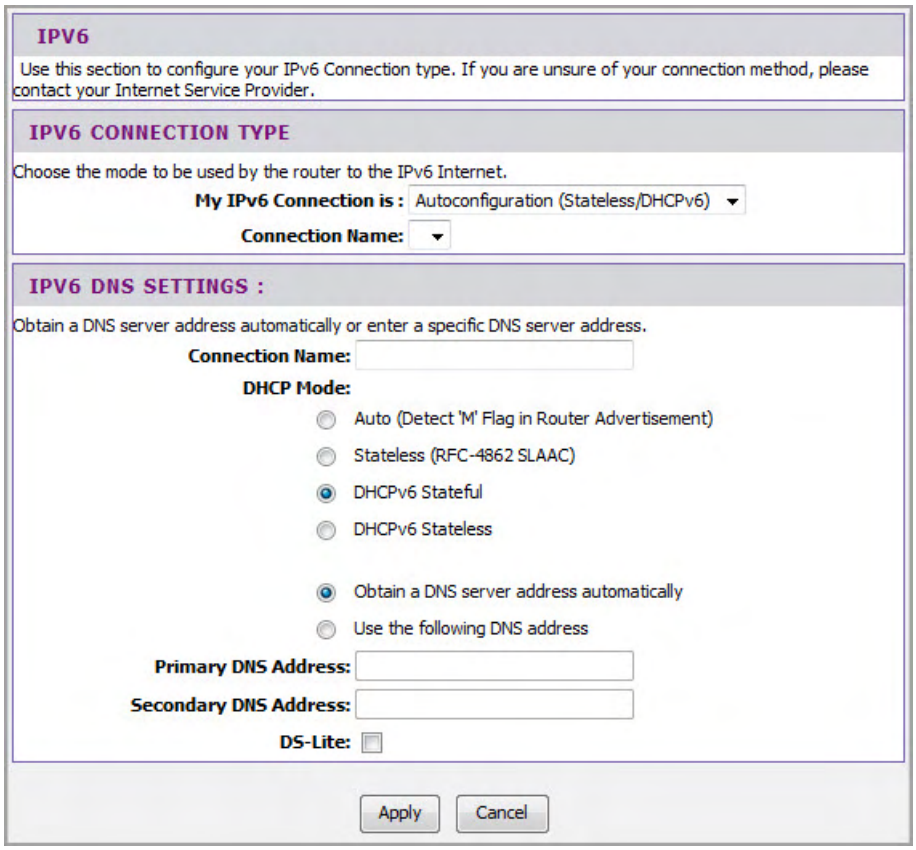
DS-Lite — Check this box to enable the Dual-Stack Lite (DS-Lite) function. DS-Lite is used to omit IPv4 address deployment from Customer-premises equipment (CPE) devices but instead use the global IPv6 address provided.

AFTR IPv6 Address — Enter an After Family Transition Router (AFTR) IPv6 address.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.4.2 Autoconfiguration (Stateless/DHCPv6)

On **My IPv6 Connection is**, select **Autoconfiguration (Stateless/DHCPv6)**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

IPv6 DNS Settings

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

DHCP Mode — Select the DHCP mode recommended by your ISP.

Obtain a DNS Server address automatically — Select to obtain the DNS sever automatically.

Use the following DNS address — Select to manually set the DNS Server addresses. When selected, enter the **Primary DNS Address** and **Secondary DNS Address** provided by your ISP.

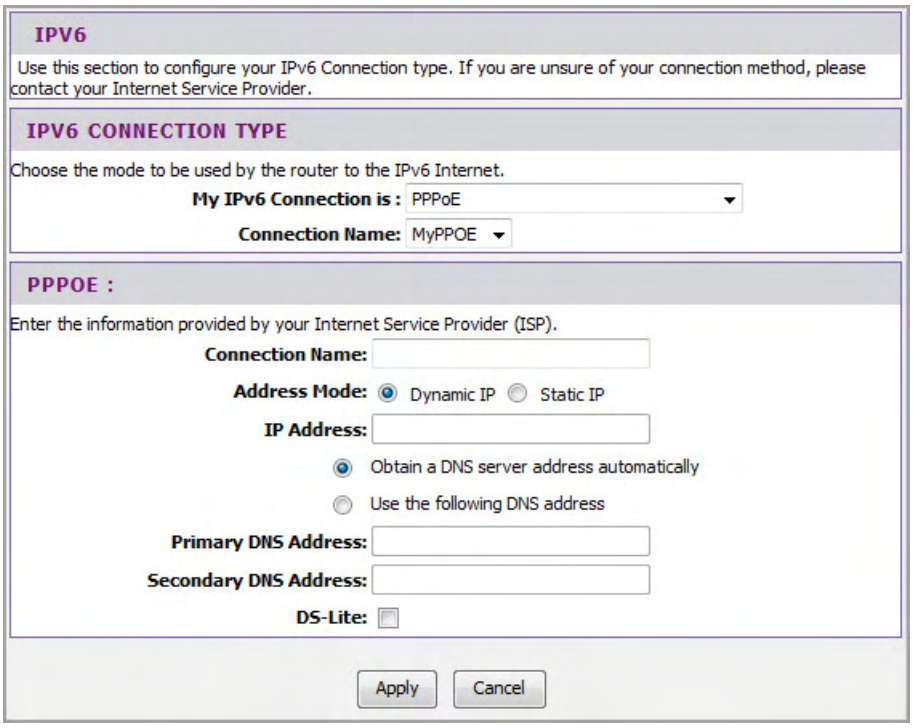
DS-Lite — Check this box to enable the Dual-Stack Lite (DS-Lite) function. DS-Lite is used to omit IPv4 address deployment from Customer-premises equipment (CPE) devices but instead use the global IPv6 address provided.

AFTR IPv6 Address — Enter an After Family Transition Router (AFTR) IPv6 address.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.4.3 PPPoE

On **My IPv6 Connection is**, select **PPPoE**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

PPPOE

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

Address Mode — Select **Dynamic IP** or **Static IP**.

IP Address — If the **Address Mode** is **Static IP**, enter the IP address.

Obtain a DNS Server address automatically — Select to obtain the DNS sever automatically. Available only if the **Address Mode** is **Dynamic IP**.

Use the following DNS address — Select to manually set the DNS Server addresses. When selected, enter the **Primary DNS Address** and **Secondary DNS Address** provided by your ISP.

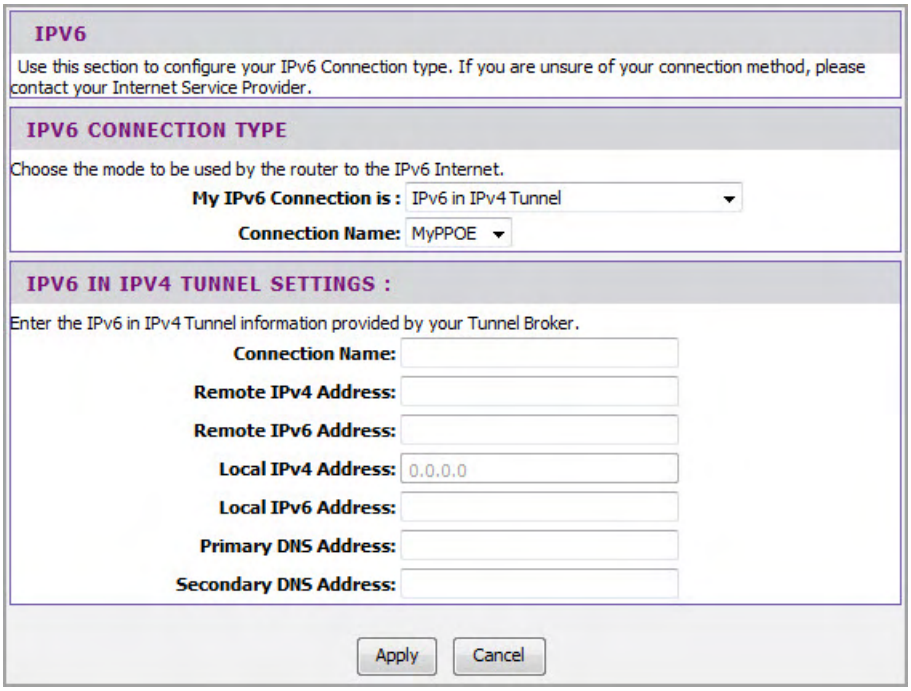
DS-Lite — Check this box to enable the Dual-Stack Lite (DS-Lite) function. DS-Lite is used to omit IPv4 address deployment from Customer-premises equipment (CPE) devices but instead use the global IPv6 address provided.

AFTR IPv6 Address — Enter an After Family Transition Router (AFTR) IPv6 address.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.4.4 IPv6 in IPv4 Tunnel

On **My IPv6 Connection is**, select **IPv6 in IPv4 Tunnel**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

IPv6 in IPv4 Tunnel Settings

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

Remote IPv4 Address — Enter the remote IPv4 address provided by your ISP.

Remote IPv6 Address — Enter the remote IPv6 address provided by your ISP.

Local IPv4 Address — Enter the local IPv4 address provided by your ISP.

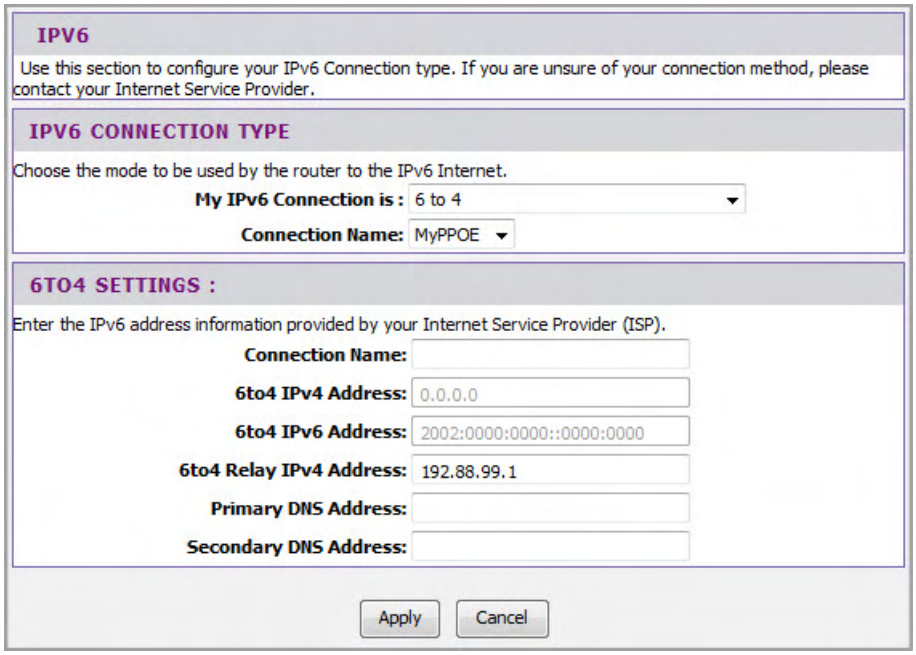
Local IPv6 Address — Enter the local IPv6 address provided by your ISP.

Primary DNS Address and **Secondary DNS Address** — If provided by your ISP, enter the DNS server address. Otherwise, leave the fields blank.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.4.5 6 to 4

On **My IPv6 Connection is**, select **6 to 4**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

6 To 4 Settings

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

6to4 IPv4 Address — Enter the 6 to 4 IPv4 address provided by your ISP.

6to4 IPv6 Address — Enter the 6 to 4 IPv6 address provided by your ISP.

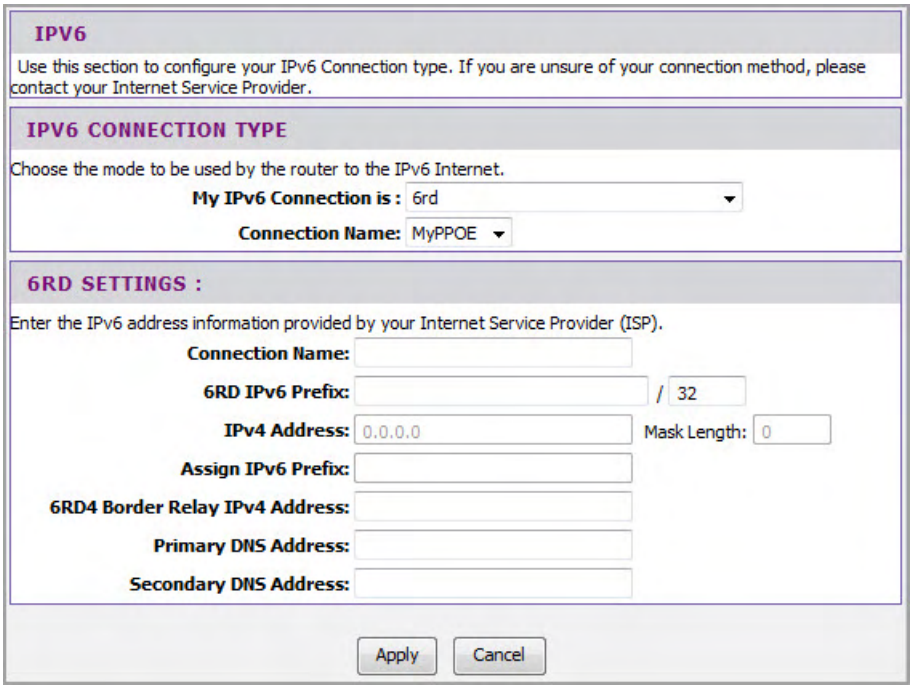
6to4 Relay IPv4 Address — Enter the 6 to 4 relay IPv4 address provided by your ISP.

Primary DNS Address and **Secondary DNS Address** — If provided by your ISP, enter the DNS server address. Otherwise, leave the fields blank.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.4.6 6rd

On **My IPv6 Connection is**, select **6rd**.



Connection Name — Select an Internet connection to use. This is the connection that you set up in **SETUP** > **Internet Setup** page. See "Internet Setup" on page 21.

6rd Settings

Connection Name — Enter the connection name provided by your ISP or a desired connection name.

6rd IPv6 Prefix — Enter the 6rd address and prefix provided by your ISP.

IPv4 Address — Enter the IPv4 address and **Mask Length** provided by your ISP.

Assign IPv6 Prefix — Enter the assigned IPv6 prefix provided by your ISP.

6RD4 Border Relay IPv4 Address — Enter the 6RD4 border relay IPv4 address provided by your ISP.

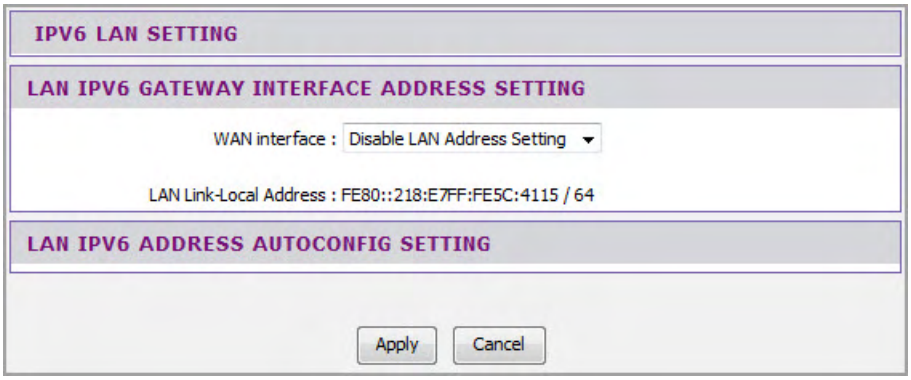
Primary DNS Address and **Secondary DNS Address** — If provided by your ISP, enter the DNS server address. Otherwise, leave the fields blank.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.5 IPv6 LAN

After creating IPv6 WAN, create IPv6 LAN to configure local IPv6 addresses.

To access the IPv6 WAN page, click **Advanced** > **IPv6 LAN**.

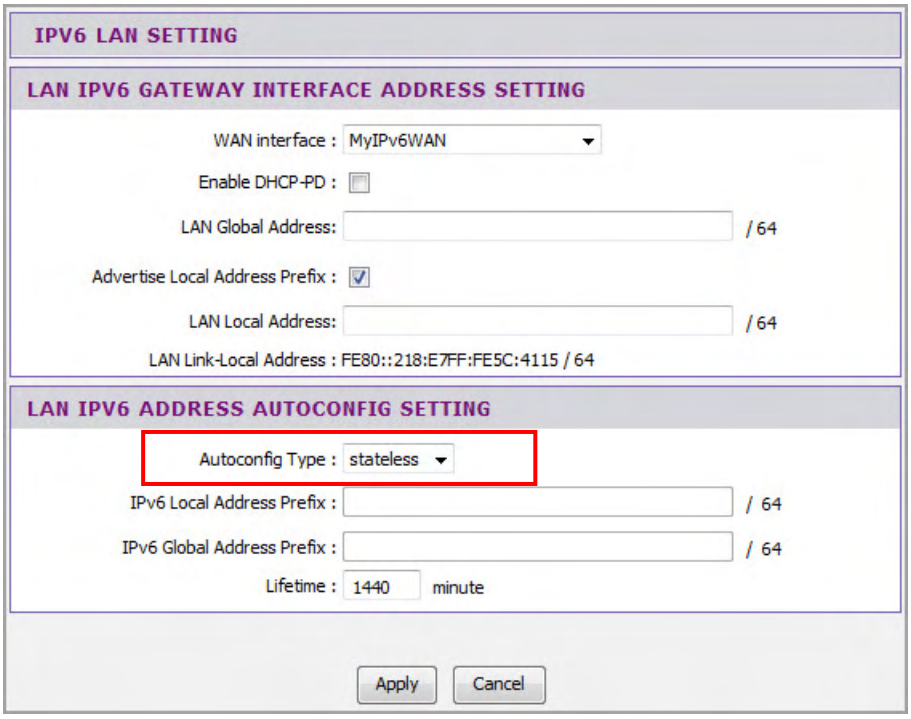


WAN Interface — Select the IPv6 WAN interface. This is the IPv6 interface that you created in **ADVANCED** > **IPv6 WAN** page. See "IPv6 WAN" on page 48.

LAN Link-Local Address — Displays the Wireless Gateway LAN Link-Local address.

6.5.1 IPv6 LAN Stateless

After selecting the **WAN interface**, on **Autoconfig Type**, select **stateless**. More fields appear. Available fields vary depending on the enabled features.



Enable DHCP-PD — Check this box to enable DHCP-PD feature.

LAN Global Address — Available only if DHCP-PD is disabled. Enter the Wireless Gateway LAN global address.

Advertise Local Address Prefix — Check this box to advertise the local address prefix.

LAN Local Address — Enter the Wireless Gateway LAN local address.

IPv6 Local Address Prefix — Enter the IPv6 local address prefix. Available only if **Advertise Local Address Prefix** is enabled.

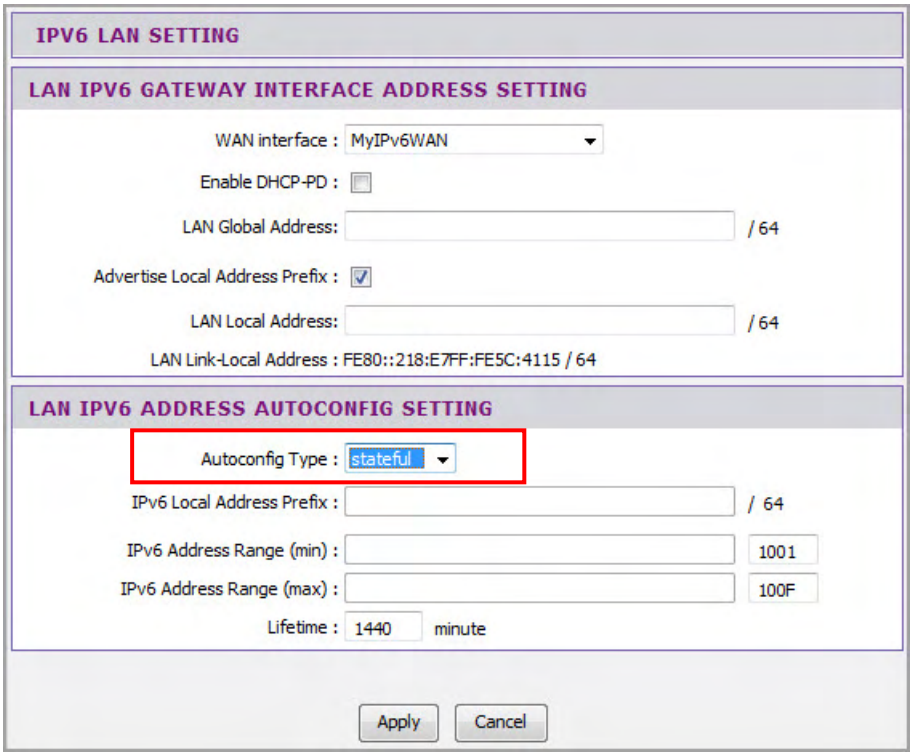
IPv6 Global Address Prefix — Enter the IPv6 global address prefix.

Lifetime — Enter the advertisement lifetime (in minutes).

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.5.2 IPv6 LAN Stateful

After selecting the **WAN interface**, on **Autoconfig Type**, select **stateful**. More fields appear. Available fields vary depending on the enabled features.



Enable DHCP-PD — Check this box to enable DHCP-PD feature.

LAN Global Address — Available only if DHCP-PD is disabled. Enter the Wireless Gateway LAN global address.

Advertise Local Address Prefix — Check this box to advertise the local address prefix.

LAN Local Address — Enter the Wireless Gateway LAN local address.

IPv6 Local Address Prefix — Enter the IPv6 local address prefix. Available only if **Advertise Local Address Prefix** is enabled.

IPv6 Address Range (min) — Enter the starting range of IPv6 address for your local computers.

IPv6 Address Range (max) — Enter the ending range of IPv6 address for your local computers.

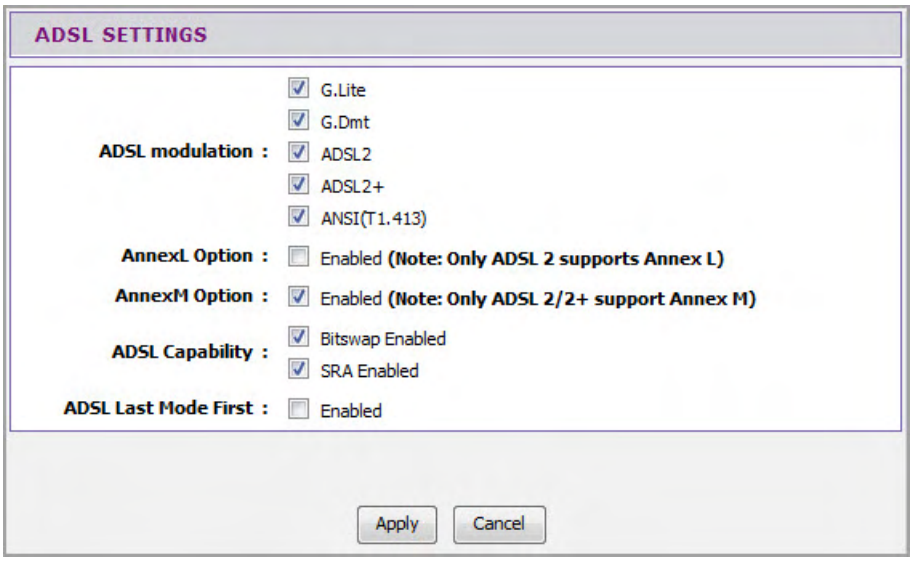
Lifetime — Enter the advertisement lifetime (in minutes).

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.6 ADSL Settings

This page allows you to select ADSL modulations, capabilities, and other options. Consult your ISP to determine the appropriate settings.

To access the ADSL Settings page, click **Advanced** > **ADSL Settings**.



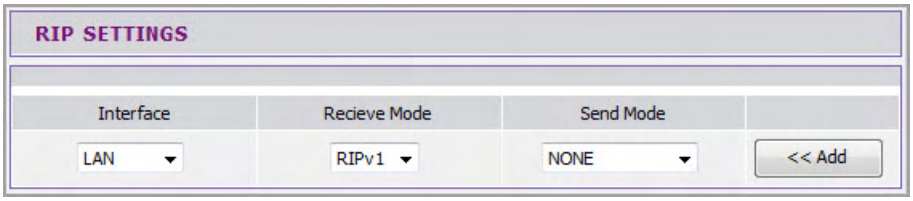
Check a corresponding box to select the option.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.7 RIP Settings

A Routing Information Protocol (RIP) is an Internet protocol that is used to share routing information table with other routing devices on the local and wide area network.

To access the RIP Settings page, click **Advanced** > **RIP Settings**.



To add RIP settings, do the following:

1. Select the **Interface**.
2. On the **Receive Mode** and **Send Mode** drop-down lists, select the appropriate versions.

> **NOTE:**
> The selected versions should match the versions supported by the other routers on your network.

3. Click the **Add** button.

To delete an RIP setting, click the corresponding button.

6.8 NAT

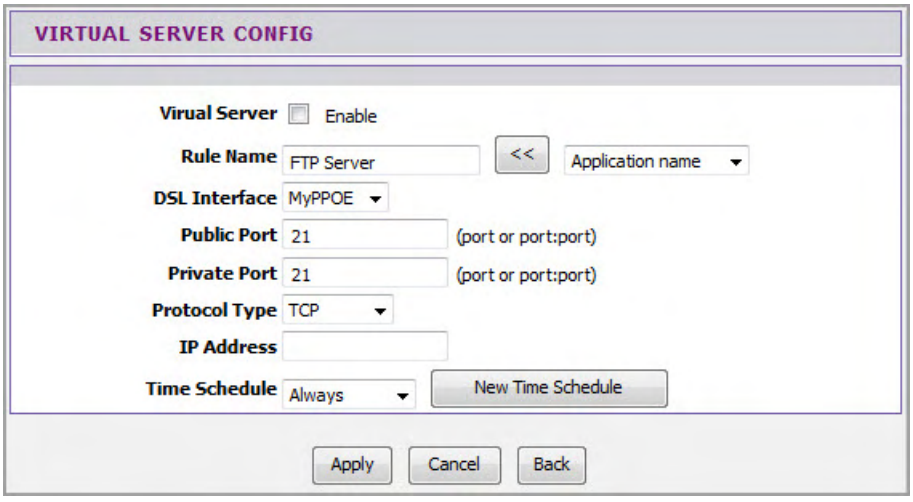
6.8.1 Virtual Server

A virtual server allows remote devices accessing the Web or FTP services via a public IP address be redirected to local servers in the LAN. Depending on the requested service (TCP/UDP port number), your Wireless Gateway redirects the external service request to the appropriate server in the LAN.

To access the Virtual Server page, click **Advanced** > **NAT** > **Virtual Server** or click the **Virtual Server** button.

The table displays the virtual servers on your network. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding button.

To add virtual servers, click the **Add** button. The Virtual Server Config screen is displayed.



Virtual Server — Check this box to enable the virtual server function.

Rule Name — Enter a rule name or select an application name from the drop-down list on the right, then click the **<<** button. If you select a predefined application name, the **Public Port**, **Private Port**, and **Protocol Type** are automatically configured.

DSL Interface — Select a DSL interface from the drop-down list.

Public Port — Enter the public port. This is the port seen from the WAN side.

Private Port — Enter the private port. This is the port being used by applications within your local network.

> **NOTE:**
>
> The public and private ports are usually the same.

Protocol Type — Select the protocol from the drop-down list.

IP Address — Enter the local network IP address of the system hosting the server.

Time Schedule — Select a schedule when to use the virtual server or click the **New Time Schedule** button to create a new schedule.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

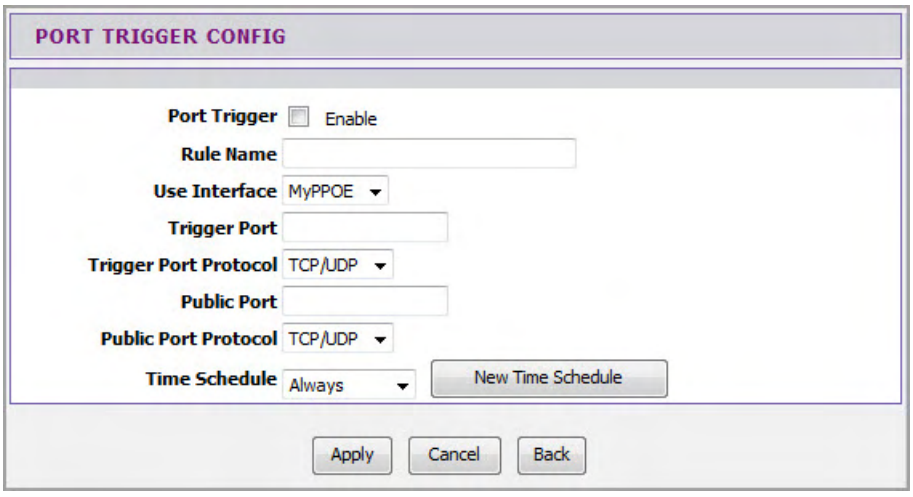
6.8.2 Port Trigger

This page allows you to add port trigger rules and displays the port trigger settings on your network. Port triggering is a type of port forwarding where outgoing data from specific ports are sent to specific incoming ports.

To access the Port Trigger page, click **Advanced** > **NAT** > **Port Trigger** or click the **Port Trigger** button.

The table displays the port triggers on your network. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding button.

To add port triggers, click the **Add** button. The Port Trigger Config screen is displayed.



Port Trigger — Check this box to enable port triggering.

Rule Name — Enter a rule name.

Use Interface — Select a DSL interface from the drop-down list.

Trigger Port — Enter the port that will trigger the device to open ports for incoming data.

Trigger Port Protocol — Select the trigger port protocol from the drop-down list.

Public Port — Enter the public port to be opened.

Public Port Protocol — Select the public port protocol.

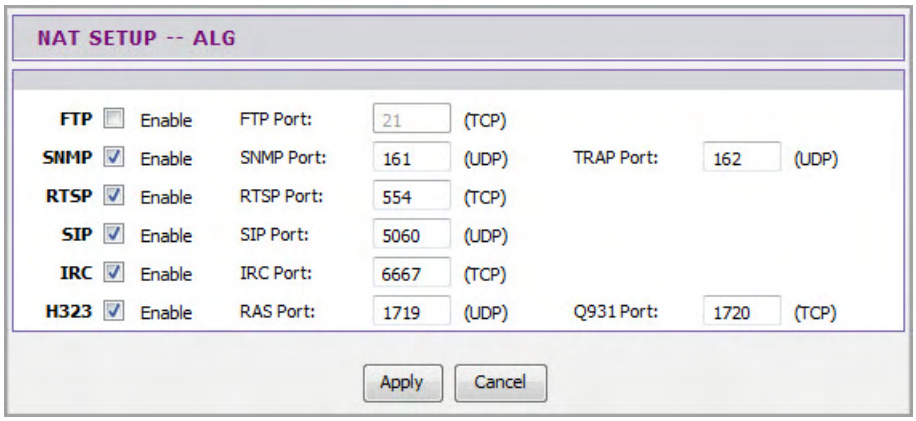
Time Schedule — Select a schedule to apply port triggering from the drop-down list or click the **New Time Schedule** button to create a new schedule.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.8.3 ALG

Application Layer Gateway (ALG) consists of a security component that augments NAT or a firewall. Your Wireless Gateway allows NATs to support address and port translation for certain application layer protocols such as FTP, SNMP, and others.

To access the ALG page, click **Advanced** > **NAT** > **ALG** or click the **ALG Setting** button.



FTP — File Transfer Protocol (FTP) is used to transfer files between computers on a TCP/IP based network, such as the Internet. Check this box to enable this function to work through your Wireless Gateway.

SNMP — Simple Network Management Protocol (SNMP) is a network protocol used to monitor the devices connected to a network. Check this box to enable this function to work through your Wireless Gateway.

RTSP — Real Time Streaming Protocol (RTSP) is a network protocol used for entertainment and communication systems to control streaming media sessions. Check this box to enable this function to work through your Wireless Gateway.

SIP — Session Initiation Protocol (SIP) is a signaling protocol used to control multimedia communication sessions such as voice and video calls over Internet Protocol (IP). Check this box to enable this function to work through your Wireless Gateway.

IRC — Internet Relay Chat (IRC) is a real-time Internet chatting protocol designed for group communications. Check this box to enable this function to work through your Wireless Gateway.

H323 — H.323 is a standard that provides audio-visual communication sessions on a network. It is widely implemented in voice and video conferencing equipments and is used within various Internet real-time applications such as NetMeeting. Check this box to enable this function to work through your Wireless Gateway.

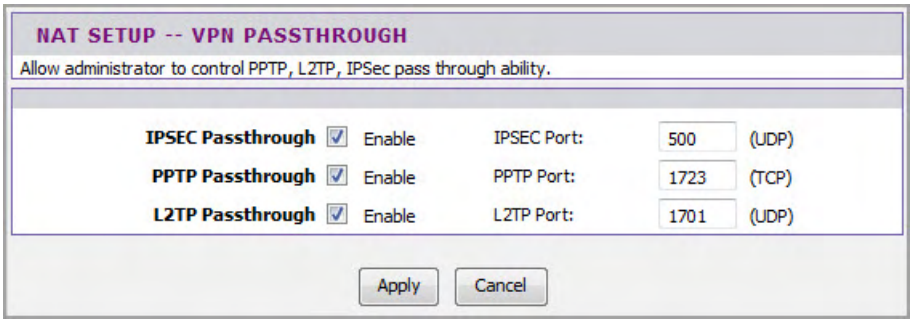
It is recommended to retain the default ports of these protocols.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.8.4 VPN Passthrough

This page allows you to control VPN tunnels using IPSEC, PPTP, and L2TP protocols to pass through your Wireless Gateway.

To access the VPN Passthrough page, click **Advanced** > **NAT** > **VPN Passthrough** or click the **VPN Setting** button.



IPSEC Passthrough — Internet Protocol Security (IPSec) is a protocol suite used to secure IP communications by authenticating and encrypting IP packets. Check this box to enable this function to work through your Wireless Gateway.

PPTP Passthrough — Point-to-Point Tunneling Protocol (PPTP) allows Point-to-Point protocol (PPP) to be tunneled through a network. Check this box to enable this function to work through your Wireless Gateway.

L2TP Passthrough — Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate VPNs. Check this box to enable this function to work through your Wireless Gateway.

It is recommended to retain the default ports of these protocols.

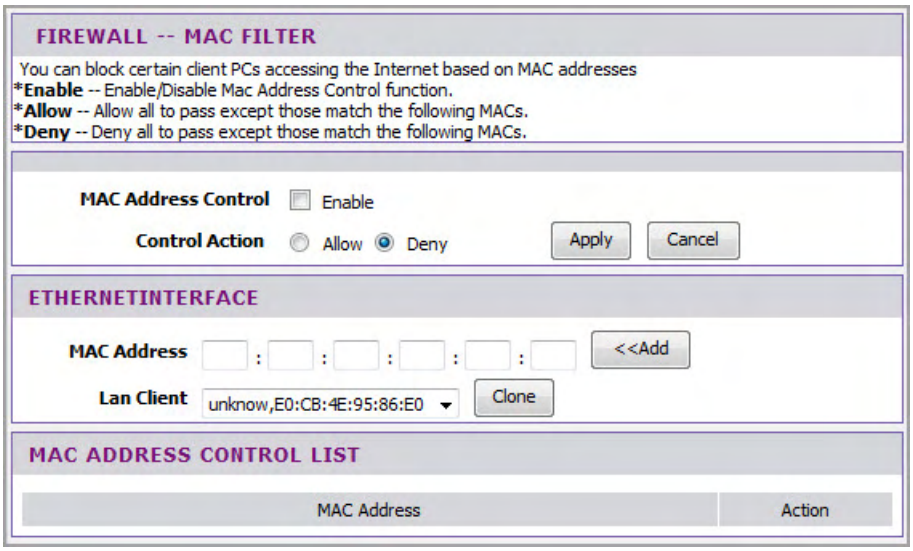
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.9 Firewall

6.9.1 MAC Filter

This page allows you to set up a list of MAC addresses which will be allowed or restricted to access the Internet.

To access the MAC Filter page, click **ADVANCED** > **Firewall** > **MAC Filter** or click the **MAC Filter** button.



MAC Address Control — Check this box to enable the MAC filter function.

Control Action — Select **Allow** to allow all clients to access the Internet except those MAC addresses specified below or select **Deny** to restrict all clients to access the Internet except those MAC addresses specified below.

Click the **Apply** button to save and activate the MAC filter or click the **Cancel** button to discard your changes.

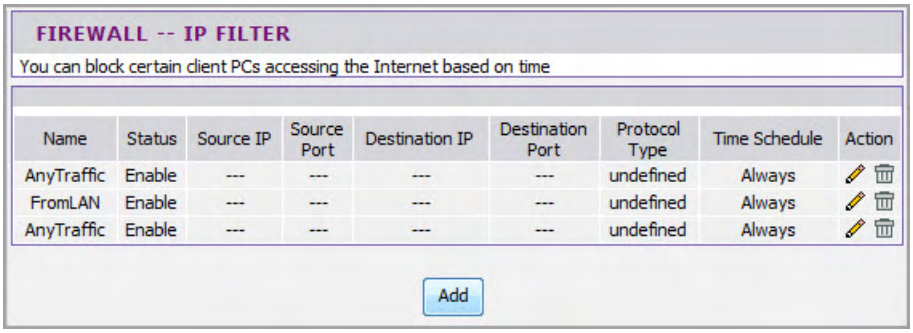
MAC Address — Enter the MAC address of the device you want to allow or deny access to the Internet. To use the MAC address of the DHCP client, click the **Clone** button. The MAC address is automatically copied to the MAC address field. Click the **Add** button to add the MAC address to the filter list.

The MAC ADDRESS CONTROL LIST displays the MAC address of the devices that are either allowed or denied access to the Internet. To remove an entry from the list, click the corresponding 🗑 button.

6.9.2 IP Filter

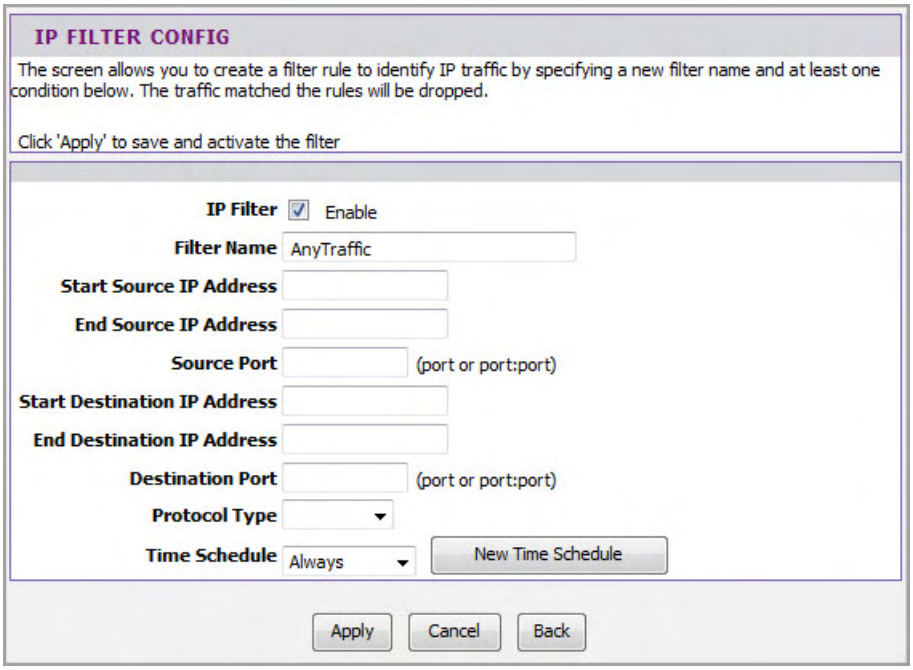
This page allows you to create filter rules to control outgoing traffic to the Internet based on a range of IP addresses and their protocols.

To access the IP Filter page, click **ADVANCED** > **Firewall** > **IP Filter** or click the **IP Filter** button.



The table lists the existing filter rules. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding button.

To add a filter, click the **Add** button. The IP Filter Config screen is displayed.



IP Filter — Check this box to enable IP filtering.

Filter Name — Enter a filter rule name.

Start Source IP Address — Enter the starting point of the source IP address.

End Source IP Address — Enter the ending point of the source IP address.

Source Port — Enter the source port number.

Start Destination IP Address — Enter the starting point of the destination IP address.

End Destination IP Address — Enter the ending point of the destination IP address.

Destination Port — Enter the destination port number.

Protocol Type — Select the protocol from the drop-down list.

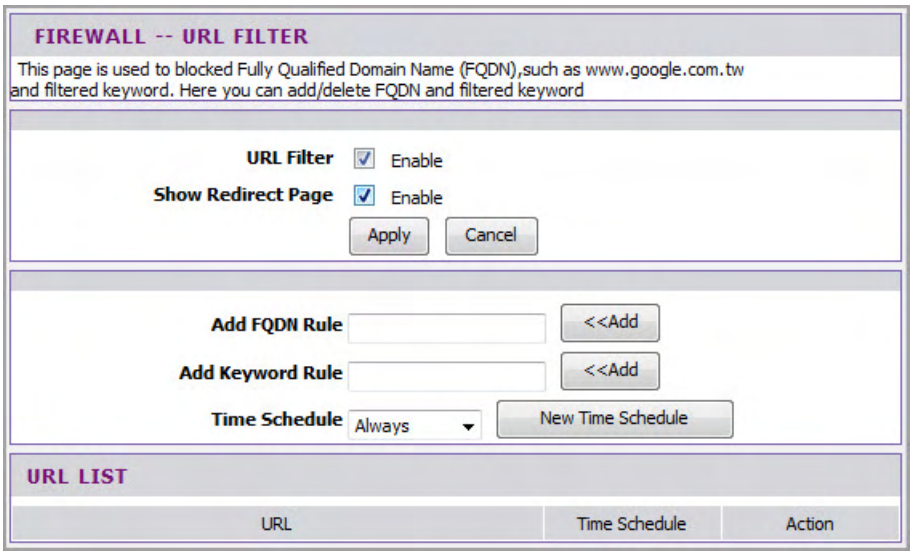
Time Schedule — Select the time to implement the IP filter or click the **New Time Schedule** button to create a new schedule.

Click the **Apply** button to save and activate the filter or click the **Cancel** button to discard your changes.

6.9.3 URL Filter

This page allows you to deny network devices to access specific URLs or URLs that contain specific keywords.

To access the URL Filter page, click **ADVANCED** > **Firewall** > **URL Filter** or click the **URL Filter** button.



URL Filter — Check this box to enable URL filtering.

Show Redirect Page — Check this box to redirect devices to another website when the website they are trying to access is blocked.

Click the **Apply** button to save and activate the filter or click the **Cancel** button to discard your changes.

To Filter a URL

1. On the **Add FQDN Rule** field, enter a Fully Qualified Domain Name (FQDN) that you want to block.

NOTE:

For example, if you block www.google.com, then you cannot access the website www.google.com.

2. Select the time to implement the URL filter or click the **New Time Schedule** button to create a new schedule.

3. Click the **Add** button of the Add FQDN Rule. The entry is listed on the URL LIST table.

To Filter Keyword

1. On the **Add Keyword Rule** field, enter a keyword. If a part of the URL contains this keyword, the website will not be accessible.

2. Select the time to implement the URL filter or click the **New Time Schedule** button to create a new schedule.

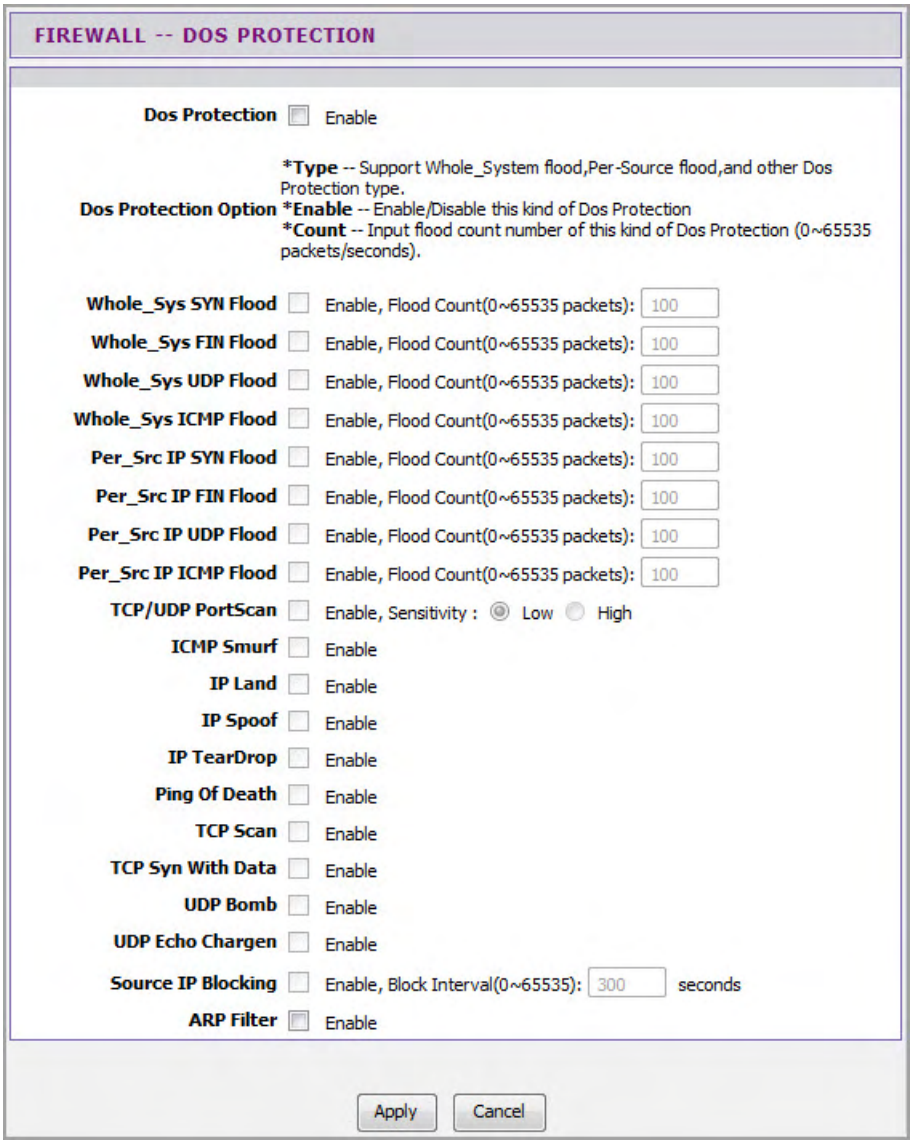
3. Click the **Add** button of the Add Keyword Rule. The entry is listed on the URL LIST table.

To delete an entry, click the corresponding button.

6.9.4 DOS Protection

This page allows you to protect your network from hackers to run Denial of Service (DoS) attacks.

To access the DOS Protection page, click **ADVANCED** > **Firewall** > **DOS Protection** or click the **DOS Protection** button.



Dos Protection — Check this box to enable DoS protection.

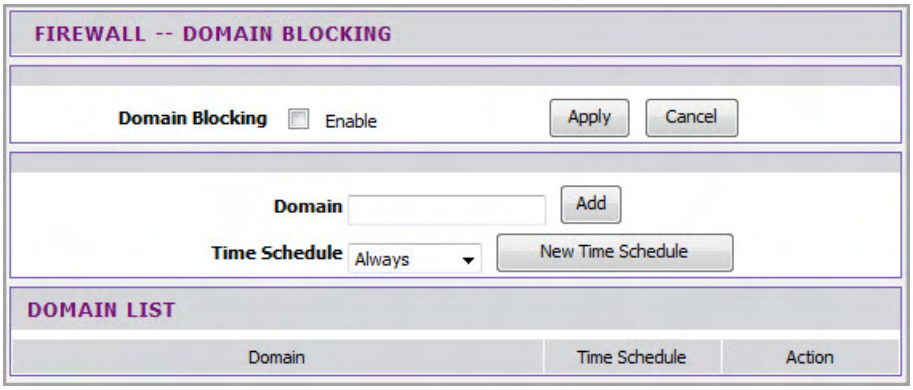
Dos Protection Option — Check the appropriate boxes to enable protection from SYN flood, FIN flood, UDP flood, ICMP flood, SMURF, IP spoofing, and others. Enter the flood count numbers or retain the default values if you are unsure about them.

Check the **Apply** button to save and activate DoS protection or click the **Cancel** button to discard your changes.

6.9.5 Domain Blocking

This page allows you to deny network devices to access specific domains such as an http and an ftp.

To access the Domain Blocking page, click **ADVANCED** > **Firewall** > **Domain Blocking** or click the **Domain Blocking** button.



Domain Blocking — Check this box to enable domain blocking. Click the **Apply** button to activate domain blocking.

To Block Domains

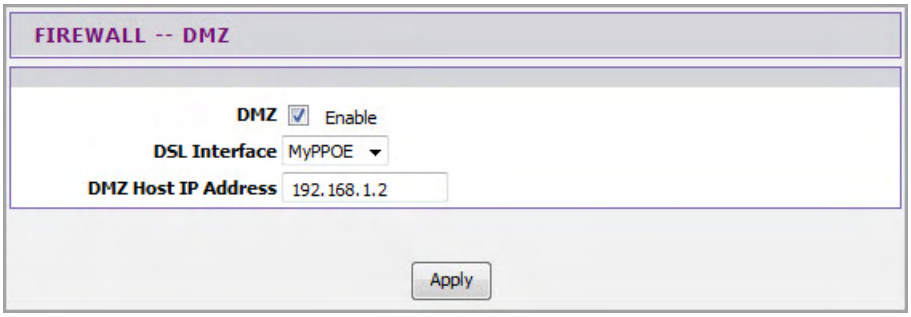
1. On the **Domain** field, enter the domain name to block.
2. Select the time to implement the domain blocking or click the **New Time Schedule** button to create a new schedule.
3. Click the **Add** button to add the domain. The entry is listed on the DOMAIN LIST table.

To delete an entry, click the corresponding icon.

6.9.6 DMZ

A DMZ (Demilitarized Zone) sets a single computer, called a DMZ host, on your network to have unrestricted Internet access. This function is useful for gaming purposes or when a computer on your network cannot access the Internet properly. However, this places the DMZ host outside the firewall and exposes it to security risks.

To access the DMZ page, click **ADVANCED** > **Firewall** > **DMZ** or click the **DMZ** button.



DMZ — Check this box to enable DMZ.

DSL Interface — Select the DSL interface to activate DMZ from the drop-down list.

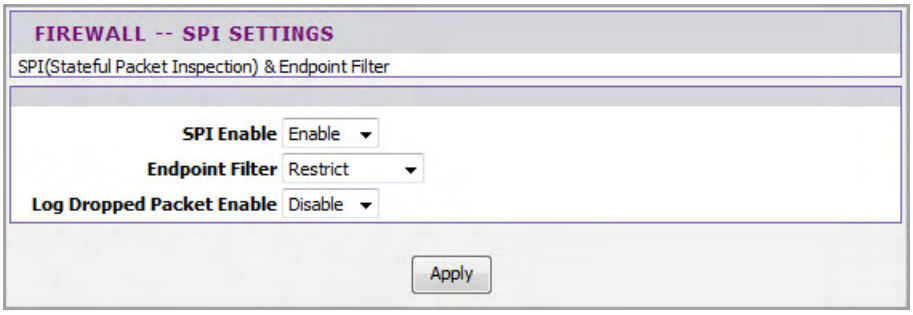
DMZ Host IP Address — Enter the IP address of the computer to set as the DMZ host.

Check the **Apply** button to save and activate DMZ.

6.9.7 SPI Settings

SPI (Stateful Packet Inspection) filters more kinds of attacks by closely examining packet data structures.

To access the SPI Settings page, click **ADVANCED** > **Firewall** > **SPI Settings** or click the **SPI Settings** button.



SPI Enable — Select whether to enable or disable the SPI function.

Endpoint Filter — Select an endpoint filter option:

- **Independent**: Forwards all incoming traffic from an open port to the application that opened the port.
- **Restrict**: Incoming traffic must match the IP address of the outgoing connection.

Log Dropped Packet Enabled — Select whether to enable or disable logging of dropped packets from your network or the Internet.

Click the **Apply** button to save and activate the SPI settings.

6.10 Packet Filter

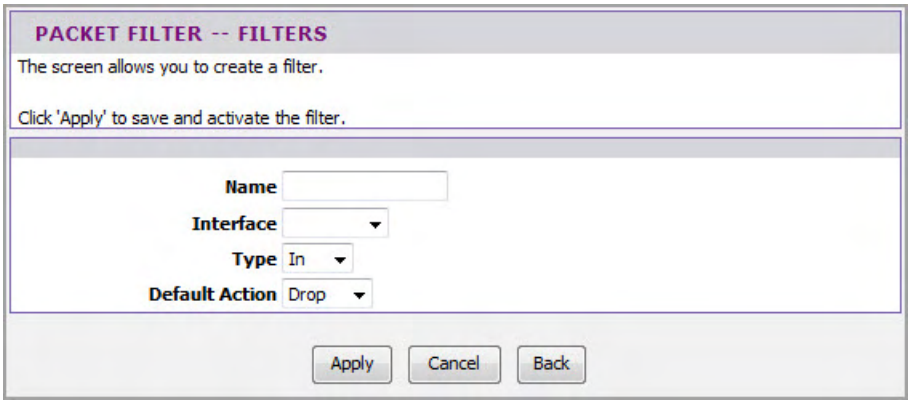
6.10.1 Filters & Rules

This page allows you to create packet filters and rules. These filters are used to check each data that passes within your network. If the packet data does not meet the requirements, the packet is either dropped or rejected.

To access the Filters & Rules page, click **ADVANCED** > **Packet Filter** > **Filters & Rules** or click the **Filters & Rules** button.

Filters

Click the **Add** button to create a new filter.



Name — Enter desired filter name.

> **NOTE:**
>
> The filter name cannot contain spaces.

Interface — Select the interface to implement the filter.

Type — Select **In** to filter incoming packets or select **Out** to filter outgoing packets.

Default Action — Select **Drop** to drop the packets or select **Permit** to allow packets to pass through if the rule requirement is met.

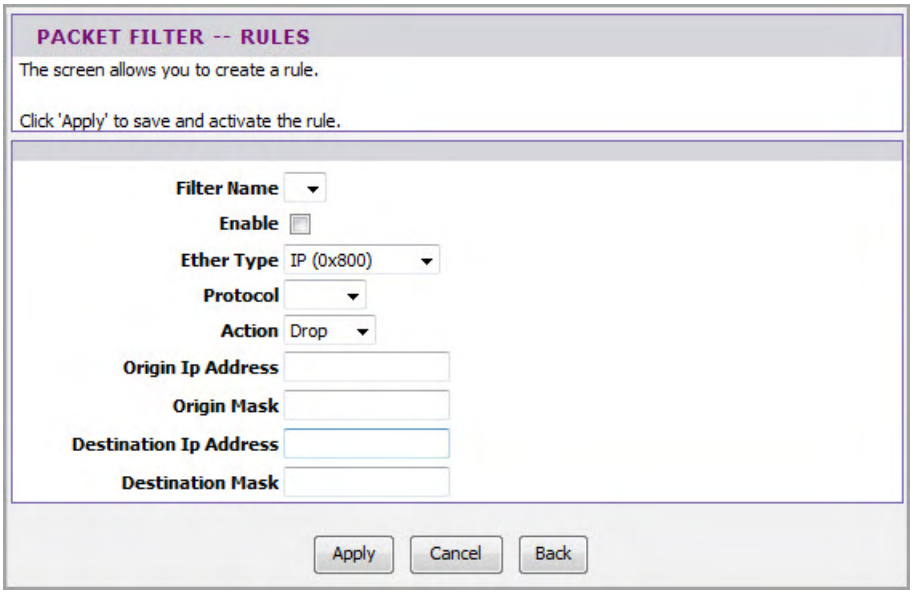
Click the **Apply** button to save the filter or click the **Cancel** button to discard your changes.

The new entry is listed on the FILTERS table. An **Index** is automatically assigned to each filter that you create.

To edit a filter, click the corresponding icon. To delete a filter, click the corresponding icon.

Rules

After creating filters, click the **Add** button to set the rules on how to implement the filters.



Filter Name — Select the filter to assign the rule.

Enable — Check this box to enable this rule.

Ether Type — Select the Ether type: **IP (0x800)** or **IPv6 (0x86DD)**.

Protocol — Select a protocol from the drop-down list. Options are **TCP**, **UDP**, or **ICMP**.

Action — Select the action to execute when the rule requirement is met. Options are:

- **Drop**: Select to drop the packets if the rule requirement is met.
- **Permit**: Select to allow packets to pass through if the rule requirement is met.
- **Reject**: Select to reject the packets if the rule requirement is met. Select the **Reject Type** from the drop-down list.

Depending on the selected protocol and the selected action, the fields below may or may not be displayed on the screen.

Origin IP Address — Enter the IP address of the origin of the packets.

Origin Mask — Enter the subnet mask of the origin of the packets.

Origin Start Port and **Origin End Port** — Enter the starting and ending port range of the origin of the packets.

Destination IP Address — Enter the IP address of the destination of the packets.

Destination Mask — Enter the subnet mask of the destination of the packets.

Destination Start Port and **Destination End Port** — Enter the starting and ending port range of the destination of the packets.

ICMP Type — Select an ICMP type from the drop-down list. If the selected type is met, the filter is implemented.

Click the **Apply** button to save and activate the rule or click the **Cancel** button to discard your changes.

6.10.2 Statistics

This page displays the filter and rule statistics.

To access the Statistics page, click **ADVANCED** > **Packet Filter** > **Statistics** or click the **Statistics** button.

Click the **Refresh** button to refresh the list.

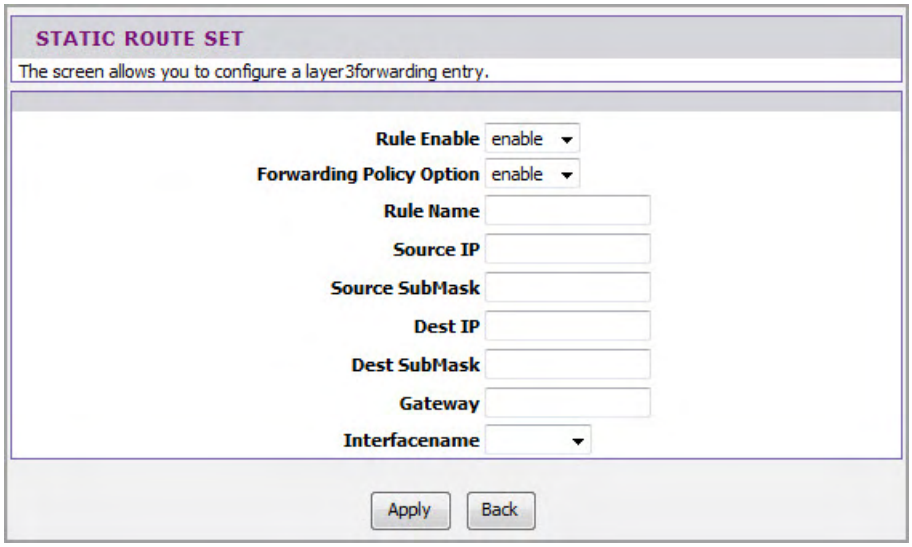
6.11 Static Route

This page allows you to create routing tables for IPv4 and IPv6 protocols.

To access the Static Route page, click **ADVANCED** > **Static Route**.

To create a static route, click the **Add** button under the desired IP protocol static route table.

IPv4 Static Route



Rule Enable — Enable or disable rule.

Forwarding Policy Option — Select whether to enable or disable routing.

Rule Name — Enter desired rule name.

Source IP — Enter the source IP address.

Source SubMask — Enter the source subnet mask.

Dest IP — Enter the destination IP address.

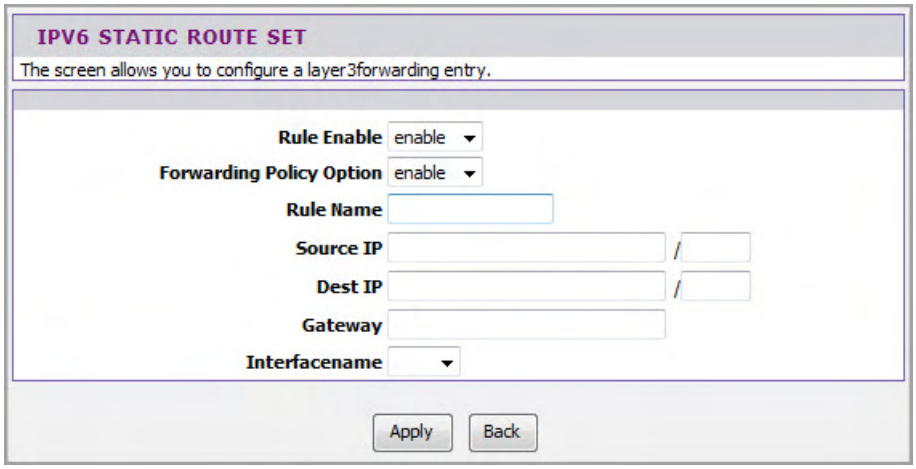
Dest SubMask — Enter the destination subnet mask.

Gateway — Enter the gateway.

Interface name — Select the interface to implement the routing.

Click the **Apply** button to save and activate the static route or click the button to discard your changes.

IPv6 Static Route



Rule Enable — Enable or disable rule.

Forwarding Policy Option — Select whether to enable or disable routing.

Rule Name — Enter desired rule name.

Source IP — Enter the source IP address.

Dest IP — Enter the destination IP address.

Gateway — Enter the gateway.

Interface name — Select the interface to implement the routing.

Click the **Apply** button to save and activate the static route or click the button to discard your changes.

6.12 Multicast

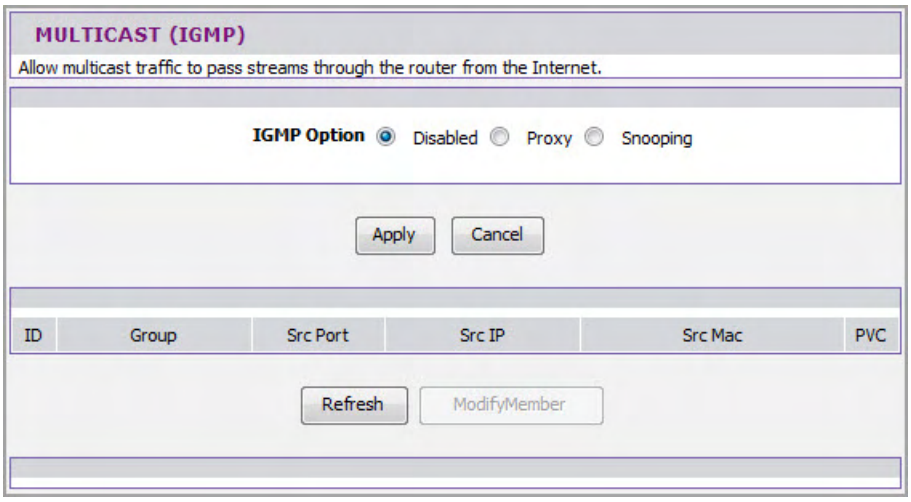
This page allows you to configure IGMP and MLD settings.

To access the Multicast page, click **ADVANCED** > **Multicast**.

6.12.1 IGMP

Internet Group Management Protocol (IGMP), for IPv4 protocol, manages members of groups of devices, called IP multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group membership. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP is used for online video and gaming, and allows more efficient use of resources that support these applications.

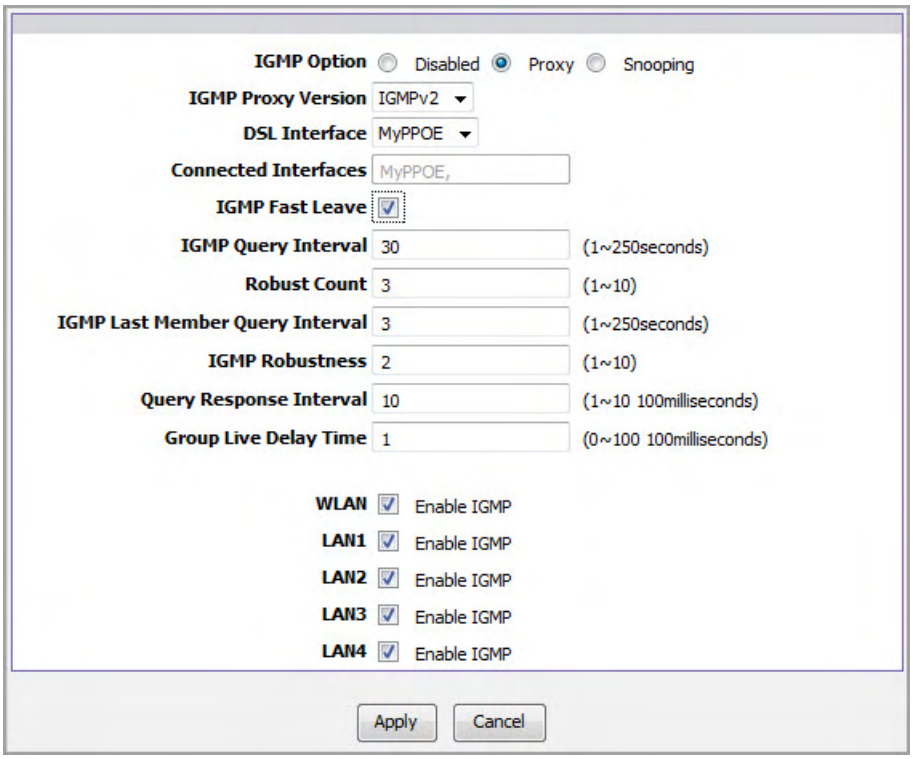
To access the Multicast IGMP page, click **ADVANCED** > **Multicast** > **IGMP** or click the **IGMP** button.



IGMP Proxy

IGMP proxy enables your Wireless Gateway to forward multicasts traffics between LAN and WAN networks.

1. On **IGMP Option**, select **Proxy**.
2. Click the **Apply** button.
3. Click the **Apply** button again. More fields appear on the screen.



4. Select the **IGMP Proxy Version**.

5. Select the **DSL Interface** to implement IGMP. Connected interfaces are displayed in the **Connected Interfaces** fields.

6. To enable IGMP fast leave option, check the **IGMP Fast Leave** box.

7. Enter values for **IGMP Query Interval**, **Robust Count**, **IGMP Last Member Query Interval**, **IGMP Robustness**, **Query Response Interval**, and **Group Live Delay Time**. If you are unsure about them, leave the default values.

8. Check the **Enable IGMP** box for **WLAN**, **LAN1**, **LAN2**, **LAN3**, or **LAN4** to enable IGMP in the respective network connection.

9. Click the **Apply** button to save and apply changes.

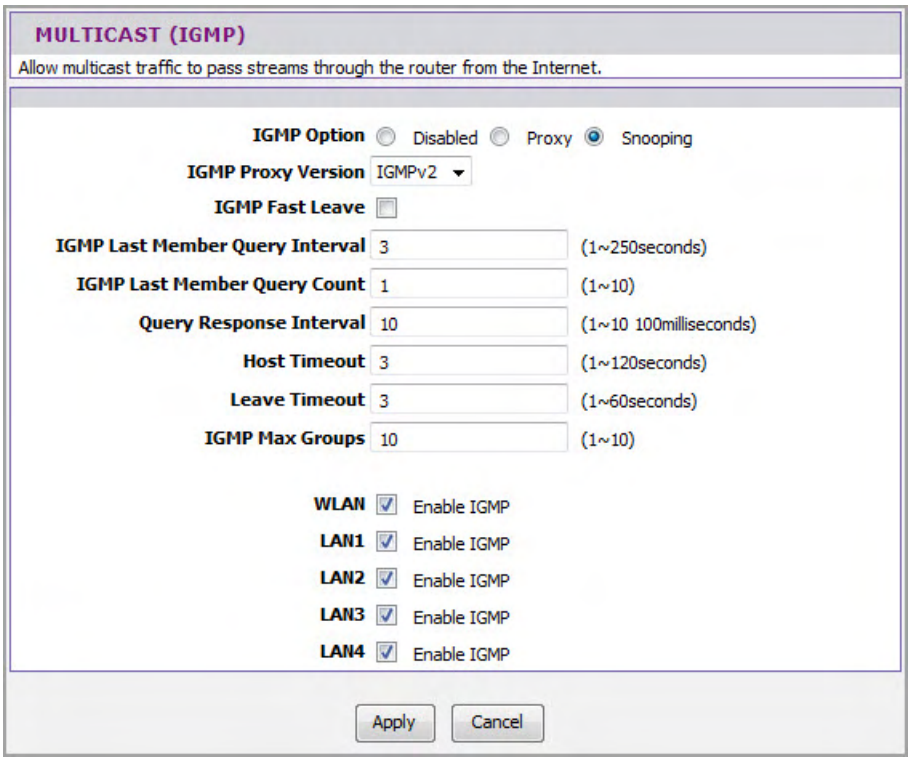
IGMP Snooping

With IGMP snooping, your Wireless Gateway can make intelligent multicast forwarding to connections that have group members attached. As a result, IGMP snooping prevents or reduces traffic on the interface that is not registered as a receiver of a specific multicast group.

1. On **IGMP Option**, select **Snooping**.

2. Click the **Apply** button.

3. Click the **Apply** button again. More fields appear on the screen.



4. Select the **IGMP Proxy Version**.

5. To enable IGMP fast leave option, check the **IGMP Fast Leave** box.

6. Enter values for **IGMP Last Member Query Interval**, **IGMP Last Member Query Count**, **Query Response Time**, **Host Timeout**, **Leave Timeout**, or **IGMP Max Groups**. If you are unsure about them, leave the default values.

7. Check the **Enable IGMP** box for **WLAN**, **LAN1**, **LAN2**, **LAN3**, or **LAN4** to enable IGMP in the respective network connection.

8. Click the **Apply** button to save and apply changes.

6.12.2 MLD

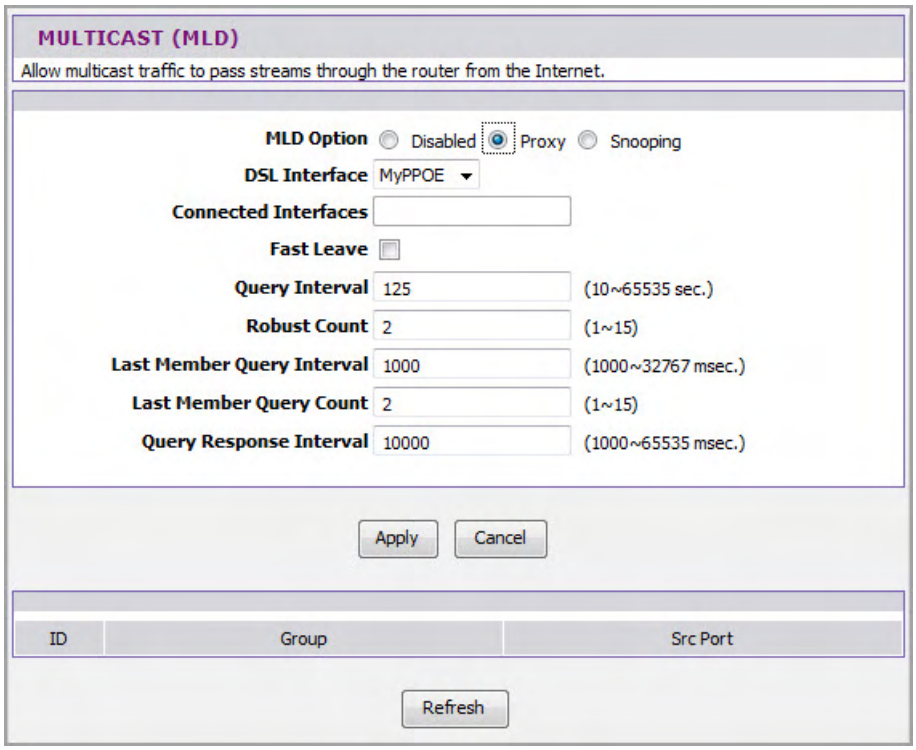
Multicast Listener Discovery (MLD) is a component of IPv6. MLD manages group membership in IPv6, similar to IGMP in IPv4.

To access the Multicast MLD page, click **ADVANCED** > **Multicast** > **MLD** or click the **MLD** button.

MLD Proxy

MLD proxy enables your Wireless Gateway to forward multicasts traffics between LAN and WAN networks in the IPv6 protocol.

1. On **MLD Option**, select **Proxy**.



2. Select the **DSL Interface** to implement IGMP. Connected interfaces are displayed in the **Connected Interfaces** fields.

3. To enable fast leave option, check the **Fast Leave** box.

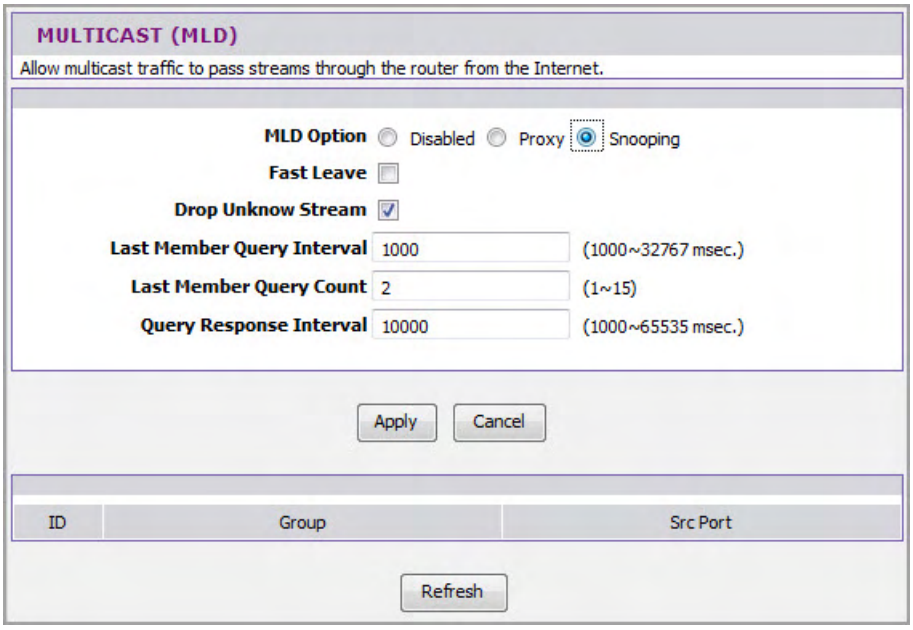
4. Enter values for **Query Interval**, **Robust Count**, **Last Member Query Interval**, **Last Member Query Count**, and **Query Response Interval**. If you are unsure about them, leave the default values.

5. Click the **Apply** button to save and apply changes.

MLD Snooping

With MLD snooping, your Wireless Gateway can make intelligent multicast forwarding to connections that have group members attached in IPv6 protocol.

1. On **MLD Option**, select **Snooping**.



2. To enable fast leave option, check the **Fast Leave** box.

3. Check **Drop Unknown Stream** box to drop unknown streams.

4. Enter values for **Last Member Query Interval**, **Last Member Query Count**, and **Query Response Interval**. If you are unsure about them, leave the default values.

5. Click the **Apply** button to save and apply changes.

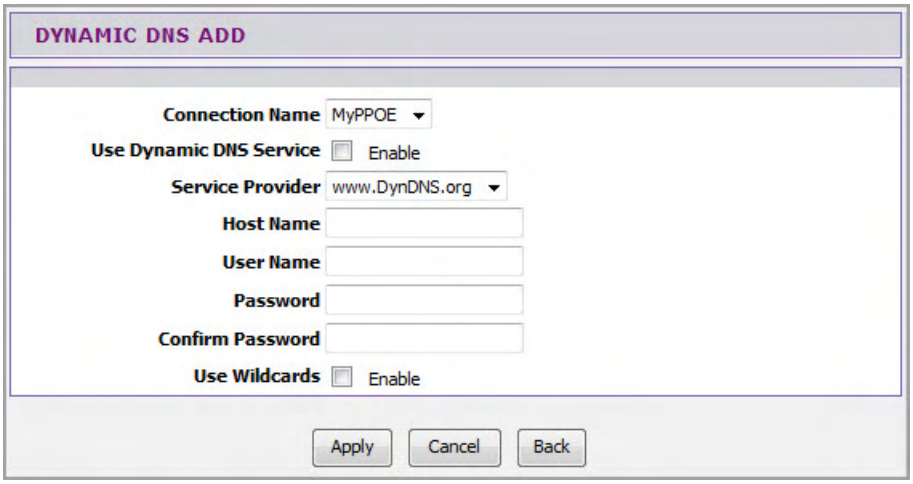
6.13 Dynamic DNS

Each time your Wireless Gateway connects to the Internet, your ISP assigns a different IP address to your device. In order to access your device from the WAN side, you need to manually track the IP that is currently used. The Dynamic DNS (DDNS) feature allows you to register your device with a DNS server and use the same host name to access your device.

To access the Dynamic DNS page, click **ADVANCED** > **Dynamic DNS**.

The table lists the current DDNS. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding icon.

To add DDNS, click the **Add** button.



Connection Name — Select a connection from the drop-down list.

Use Dynamic DNS Service — Check this box to register this account to the DNS server.

Service Provider — Select a service provider from the drop-down list.

NOTE:

Additional charges may be incurred depending on the selected service provider.

Host Name — Enter a domain name to be registered to the DNS server.

User Name — Enter the user name of your DNS account assigned by the service provider.

Password — Enter the password of your DNS account assigned by the service provider. Re-enter the password on the **Confirm Password** field.

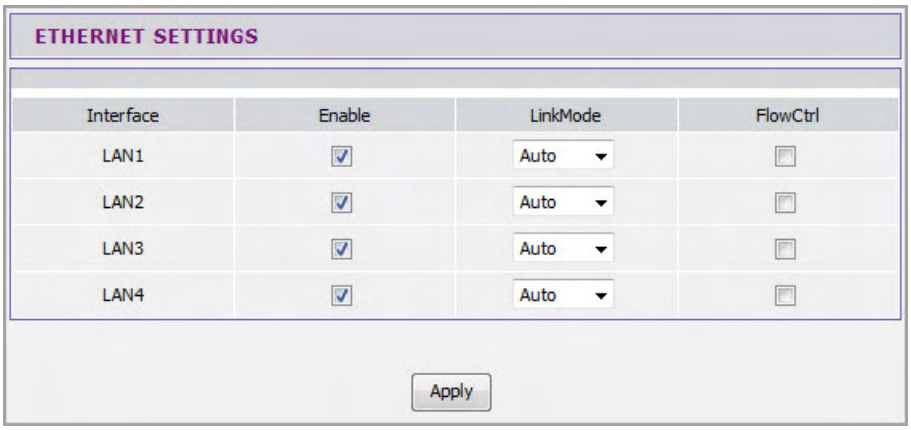
Use Wildcards — Check this box to enable searching with wildcards.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

6.14 Ethernet Setting

This page allows you to set the link mode and enable flow control for each of the four LAN ports of your Wireless Gateway.

To access the Ethernet Setting page, click **ADVANCED** > **Ethernet Setting**.



Check the **Enable** box of the LAN interface to enable the port.

Select the **LinkMode** from the drop-down list. Options are: **Auto**, **10Half**, **10Full**, **100Half**, and **100Full**.

Check the **FlowCntrl** box of the LAN interface to enable flow control.

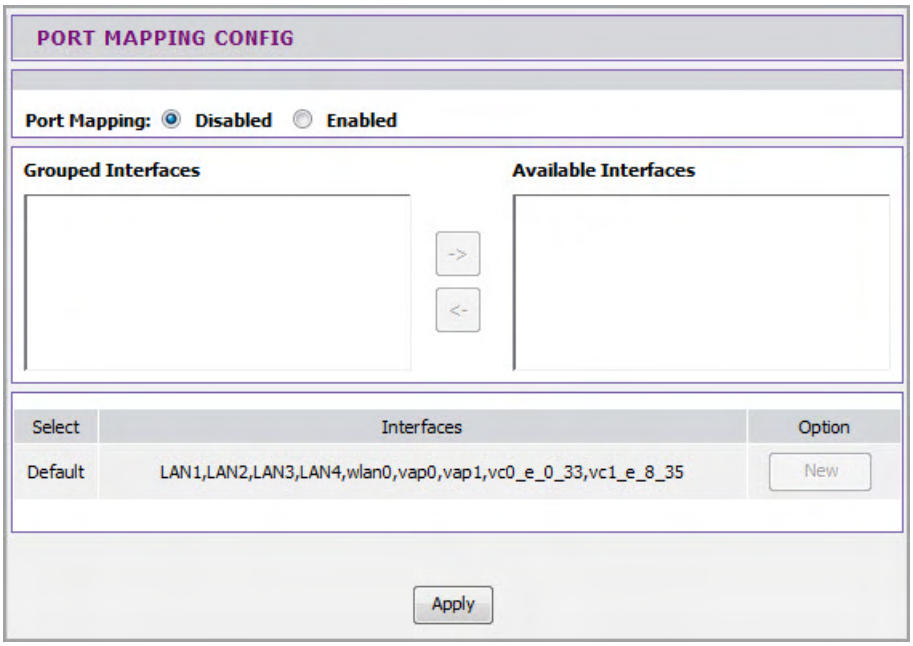
Click the **Apply** button to save your changes.

6.15 Port Mapping

Port mapping allows you to group interfaces for traffic control. Traffic is isolated from group to group. Therefore, traffic coming from an interface of a group can only be flowed to the interfaces in the same group.

By default, all interfaces belong to the **Default** group. You can create new groups and move interfaces to other groups. However, an interface can only be a member of one group.

To access the Port Mapping page, click **ADVANCED** > **Port Mapping**.



Port Mapping — Select **Enabled** to enable port mapping.

To Create New Groups

1. Click the **New** button. An empty group appears on the table.
2. Click the radio button to select the empty group.
3. Add members to the group. To do so, select an interface from the **Available Interfaces** panel. Then click the **<-** button to add the selected interface to the **Grouped Interfaces** panel.
4. Repeat step 3 to add more members to the group.
5. Click the **Apply** button to save your changes.

To Modify Groups

1. Click the radio button to select the group to modify.
2. To add or remove a member from the group, select the interface, then click the <- or -> buttons.
3. Click the **Apply** button to save your changes.

To Delete Groups

Click the corresponding **Delete** button of the group to delete. The members of that group automatically revert back to the **Default** group.

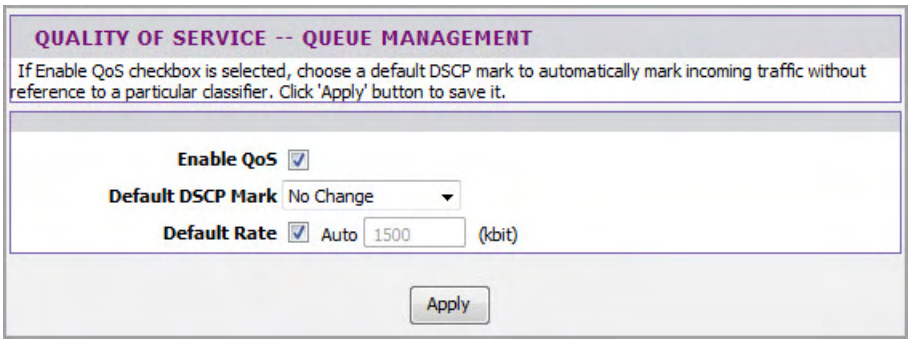
6.16 Quality of Service (QoS)

Quality of Service (QoS) is a network standard that assigns the priorities of traffic that passes through your Wireless Gateway. This ensures that demanding real-time applications, such as video streaming, are given priority over other data.

6.16.1 Queue Management

This page allows you to enable QoS and choose Differentiated Services Code Point (DSCP) markings to automatically mark incoming traffic without reference to a particular classifier.

To access the **Queue Management** page, click **ADVANCED** > **Quality of Service** > **Queue Management** or click the **Queue Management** button.



Enable QoS — Check this box to enable the QoS feature.

Default DSCP Mark — Select a DSCP mark from the drop-down list. The DSCP mark is used to classify and prioritize types of packets.

NOTE:

If the drop-down lit does not contain the DSCP marking that you want, select either Private DSCP value or Public DSCP value.

Default Rate — Check the **Auto** box to set the rate to its auto default or uncheck the box to enter the QoS rate manually.

Click the **Apply** button to save and apply the QoS settings.

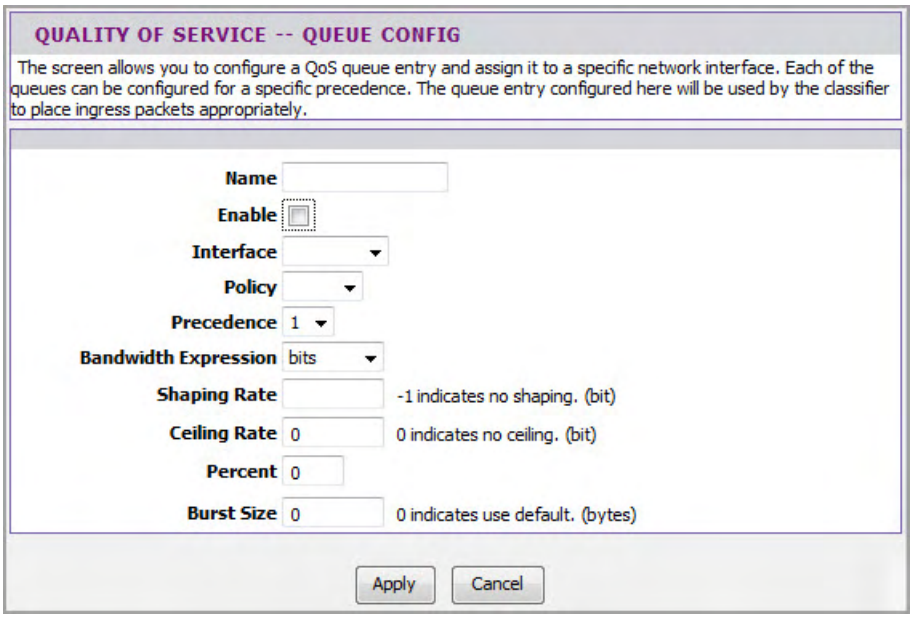
6.16.2 Queue Config

This page allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue configuration will be used in Queue Classification to place ingress packets appropriately.

To access the **Queue Config** page, click **ADVANCED** > **Quality of Service** > **Queue Config** or click the **Queue Config** button.

The table displays QoS queue configurations. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding icon.

To configure QoS queue entries, click the **Add** button.



Name — Enter a QoS queue entry name.

Enable — Check this box to enable this queue.

Interface — Select the interface to implement this QoS queue.

Policy — Select the queue policy. Options are:

- **SP**: In Strict Priority (SP), packets with a high priority are processed first. Not until the first queue is empty will another queue be processed.
- **WFQ**: In Weighted Fair Queuing (WFQ), each queue can be given a different priority level. Each traffic is assigned to a class and each class is given its own queue.

Precedence — Select the precedence from the drop-down list.

Bandwidth Expression — Select one of the following options:

- **bits**: Enter the **Shaping Rate** and **Ceiling Rate**.
- **Percent**: Enter the **Percent**.

Burst Size — Enter the burst size.

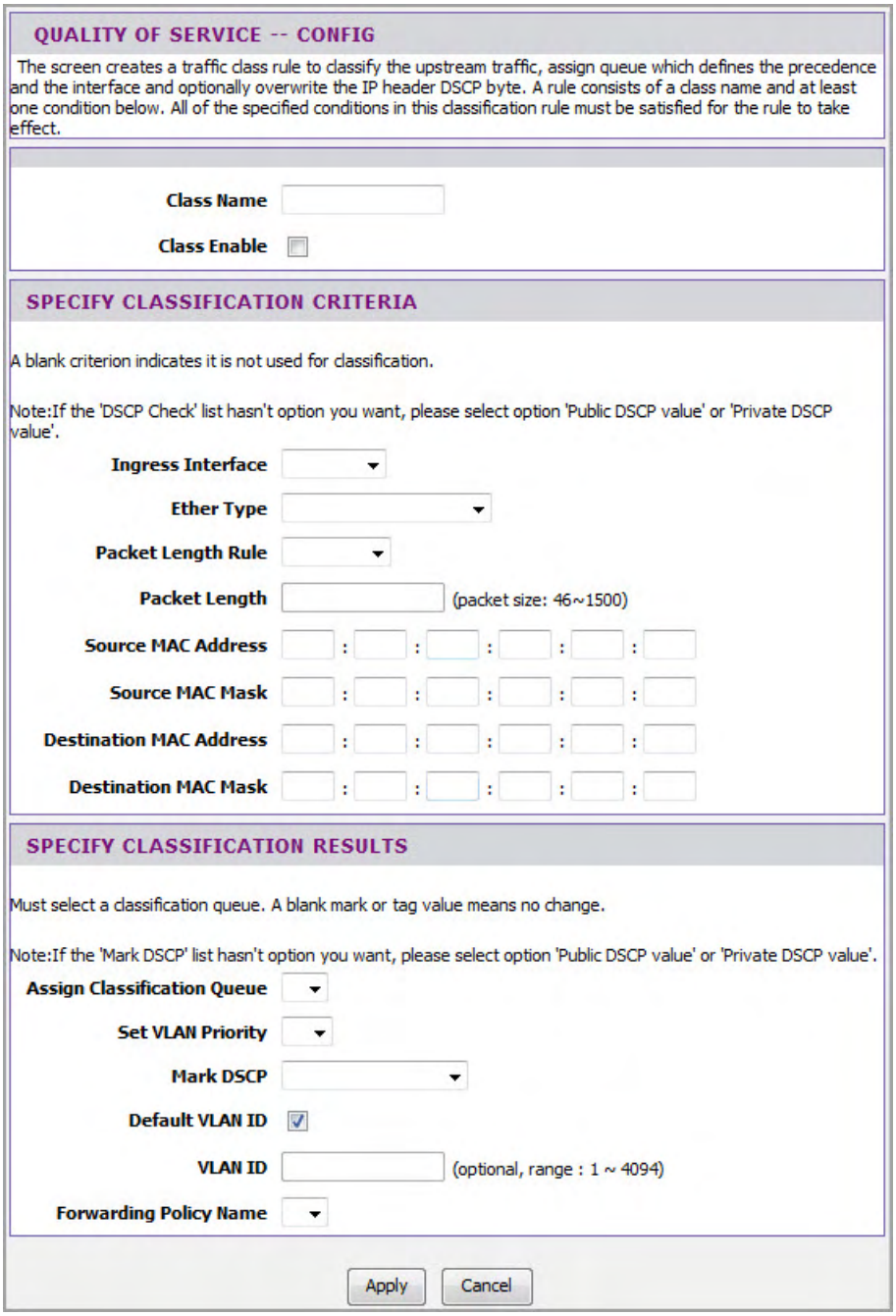
Click the **Apply** button to save the queue configuration or click the **Cancel** button to discard your changes.

6.16.3 Queue Classification

This page allows you to configure classification rules to classify upstream traffic and assign queues which define the precedence, interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All the specified conditions in the classification rule must be satisfied for the rule to take effect.

To access the **Queue Classification** page, click **ADVANCED** > **Quality of Service** > **Queue Classification** or click the **QoS Classification** button.

The table displays QoS queue classification rules. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding icon.



Class Name — Enter a classification name.

Class Enable — Check this box to enable the classification.

Specify Classification Criteria

You can classify traffic based on ingress interface, Ether type, packet length, source or destination MAC address/ MAC Mask, or a combination of them. Select an option or enter the values on the fields that you want to use for the criteria. Otherwise, leave the fields empty.

Depending on the selected **Ether Type**, the succeeding required information may vary.

If packet length is used as a criteria, select the **Packet Length Rule** from the drop-down list and enter the **Packet Length**.

Specify Classification Results

Some fields may not be applicable; if so, leave inapplicable fields empty.

Assign Classification Queue — Select the classification queue from the drop-down list. Only enabled classification queues from the Queue Classification page are listed here.

Set VLAN Priority — To set the VLAN priority, select a priority from the drop-down list

Mark DSCP — Select the DSCP mark from the drop-down list. If the DSCP mark that you want is not listed, select either **Public DSCP value** or **Private DSCP value**.

Default VLAN ID — Check this box to use the default VLAN ID.

VLAN ID — If **Default VLAN ID** is not checked, enter preferred VLAN ID.

Forwarding Policy Name — Select the forwarding policy name from the drop-down list.

Click the **Apply** button to save and apply the settings or click the **Cancel** button to discard your changes.

6.16.4 QoS Status

This page allows you to view the QoS status.

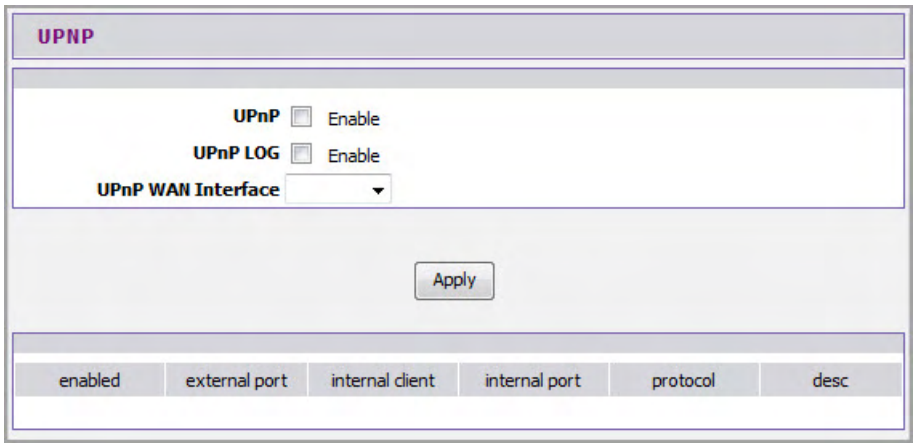
To access the **QoS Status** page, click **ADVANCED** > **Quality of Service** > **QoS Status** or click the **QoS Status** button.

Click the **Refresh** button to refresh the table.

6.17 UPnP

Universal Plug and Play (UPnP) allows automatic discovery and control of services available on the network from other devices without user intervention. This feature is commonly used for gaming and video streaming. If you feel that UPnP is a security concern, disable this feature.

To access the UPnP page, click **ADVANCED** > **UPnP**.



UPnP — Check this box to enable the UPnP feature.

UPnP LOG — Check this box to log UPnP status.

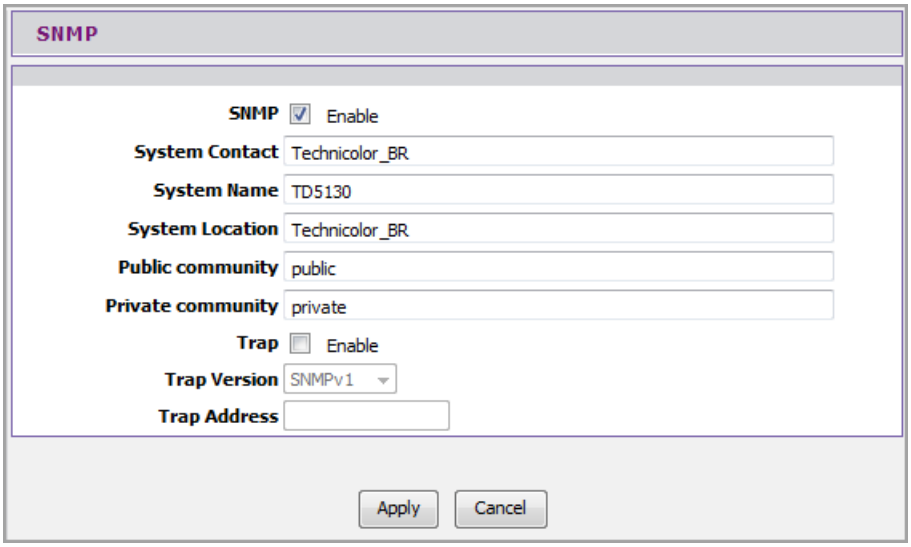
UPnP WAN Interface — Select the interface to implement UPnP.

Click the **Apply** button to save and apply the settings.

6.18 SNMP

Simplified Network Management Protocol (SNMP) is a troubleshooting and management protocol that is used to monitor the status and change the configurations of your Wireless Gateway locally or remotely. It also allows configuring and receiving of trap messages from network devices that are configured for SNMP.

To access the SNMP page, click **ADVANCED** > **SNMP**.



SNMP — Check this box to enable SNMP.

System Contact — Enter the contact person or contact information for your Wireless Gateway.

System Name — Enter an assigned name for your Wireless Gateway.

System Location — Enter an assigned location for your Wireless Gateway.

Public Community and **Private Community** — Enter a public and private community name.

Trap — Check this box to enable the Trap function, then provide the following information:

- **Trap Version**: Select an SNMP trap version from the drop-down list.
- **Trap Address**: Enter the destination IP address of the SNMP trap.

Click the **Apply** button to save and apply changes or click the **Cancel** button to discard your changes.

Chapter 7: Maintenance

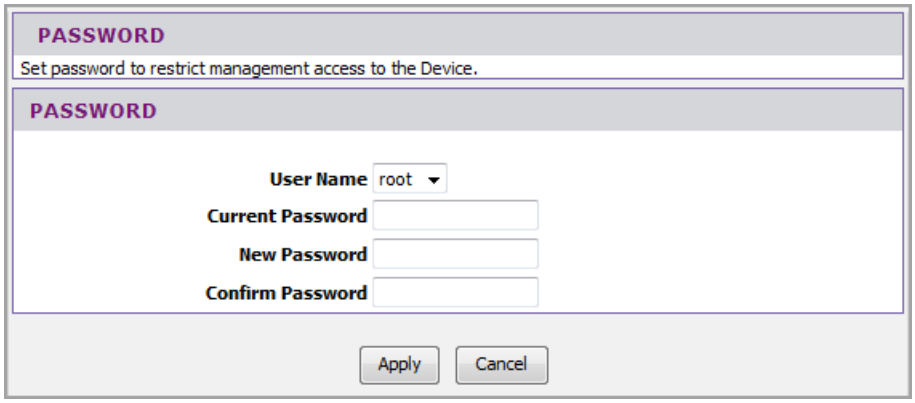
The Maintenance menu allows you to configure the web-based utility settings, such as password, remote management, backup/restore options, firmware upgrades, and others.

7.1 Password

Only one user name is allowed to login to the web-based utility of the Wireless Gateway. The only log in user name is "root", and the default password is empty.

For security reasons, it is strongly recommended to change the password. Once the password is changed, you are required to login before you can access to the Web Configurations.

To access the Password page, click **MAINTENANCE** > **Password**.



User Name — Displays the user account.

Current Password — Enter the current password.

New Password — Enter the desired password.

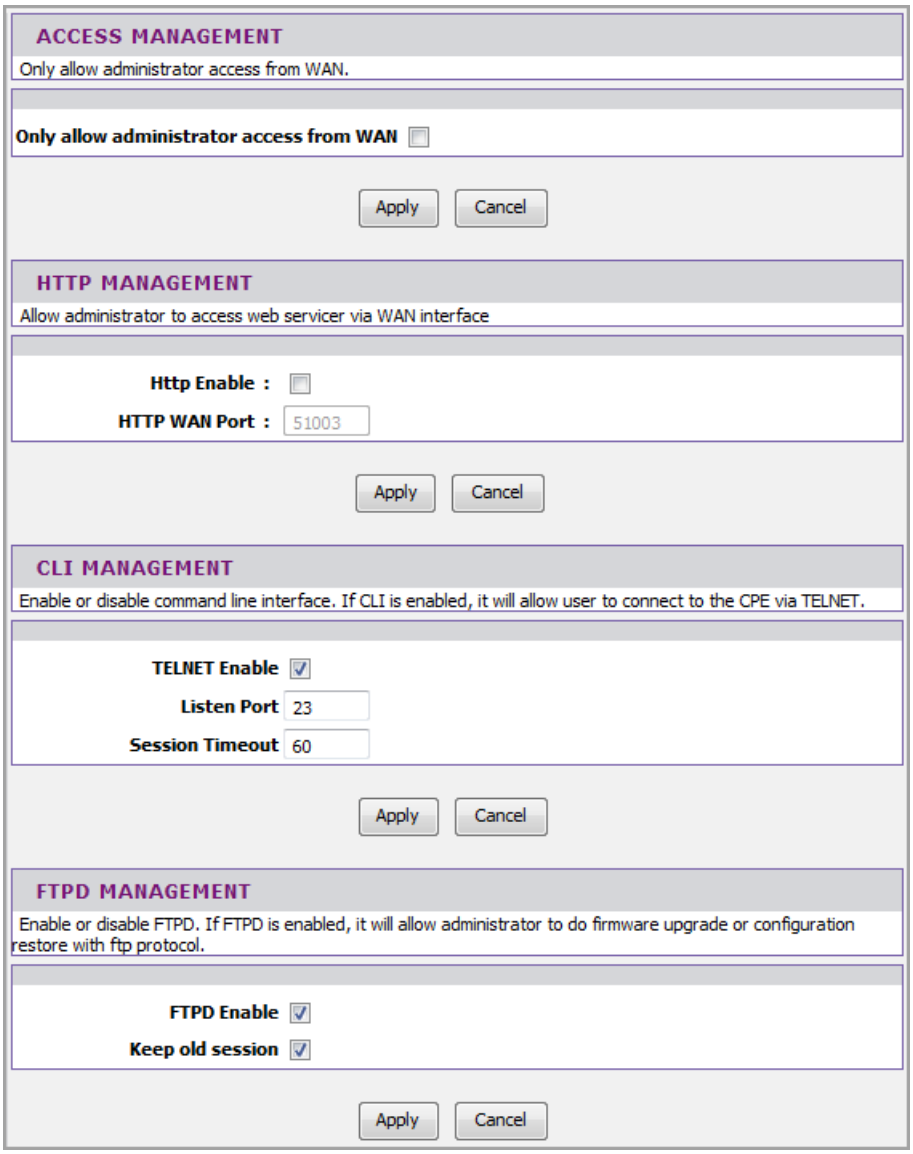
Confirm Password — Re-enter the new password.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

7.2 Remote Management

This page allows you to enable remote devices to manage your Wireless Gateway using the Hypertext Transfer Protocol (HTTP), Command-Line Interface (CLI), and File Transfer Protocol Daemon (FTPD).

To access the Remote Management page, click **MAINTENANCE** > **Remote Management**.



Access Management

Check the **Only allow administrator access from WAN** box to enable only the users who have administrator rights to login from WAN or uncheck the box to enable all users to login from WAN. Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

NOTE:

Remote access rights depend on the enabled remote management functions below.

HTTP Management

Check the **Http Enable** box to allow network administrators to remotely access the web-based utility via WAN interface. Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

CLI Management

Check the **TELNET Enable** box to allow network administrators to use the command-line interface.

Listen Port — Enter the Listen port.

Session Timeout — Enter the time wherein the session will automatically timeout after being idle for the specified time.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

FTPD Management

Check the **FTPD Enable** box to allow network administrators to upgrade the firmware or restore configurations using the FTP.

Keep old session — Check to retain the old session.

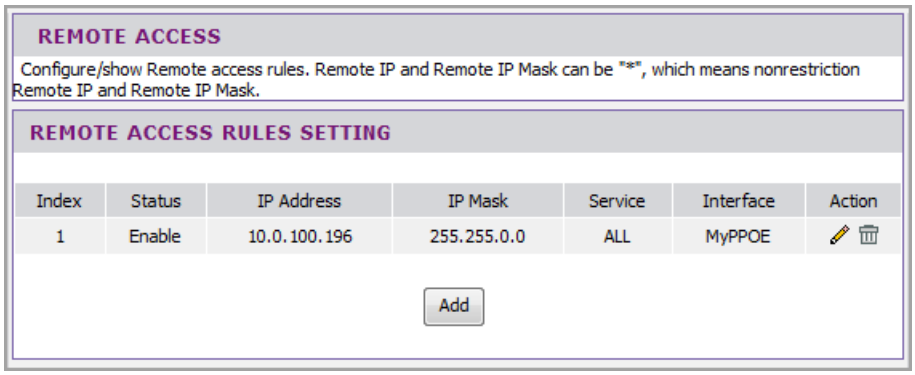
Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

7.3 Remote Access

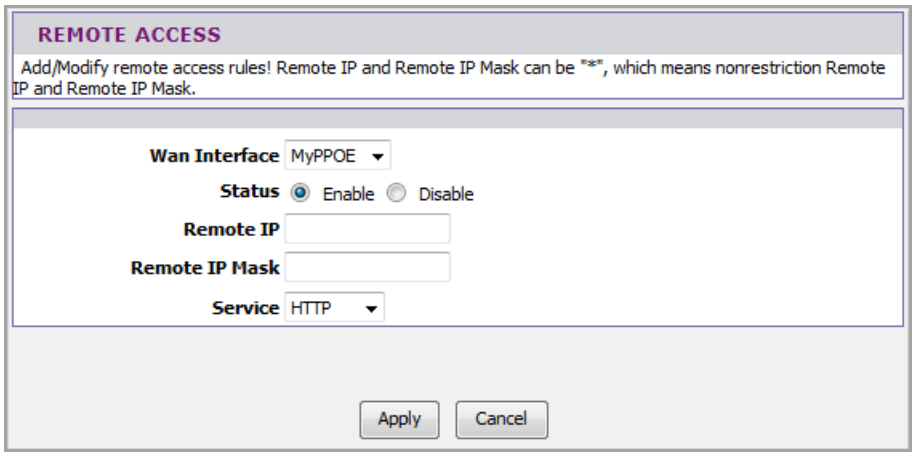
This page allows you to create and edit remote access rules. You can specify the IP address or the subnet mask of devices that are allowed or denied to remotely access your Wireless Gateway and set the type of management service that they can access.

To access the Remote Access page, click **MAINTENANCE** > **Remote Accesss**.

The table lists the remote access rules. To edit an entry, click the corresponding icon. To delete an entry, click the corresponding icon.



To create remote access rules, click the **Add** button.



Wan Interface — Select the interface from the drop-down list.

Status — Select whether to enable or disable remote access of the device.

Remote IP — Enter the IP address of the remote device.

Remote IP Mask — Enter the IP mask of the remote device.

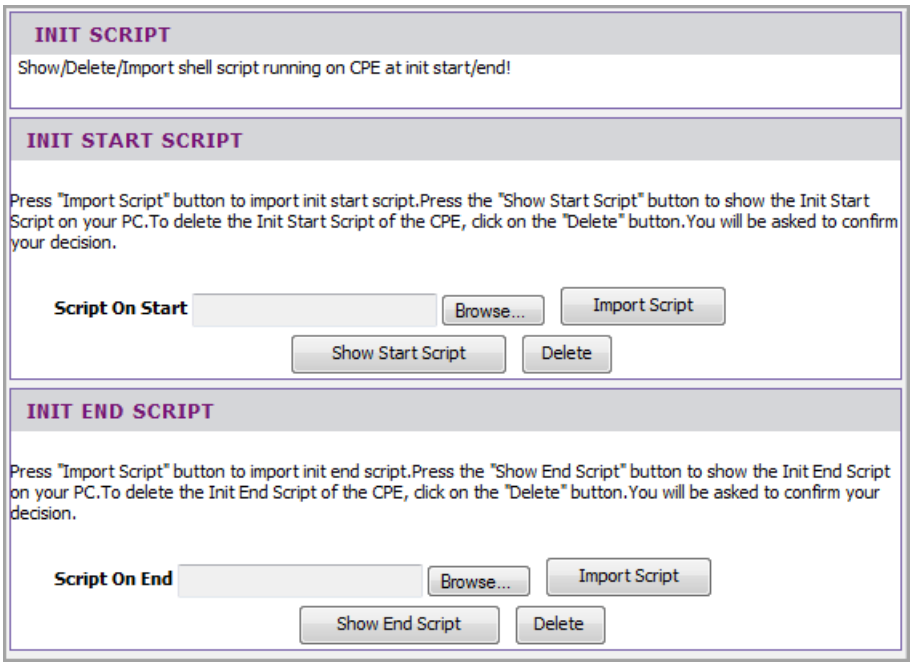
Service — Select the type of remote management service that the device can or cannot access.

Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

7.4 Init Script

This page allows you to show, delete, and import initialization scripts running on customer-premises equipment (CPE), such as telephones, routers, or set-top boxes, during system startup or shutdown.

To access the Init Script page, click **MAINTENANCE** > **Init Script**.



Init start scripts are scripts that run before the system starts up. Init end scripts are scripts that run before the system shuts down.

To import scripts, do the following:

1. Click the **Browse** button.
2. Browse for the file, then click the **Open** button.
3. Click the **Import Script** button.

To show the scripts on your computer, click the **Show Start/End Script** button.

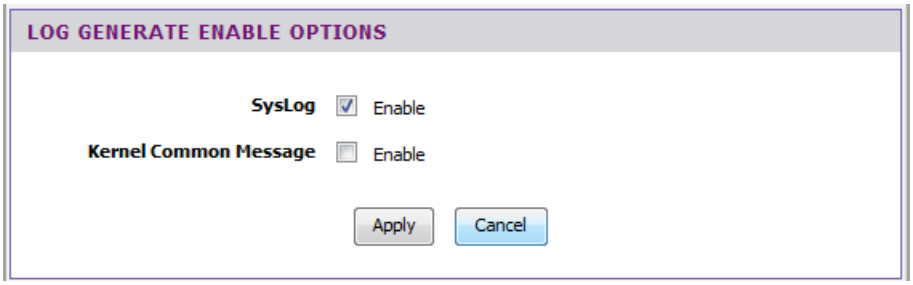
To delete the scripts on your computer, click the **Delete** button.

7.5 SysLog

This page allows you to enable and configure system logs such as device status, events, and activities. Logs can be sent to the network administrator via e-mail.

To access the SysLog page, click **MAINTENANCE** > **SysLog**.

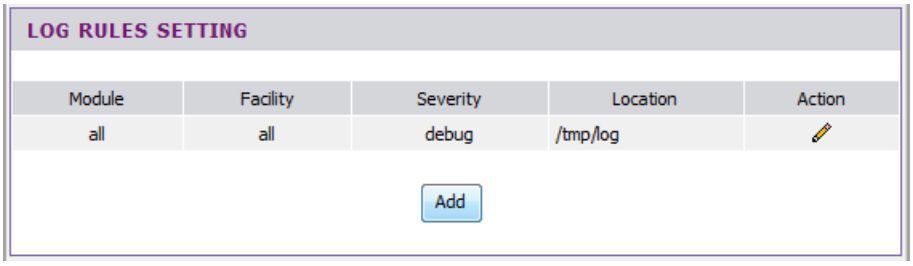
Log Generate Enable Options



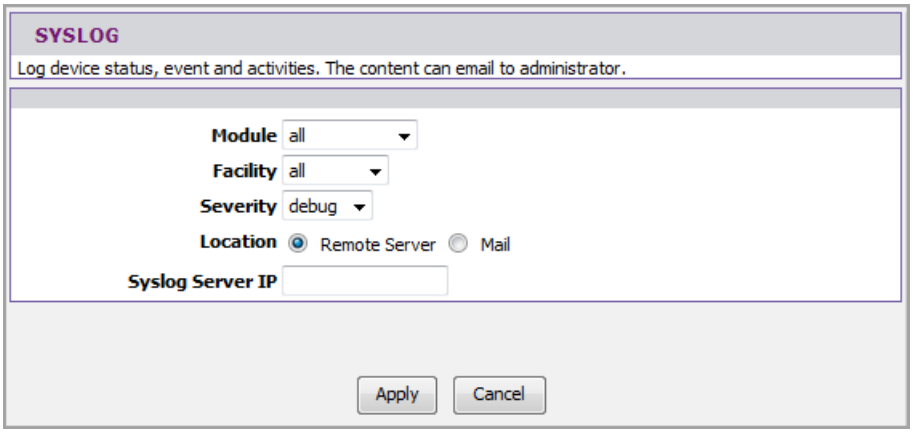
Kernel Common Message — Check this box to generate logs. Click the **Apply** button to save and apply the setting.

Log Rules Setting

The table displays current log rules. To edit an entry, click the corresponding icon.



To create log rules, click the **Add** button. The screen below is displayed.

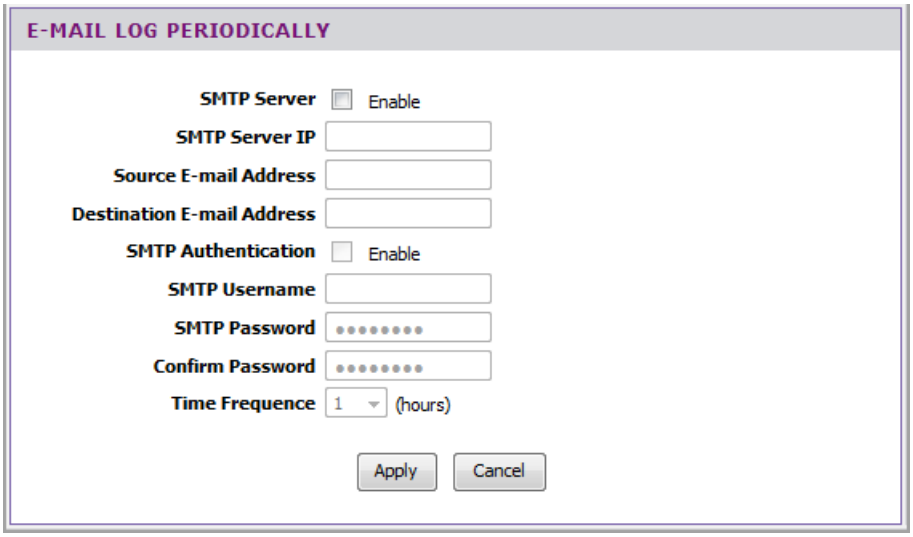


1. Select **Module** and **Facility**.
2. Select **Severity** level. **emerg** is the highest level while **debug** is the lowest level.
3. Select **Location**: **Remote Server** or **Mail**.

4. The succeeding fields may vary depending on the selected location. Enter the necessary information accordingly.

5. Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

E-mail Log Periodically



To log e-mails periodically, do the following:

1. Check the **SMTP Server** box to enable logging of e-mails periodically.

2. Enter the **SMTP Server IP**, **Source E-mail Address**, and **Destination E-mail Address**.

3. Check the **SMTP Authentication** box to enable authentication. And enter the **SMTP Username** and **SMTP Password**. Re-enter the password in the **Confirm Password** field.

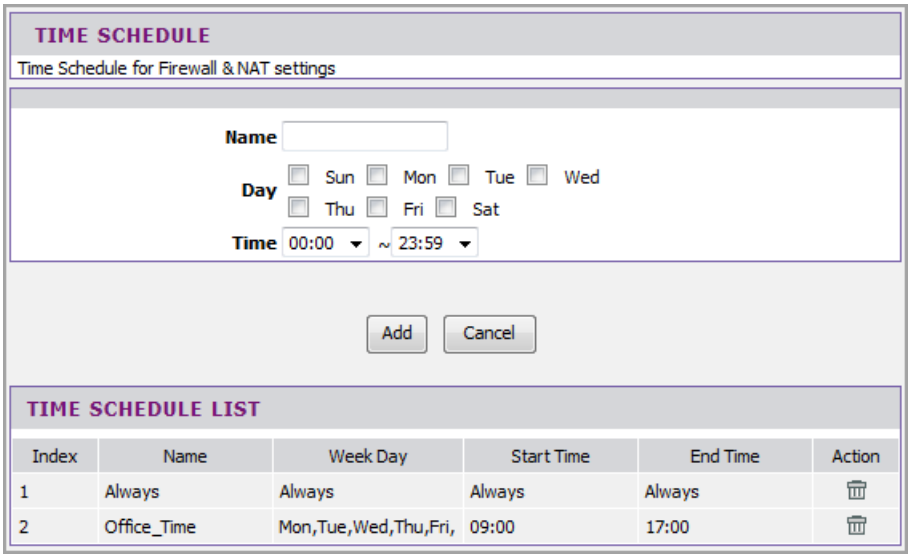
4. Select the **Time Frequency** of logging e-mails.

5. Click the **Apply** button to save your changes or click the **Cancel** button to discard your changes.

7.6 Time Schedule

This page allows you create desired time schedule.

To access the Time Schedule page, click **MAINTENANCE** > **Time Schedule**.



To create a new schedule, do the following:

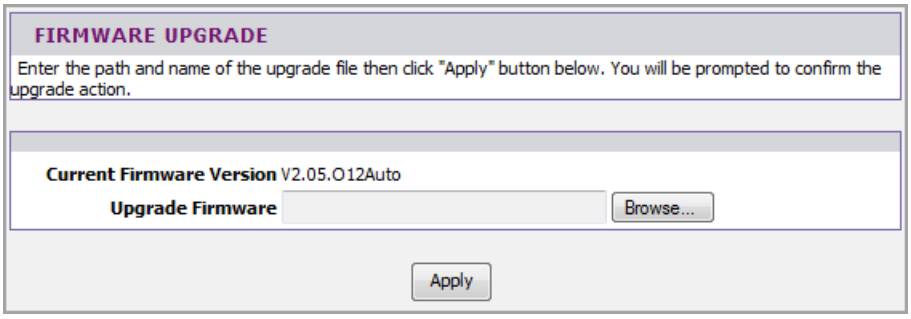
1. On the **Name** field, enter the desired schedule name.
2. Check the days to implement the schedule and select the time period.
3. Click the **Add** button to save the schedule. The new entry is listed on the TIME SCHEDULE LIST.

To delete a schedule, click the corresponding icon.

7.7 Firmware Upgrade

This page displays the current firmware version of your Wireless Gateway and allows you to install the upgrade.

To access the Firmware Upgrade page, click **MAINTENANCE** > **Firmware Upgrade**.



Click the **Browse** button and browse for the file. Click the **Apply** button to start firmware upgrade.

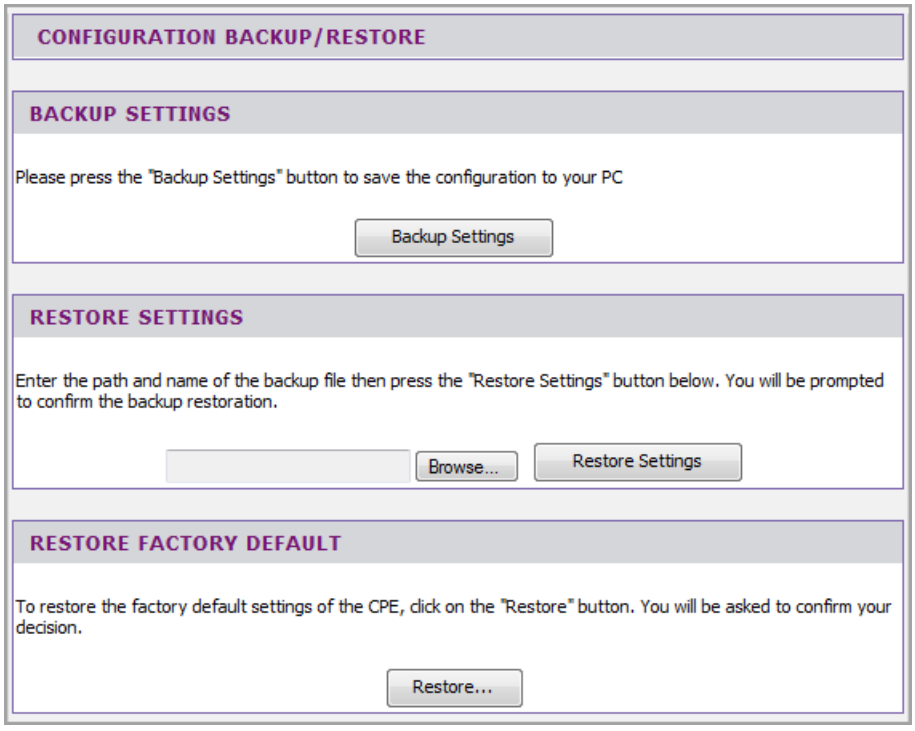
WARNING:

Do not turn off or press the Reset button on your Wireless Gateway while firmware upgrade is in progress. Doing so will crash the system.

7.8 Configuration Backup/Restore

This page allows you to save a backup of your current settings, revert settings to a backup point, or restore the default factory settings.

To access the Configuration Backup/Restore page, click **MAINTENANCE** > **Configuration Backup/Restore**.



Backup Settings

To backup the current settings, click the **Backup Settings** button.

Restore Settings

To restore settings from a backup point, do the following:

1. Click the **Browse** button.
2. Browse for the backup file, and then click the **Open** button.

3. Click the **Restore Settings** button to restore.

Restore Factory Default

You can restore the Wireless Gateway to its factory defaults. However, doing so will delete all your settings. To restore the factory defaults, do the following:

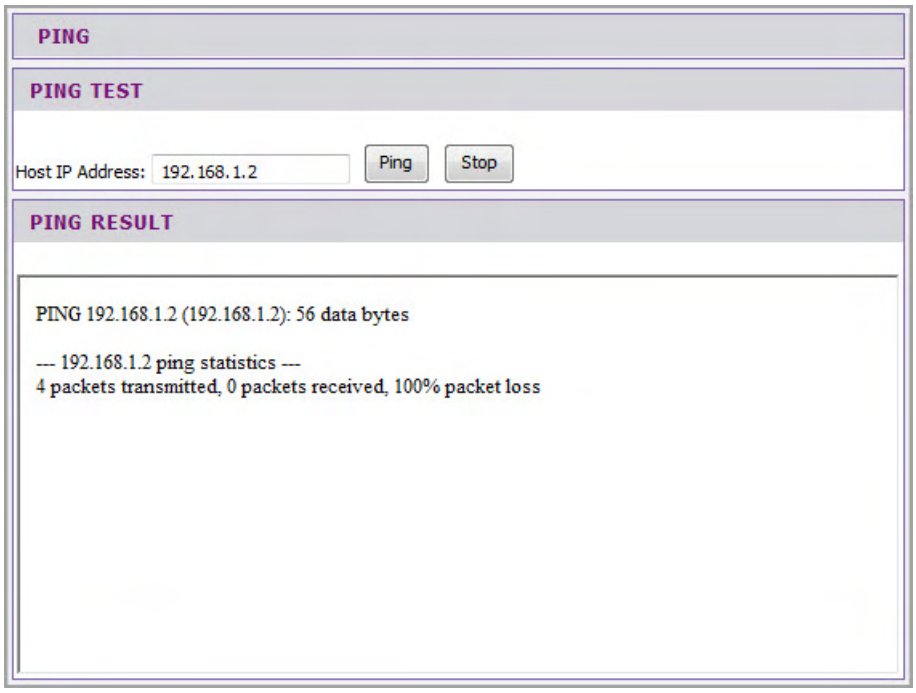
1. Click the **Restore** button.
2. When prompted, click the **OK** button.
3. A warning message appears. Click the **OK** button to continue.

> **NOTE:**
>
> Restoring to factory defaults may take some time. Do not turn off the Wireless Gateway.

7.9 Ping

Once you have configured your Wireless Gateway, it is recommended to ping the network devices to verify their connection. When you execute a ping test, a series of packets are sent to a specific computer. When the computer receives the packets, it will respond with an acknowledgment that it received the packets.

To access the Ping page, click **MAINTENANCE** > **Ping**.

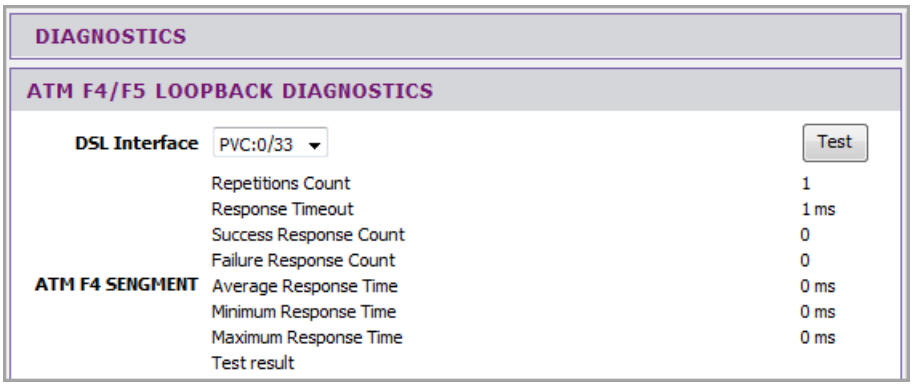


Host IP Address — Enter the IP address of the network device that you want to ping. Click the **Ping** button to start ping. The results are displayed on the PING RESULT screen.

7.10 Diagnostics

This page allows you to test the connectivity of the physical and protocol layers on the WAN side.

To access the Diagnostics page, click **MAINTENANCE** > **Diagnostics**.

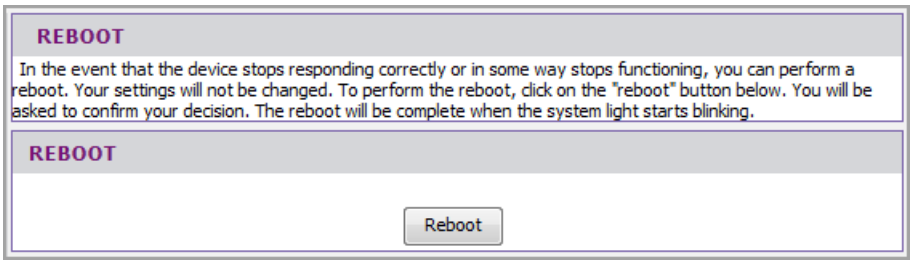


To start the test, select the **DSL Interface** from the drop-down list, and then click the **Test** button.

7.11 Reboot Device

In the event that your device does not respond correctly or stops responding, reset your device. All your settings will be retained.

1. Click **MAINTENANCE** > **Diagnostics**.



2. Click the **Reboot** button.
3. Click **OK** to confirm.
4. When prompted, click **OK**.

NOTE:

Rebooting the Wireless Gateway may take some time. Do not turn off the power until the reboot is complete.

Chapter 8: Status

The Status menu provides the current status and settings of your Wireless Gateway.

8.1 Summary

This page displays the summary of the system, DSL link, ATM PVC, Internet connection, LAN, and wireless ports status.

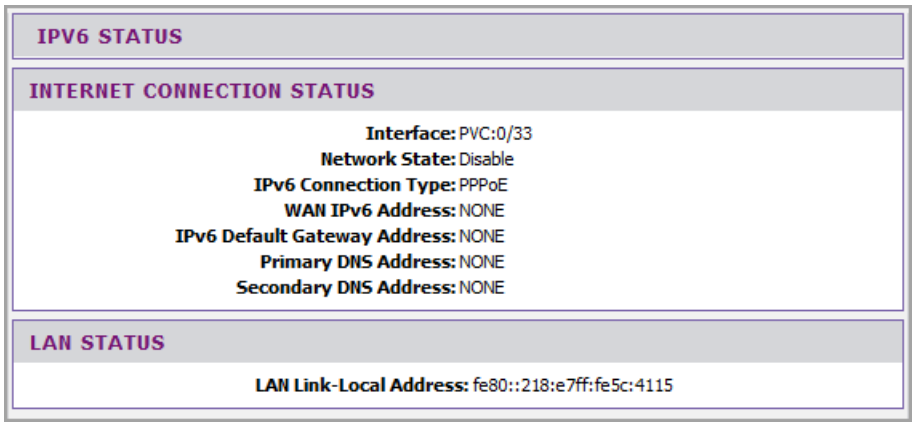
To access the Summary page, click **STATUS** > **Summary**.

The status is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.2 IPv6 Info

This page displays the status of the IPv6 Internet and LAN status.

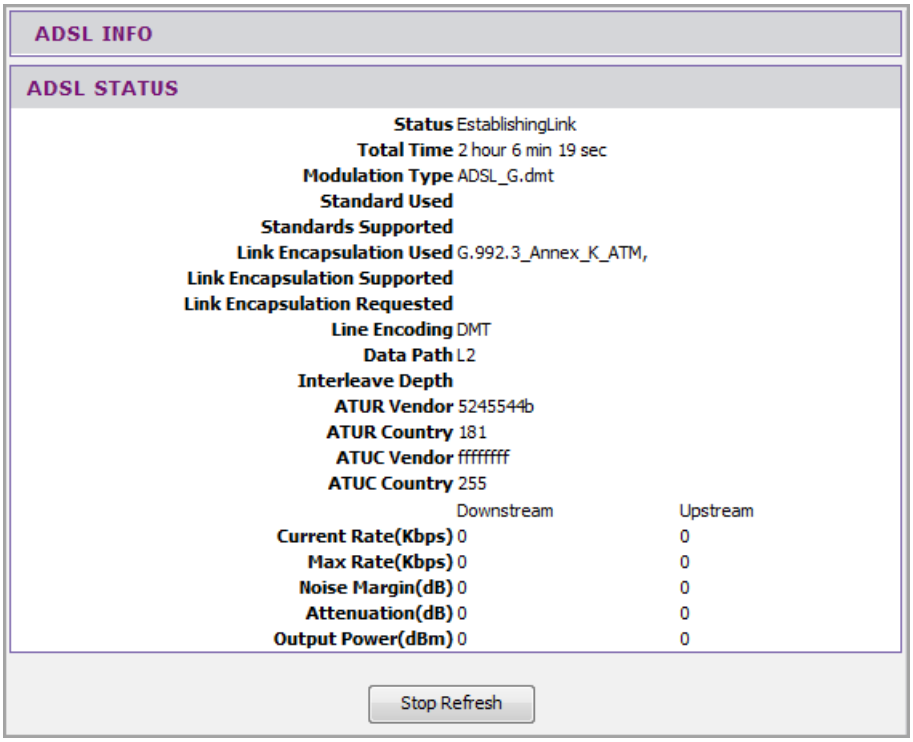
To access the IPv56 Info page, click **STATUS** > **IPv6 Info**.



8.3 ADSL Info

This page displays the status of your DSL line.

To access the ADSL Info page, click **STATUS** > **ADSL Info**.



The status of the ADSL connection is displayed:

Status — Displays the ADSL connection status.

Total Time — Displays the total time when the Wireless Gateway is connected to ADSL.

Modulation Type — Displays the modulation type.

Standard Used — Displays the standard being used.

Standards Supported — Displays the supported standards.

Link Encapsulation Used — Displays the used link encapsulation mode.

Link Encapsulation Supported — Displays the supported link encapsulation mode.

Link Encapsulation Requested — Displays the requested link encapsulation mode.

Line Encoding — Displays the line encoding.

Data Path — Displays the data path.

Interleaved Depth — Displays the interleaved depth.

ATUR Vendor — Displays the ATUR vendor.

ATUR Country — Displays the ATUR country.

ATUC Vendor — Displays the ATUC vendor.

ATUC Country — Displays the ATUC country.

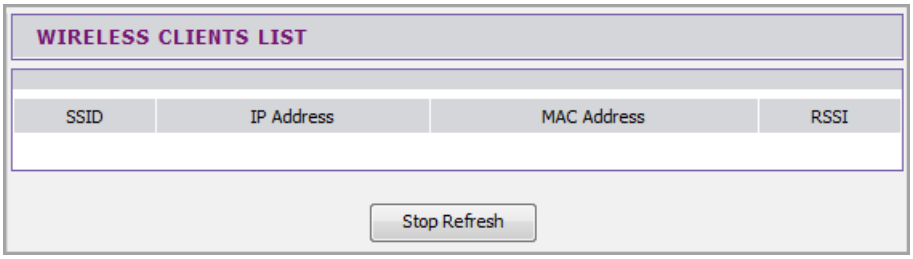
The Downstream and Upstream rates are displayed as **Current Rate**, **Max Rate**, **Noise Margin**, **Attenuation**, and **Output Power**.

The status is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.4 Wireless Clients

This page displays the clients connected on your network via wireless connection.

To access the Wireless Clients page, click **STATUS** > **Wireless Clients**.

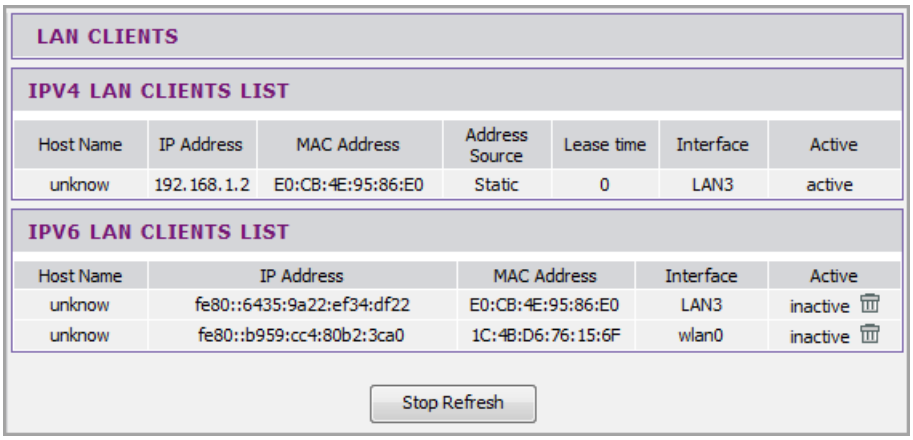


The list is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.5 LAN Clients

This page displays the clients connected on your network.

To access the LAN Clients page, click **STATUS** > **LAN Clients**.

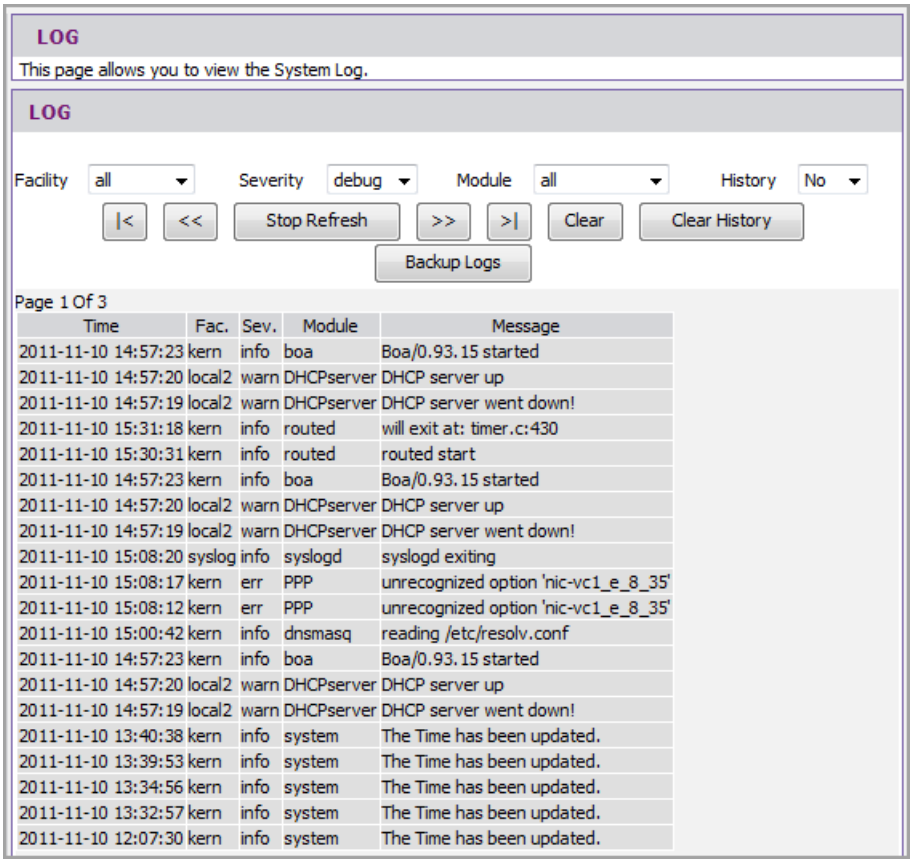


The lists are automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.6 Logs

This page allows you to view, clear, and backup system logs.

To access the Logs page, click **STATUS** > **Logs**.



Time	Fac.	Sev.	Module	Message
2011-11-10 14:57:23	kern	info	boa	Boa/0.93.15 started
2011-11-10 14:57:20	local2	warn	DHCPserver	DHCP server up
2011-11-10 14:57:19	local2	warn	DHCPserver	DHCP server went down!
2011-11-10 15:31:18	kern	info	routed	will exit at: timer.c:430
2011-11-10 15:30:31	kern	info	routed	routed start
2011-11-10 14:57:23	kern	info	boa	Boa/0.93.15 started
2011-11-10 14:57:20	local2	warn	DHCPserver	DHCP server up
2011-11-10 14:57:19	local2	warn	DHCPserver	DHCP server went down!
2011-11-10 15:08:20	syslog	info	syslogd	syslogd exiting
2011-11-10 15:08:17	kern	err	PPP	unrecognized option 'nic-vc1_e_8_35'
2011-11-10 15:08:12	kern	err	PPP	unrecognized option 'nic-vc1_e_8_35'
2011-11-10 15:00:42	kern	info	dnsmasq	reading /etc/resolv.conf
2011-11-10 14:57:23	kern	info	boa	Boa/0.93.15 started
2011-11-10 14:57:20	local2	warn	DHCPserver	DHCP server up
2011-11-10 14:57:19	local2	warn	DHCPserver	DHCP server went down!
2011-11-10 13:40:38	kern	info	system	The Time has been updated.
2011-11-10 13:39:53	kern	info	system	The Time has been updated.
2011-11-10 13:34:56	kern	info	system	The Time has been updated.
2011-11-10 13:32:57	kern	info	system	The Time has been updated.
2011-11-10 12:07:30	kern	info	system	The Time has been updated.

You can filter the list by selecting a particular **Facility**, **Severity**, **Module**, or **History** from the drop-down lists.

The log is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

Click the **|<** **<<** **>>** **>|** buttons to scroll through the logs.

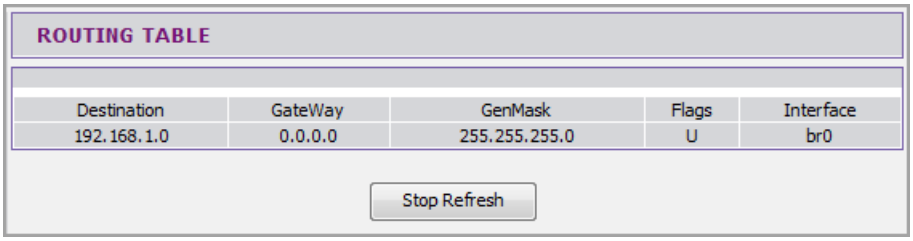
Click the **Clear History** button to delete old logs.

Click the **Backup Logs** button to save a backup of the logs.

8.7 Routing Table

This page displays the destination routes commonly accessed by your network.

To access the Routing Table page, click **STATUS** > **Routing Table**.

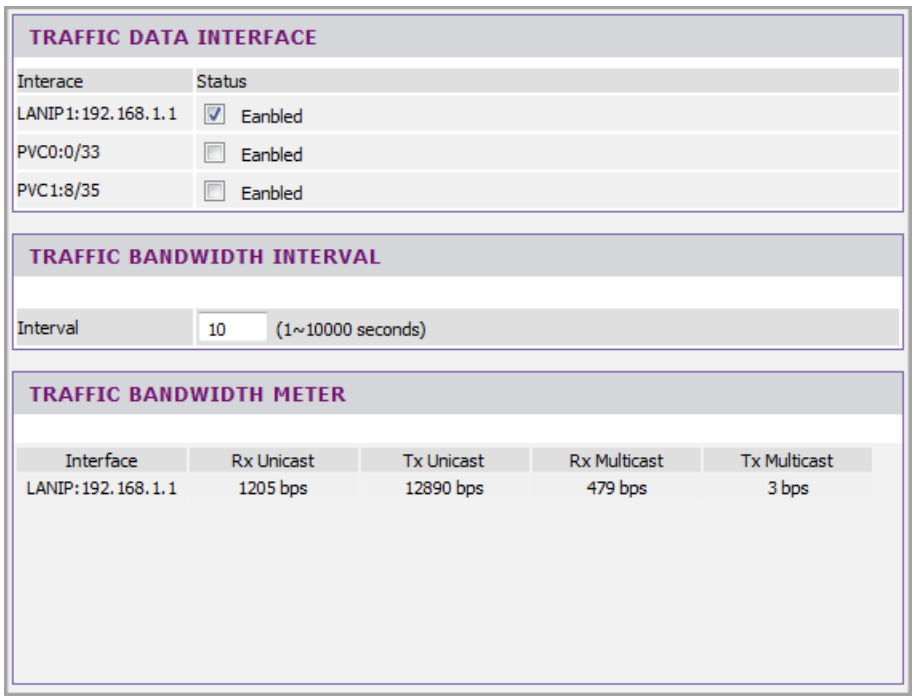


The routing table is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.8 Traffic Meter

This page displays the transmission and reception statistics of packets that pass through the specified interface.

To access the Traffic Meter page, click **STATUS** > **Traffic Meter**.



Traffic Data Interface

The table lists the available interfaces on your network. Check the **State** box of the interface to view its traffic. You may check more than one interface.

Traffic Bandwidth Interval

Interval — Enter the interval of refreshing the traffic bandwidth.

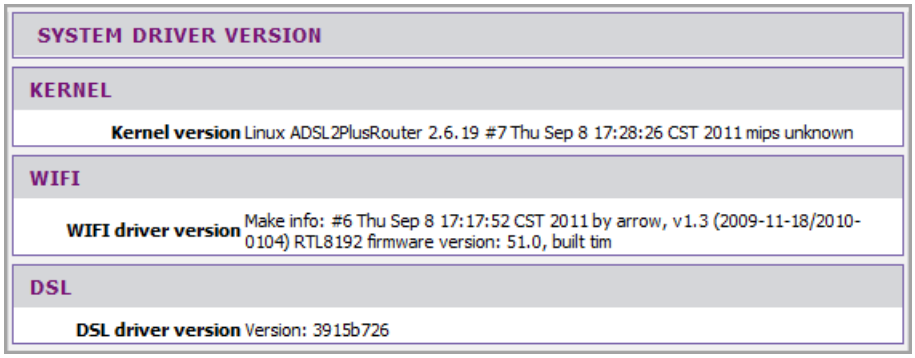
Traffic Bandwidth Meter

This table lists the current traffic.

8.9 Driver Version

This page displays the current kernel, Wi-Fi, and DSL driver versions.

To access the Driver Version page, click **STATUS** > **Driver Version**.

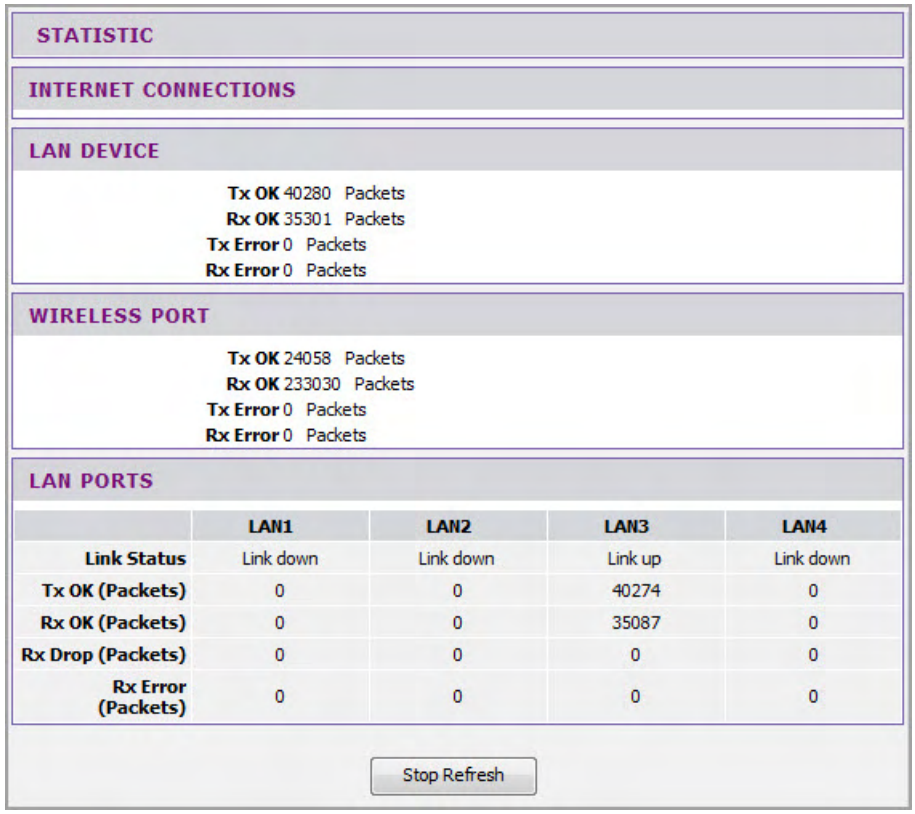


8.10 Statistics

8.10.1 Basic Statistics

This page displays the transmission and reception statistics of the Internet connection, LAN device, wireless port, and the LAN ports.

To access the Basic Statistics page, click **STATUS** > **Statistics** > **Basic Statistics** or click the **Basic Statistics** button.

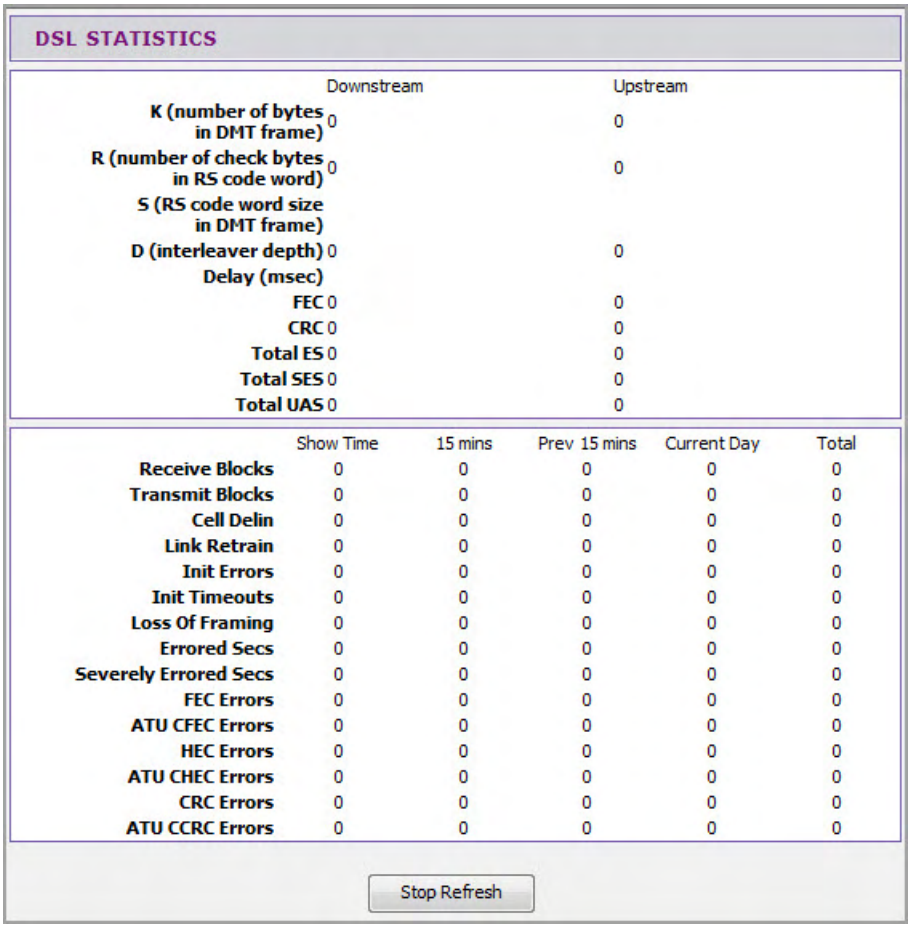


The statistics is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

8.10.2 Statistics > DSL Statistics

This page displays the transmission and reception statistics of the DSL line.

To access the DSL Statistics page, click **STATUS** > **Statistics** > **DSL Statistics** or click the **DSL Statistics** button.



The statistics is automatically refreshed every 10 seconds. To stop automatic refresh, click the **Stop Refresh** button.

Appendix

A. Wireless Considerations

Connection Performance

A number of factors affect wireless connections. To ensure high-range and stable connectivity, do the following:

1. Keep the Wireless Gateway and other wireless devices away from obstructions, such as walls or buildings. Each obstruction can reduce the range of a wireless device.

2. Keep the Wireless Gateway and other wireless devices away from devices that produce radio frequency (RF) noise, such as microwave ovens or radios.

3. Keep the Wireless Gateway and other wireless devices away from any device operating on the 2.4GHz frequency, such as cordless phones or remote controls.

Security Checklist

Wireless network signals can be intercepted easily. To prevent unauthorized users from connecting to your wireless network, follow the guidelines below.

1. Change the default wireless network name.

   Your device has a default Service Set Identifier (SSID) which is the wireless network name. Change the SSID with a unique name to identify your network. The SSID can be up to 32 characters in length.

2. Change the default password.

   Your device has a default password. You have to enter this password to change your network settings. Change the password to prevent unauthorized users from hacking into your network and changing the settings.

3. Enable MAC address filtering.

   Your device supports Media Access Control (MAC) address filtering. You can assign a MAC address on each computer that you want to connect to your wireless network. When MAC address filtering is enabled, only the computers with the specified MAC addresses are allowed access.

4. Enable encryption

   Your device supports Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WAP/WPA2) encryption. To ensure a high level of security, enable the highest security encryption and use strong passphrases, avoid using words that can be found in the dictionary.

B. Regulatory & Safety Information

Wireless LAN, Health and Authorization

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

Onboard airplanes, or

In an explosive environment, or

In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

FCC (Federal Communications Commission) Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that my cause undesired operation of this device.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

CE statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1: 2006

Safety of Information Technology Equipment

EN 50385: 2002

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V2.1.1 (2009-05)

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for Broadband Data Transmission Systems.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

C. Specifications

IC	• Main chip: RTL8672 • AFE: RTL8271B • Ethernet: RTL8305N • WiFi: RTL8188RE • DDR1: 32MB • Flash: 4MB or 8 MB Serial (depends on software requirement)
User Interface	• ADSL2+: POTS • 1x1 11n 2.4GHz single band • 4x 10/100 Base-T Ethernet LAN ports
Buttons	• 1 x Power ON/OFF button • 1 x WPS button • 1 x Reset to default button
LEDs	Front panel • Power LED • Ethernet LED • Wi-Fi LED • WPS LED • ADSL LED • Internet LED Back panel • 4 x Ethernet LEDs
IO Ports	• 1 x RJ-11 DSL connector • 4 x RJ-45 Ethernet connector • 1 x DC In jack
Antenna	Standard: 1 internal printed antenna
DC inputs	12VDC 1A
Temperature	Operating: 0°C ~ 40° C Storage: -10°c ~ 70°C
Humidity	Operating: 10% ~ 95%, RH, no condensation
PCB Dimensions	142 x 117 x 1.6 mm