Ethernet Wireless Router

User Manual

VERSION 0.1

⚠ Safety Precautions

- Do not open, service, or change any component.
- Only qualified technical specialists are allowed to service the equipment.
- Observe safety precautions to avoid electric shock
- Check voltage before connecting to the power supply. Connecting to the wrong voltage will damage the equipment.

Copyright © 2006. All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission of the owner. Product specifications contained in this document are subject to change without notice. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

Contents

About this Manual

This manual provides a description of the components, basic operation, and advanced configuration options of the router.

Scope and Purpose

This manual provides the following:

- Installation instructions
- Description of the router components and the web interface
- Operating instructions of the router and the web interface

Target Audience

This manual is designed and developed for users who are required to install and maintain the router. It assumes the user of this manual has basic knowledge and experience in configuring routers, computer networks, and computer systems.

Document Structure

The manual is divided into the following sections:

Chapter	About
1	About the router
2	Understanding the web interface
3	Basic setup
4	Advanced settings
5	Diagnostics

About the Router

Congratulations on the purchase of your router. This router provides advanced features that allow you to converge your phone, Internet, and other network appliances into a single network either through wired or wireless connection.

Requirements

Your computer must meet the following minimum requirements.

Software

Operating System:

- Any operating system can be used

Browser:

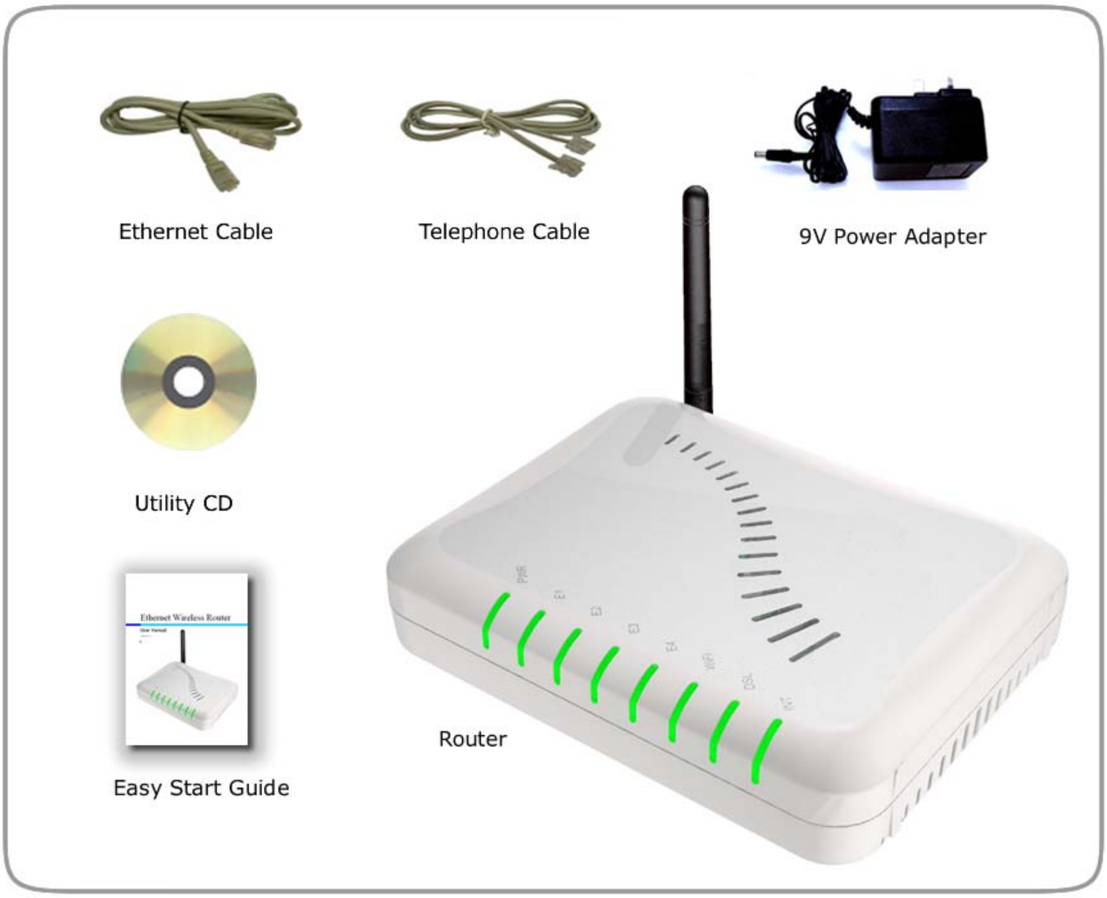
- Internet Explorer 4.0
- Netscape Navigator 3.02

Hardware

- 233MHz processor
- CD-ROM Drive
- Ethernet network adapter

Package Contents

For any missing items, please contact your dealer immediately. Product contents vary for different models.

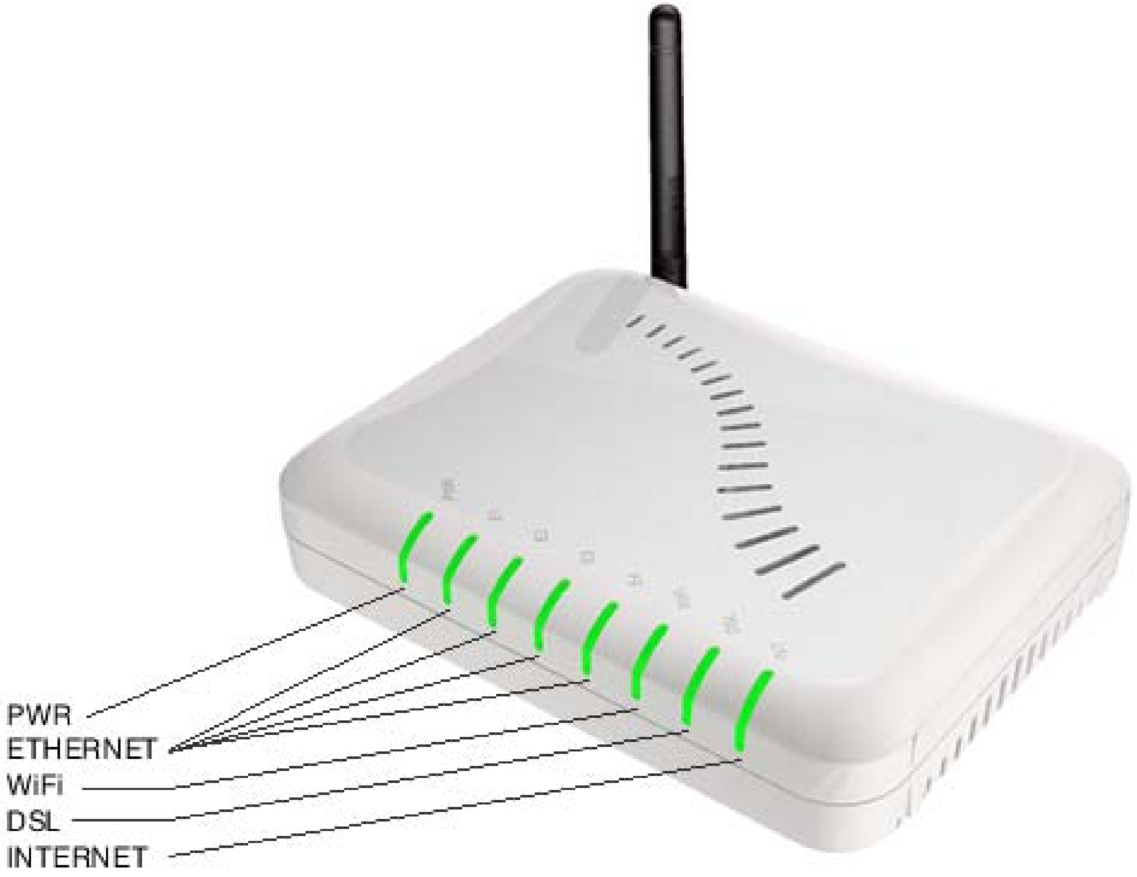


Package Contents

Device Design

Front Panel

The LEDs on the front panel gives you an idea about the power and connection status.

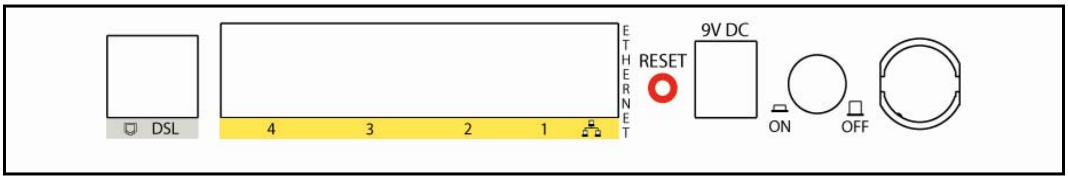


Label	Action	Description
POWER	Off	No power is supplied to the device
	Steady light	Connected to an AC power supply
ETHERNET	Off	No Ethernet connection
	Steady light	Connected to an Ethernet port
	Blinking light	Transmitting/Receiving data
WiFi	Off	Access point is disabled
	Steady light	Access point is enabled

	Blinking light	Transmitting/Receiving data
DSL	Off	No DSL signal
	Blinking light	Establishing DSL signal
	Steady light	DSL signal is established
INTERNET	Off	No Internet connection
	Steady light	Connected to the Internet
	Blinking light	Transmitting/Receiving data

Back Panel

The back panel provides ports to power up and connect the router into the network.

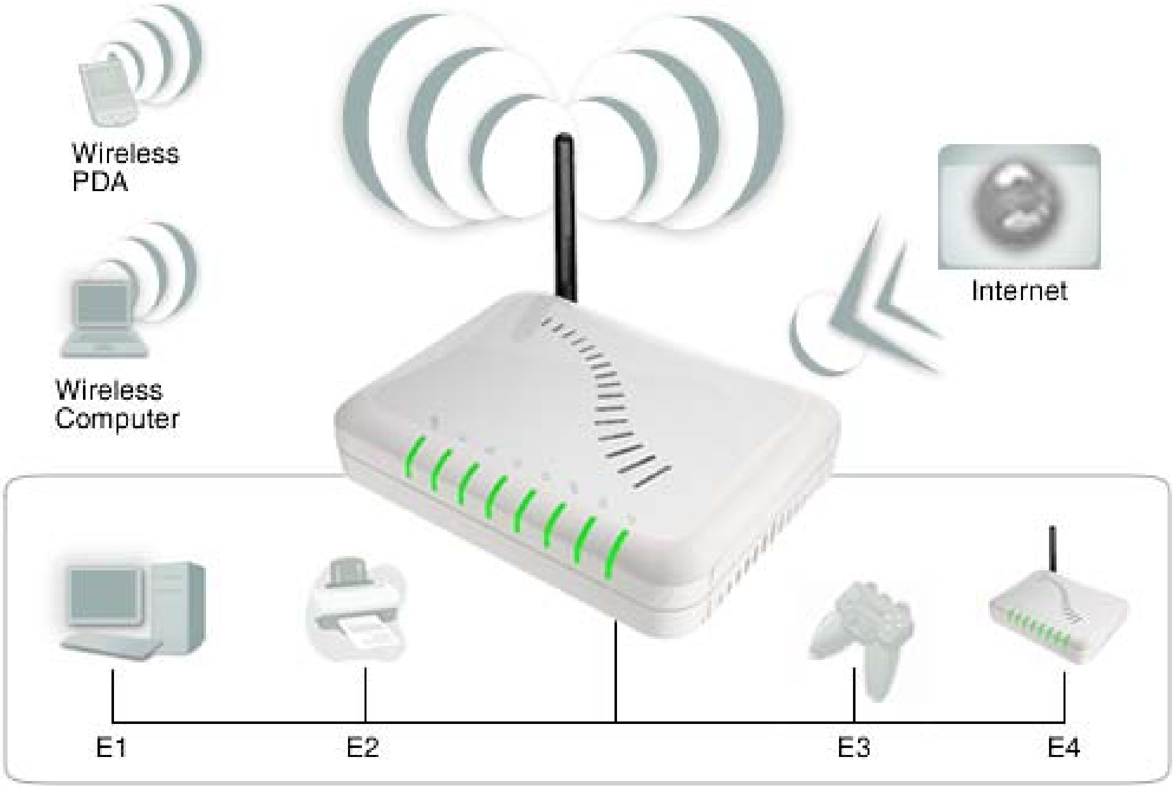


Back Panel

Label	Used for...
DSL	Connecting the telephone cable
ETHERNET 1-4	Connecting with computers/devices through Ethernet cable
RESET	Resetting the device. Press for 10 seconds to reset.
9V DC	Connecting with the 9V power adapter
ON/OFF	Switching the device on/off
Antenna	Sending/receiving wireless signals

Planning Your Network

Before moving ahead to setup your network, it is a good idea to draw out a network diagram to help identify the devices and plan out how to connect these devices. The illustration below is an example of a network diagram.



Sample network diagram

To create a network diagram:

- For wireless devices, identify the wireless devices you want to include in the network
- For wired devices, identify which router port you want to use for each device.

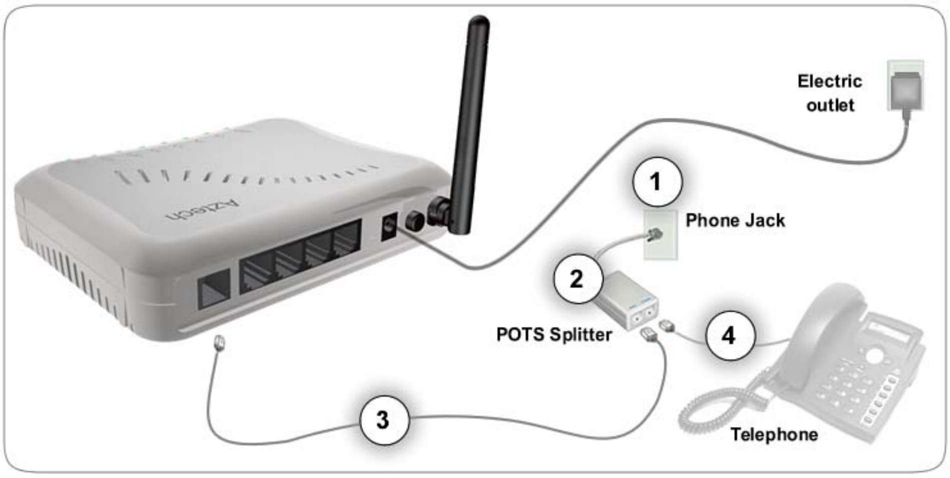
Installing the Router

When installing the router, the common practice is to have the router, the main computer, and phone jack in the same room. The room should also have enough electrical outlets to match your needs.

Connecting with the POTS Splitter

A phone line can carry phone call and Internet signals. When you enable the phone line for high speed Internet, the connection produces high-pitched tones when using the phone. Installing a Plain Old Telephone Service (POTS) splitter separates the two signals and eliminates the noise.

Note: Consult your service provider what type of POTS Splitter should be used.



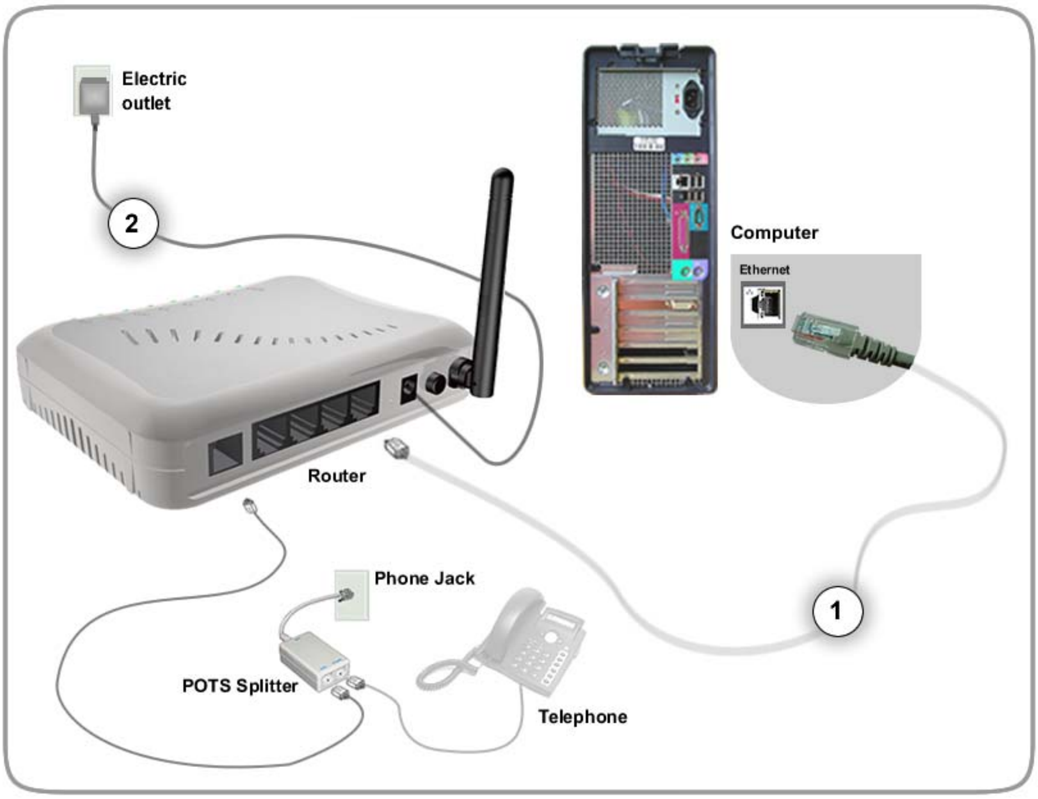
The POTS Splitter separates the connection for the router and telephone

To connect with the POTS Splitter:

1. Locate the phone jack in your house.
2. Insert the POTS Splitter into the phone jack.
3. Plug one end of the telephone cable from the POTS Splitter's **ADSL** port and then plug the other end into the router's **DSL** port.
4. Plug one end of the telephone cable from the POTS Splitter's **TEL** port and then plug the other end into the telephone.

Connecting with the Computer

You need to connect the router with the computer before connecting with other devices. The computer will be used to configure the router settings.



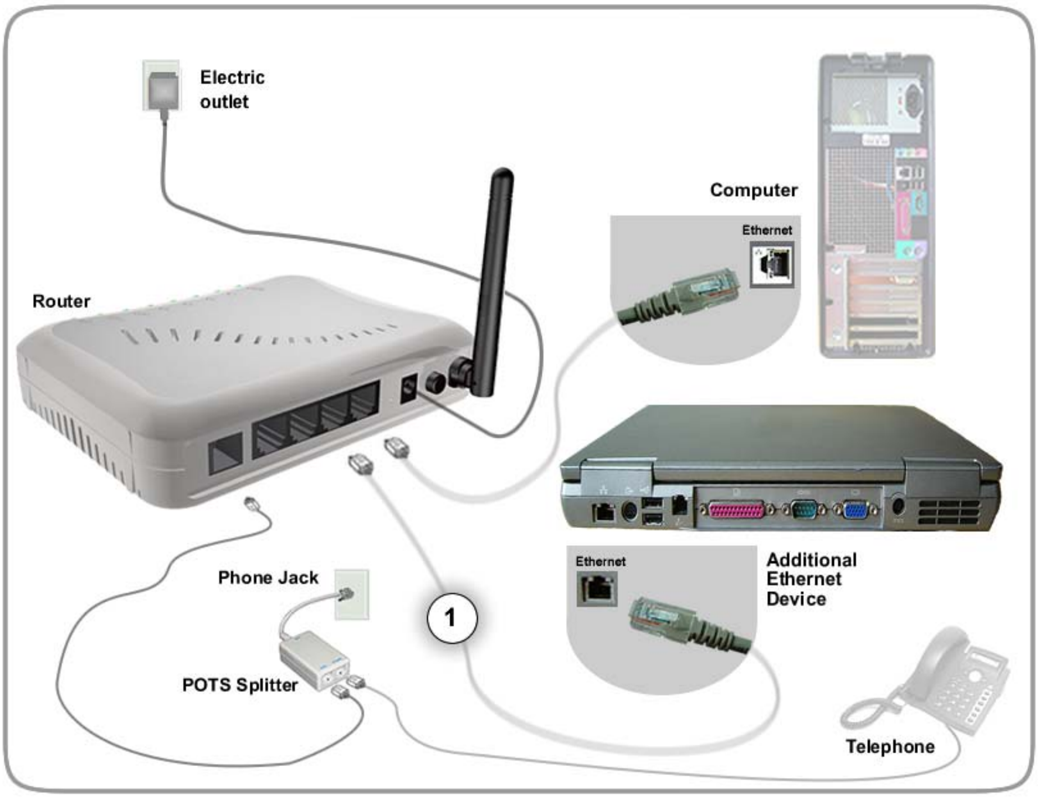
Connecting the router with the computer

To connect with the computer:

1. Plug one end of the Ethernet cable from the router's **ETHERNET** port and then plug the other end into the Ethernet port in your computer.
2. Connect the power adapter from the router's **9V DC** port into the electrical outlet.
3. Use the web interface to configure the device settings. Please refer to Using the Setup Menu.

Connecting Other Ethernet Devices

Aside from the main computer, you can grow your network by adding devices with Ethernet ports. Connect these devices into available Ethernet ports on the router.



Connecting other devices

To the connect with other devices:

1. Plug one end of the Ethernet cable from computer's Ethernet port and then plug the other end into the router's vacant **E** port.

2. Use the web interface to configure the settings for the newly added device.

Connecting Wireless Devices

After you setup the device settings through the main computer, you can connect other devices with wireless capabilities. Wireless devices relieve you from the task of laying out cables and allow you to use the Internet connection from your router.

Your router allows you to connect with several wireless devices

To the connect with wireless devices:

1. Turn on your wireless device.
2. Open the software you use to detect a wireless connection. This opens a window to ask for the connection settings.
3. Enter the connection settings. These settings are defined in your router during setup. For more details about wireless connections, please refer to Wireless Menu.

Understanding the Web Interface

Web Interface Components

Buttons, commands, and menus make up the browser-based user interface.

Buttons

Apply

Click to implement the configuration changes. Clicking Apply will not implement the changes when the router is restarted.

Cancel

Click to revert to the last saved configuration.

Commands

Save Setting

Click to permanently apply configuration changes.

Restart Router

Restarts the router

Restart Access Point

Restarts the wireless connection

Menus

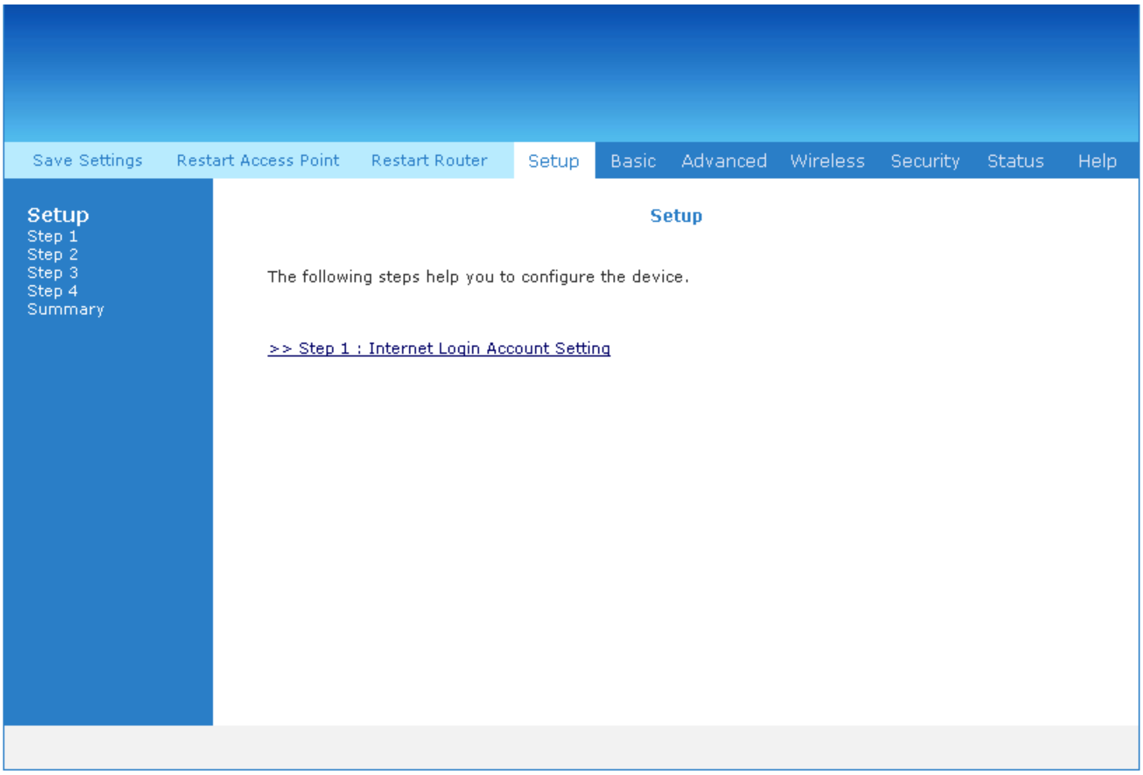
The web interface includes the following menus:

- Setup Menu
- Basic Menu
- Advanced Menu

- Wireless Menu
- Security Menu
- Status Menu
- Help Menu

Setup Menu

The Setup menu is used to complete the initial device configuration.



Setup

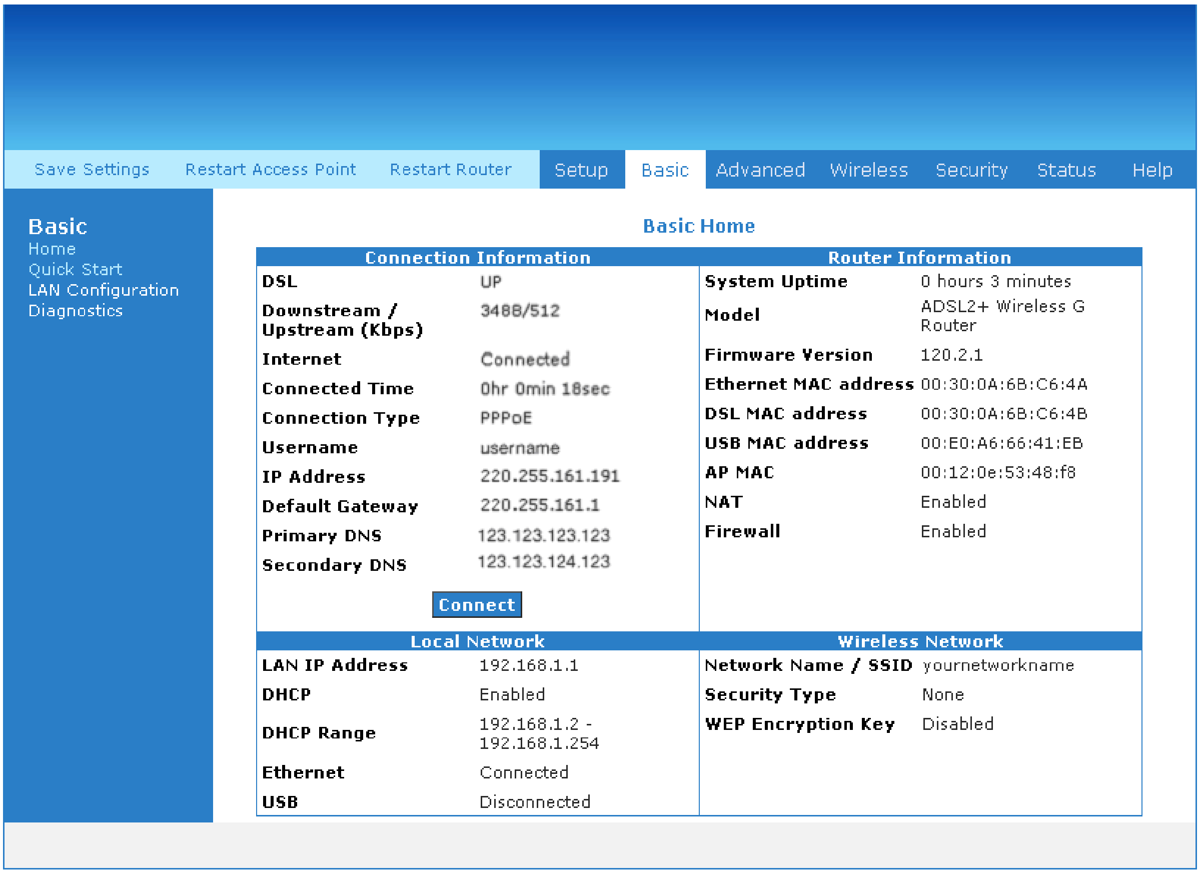
The following steps help you to configure the device.

>> Step 1 : Internet Login Account Setting

Setup Menu

Basic Menu

The Basic Menu provides the Home, Quick Start, LAN Configuration, and Diagnostics links.



Basic Home

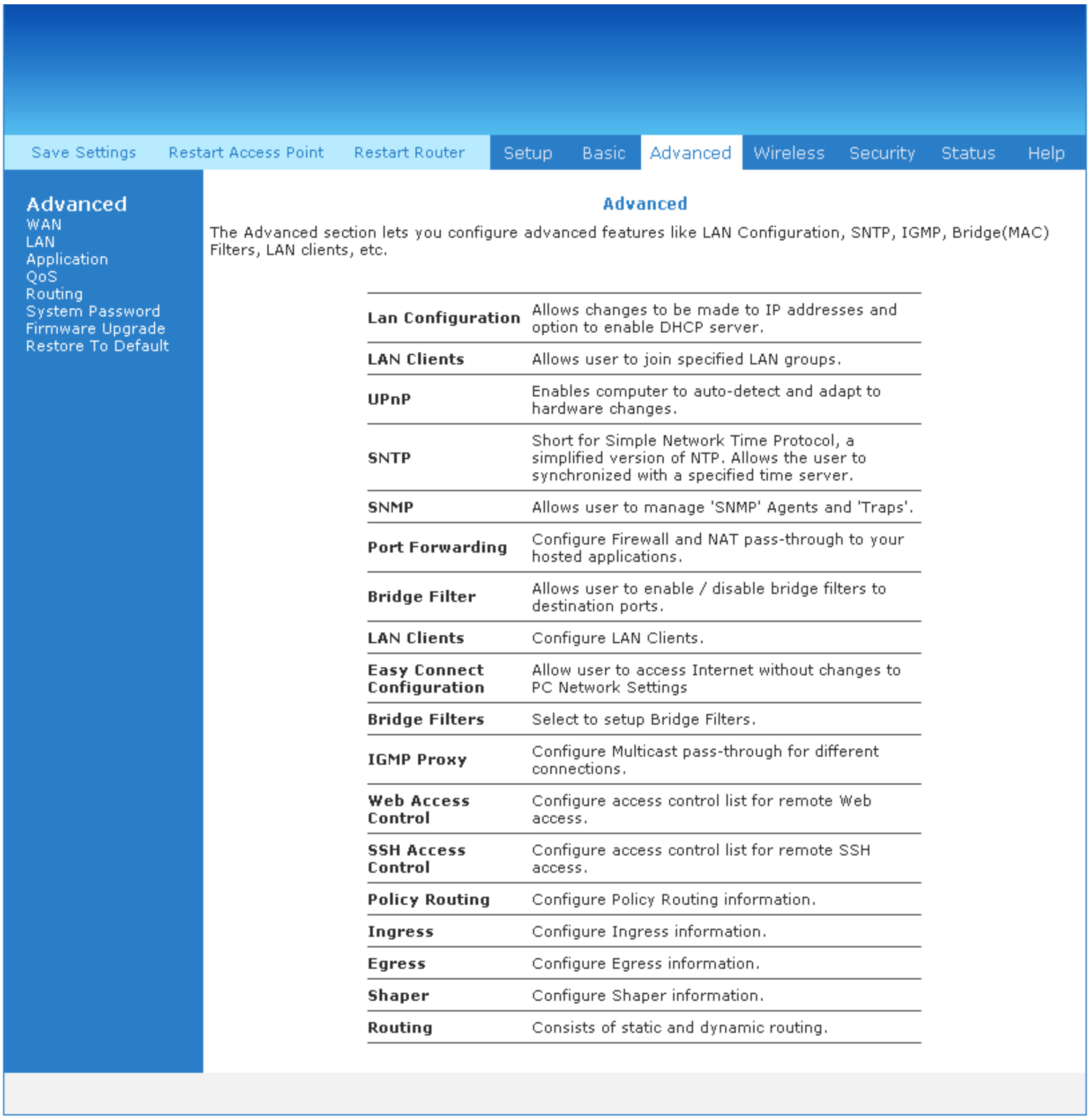
Connection Information		Router Information	
DSL	UP	System Uptime	0 hours 3 minutes
Downstream / Upstream (Kbps)	3488/512	Model	ADSL2+ Wireless G Router
Internet	Connected	Firmware Version	120.2.1
Connected Time	0hr 0min 18sec	Ethernet MAC address	00:30:0A:6B:C6:4A
Connection Type	PPPoE	DSL MAC address	00:30:0A:6B:C6:4B
Username	username	USB MAC address	00:E0:A6:66:41:EB
IP Address	220.255.161.191	AP MAC	00:12:0e:53:48:f8
Default Gateway	220.255.161.1	NAT	Enabled
Primary DNS	123.123.123.123	Firewall	Enabled
Secondary DNS	123.123.124.123		

Local Network		Wireless Network	
LAN IP Address	192.168.1.1	Network Name / SSID	yournetworkname
DHCP	Enabled	Security Type	None
DHCP Range	192.168.1.2 - 192.168.1.254	WEP Encryption Key	Disabled
Ethernet	Connected		
USB	Disconnected		

Basic Menu

Advanced Menu

The Advanced mode provides advanced configuration settings for existing connections. At least one WAN connection must be configured before implementing advanced WAN configuration features. At least one LAN group must be defined before implementing advanced LAN configuration features.



Advanced

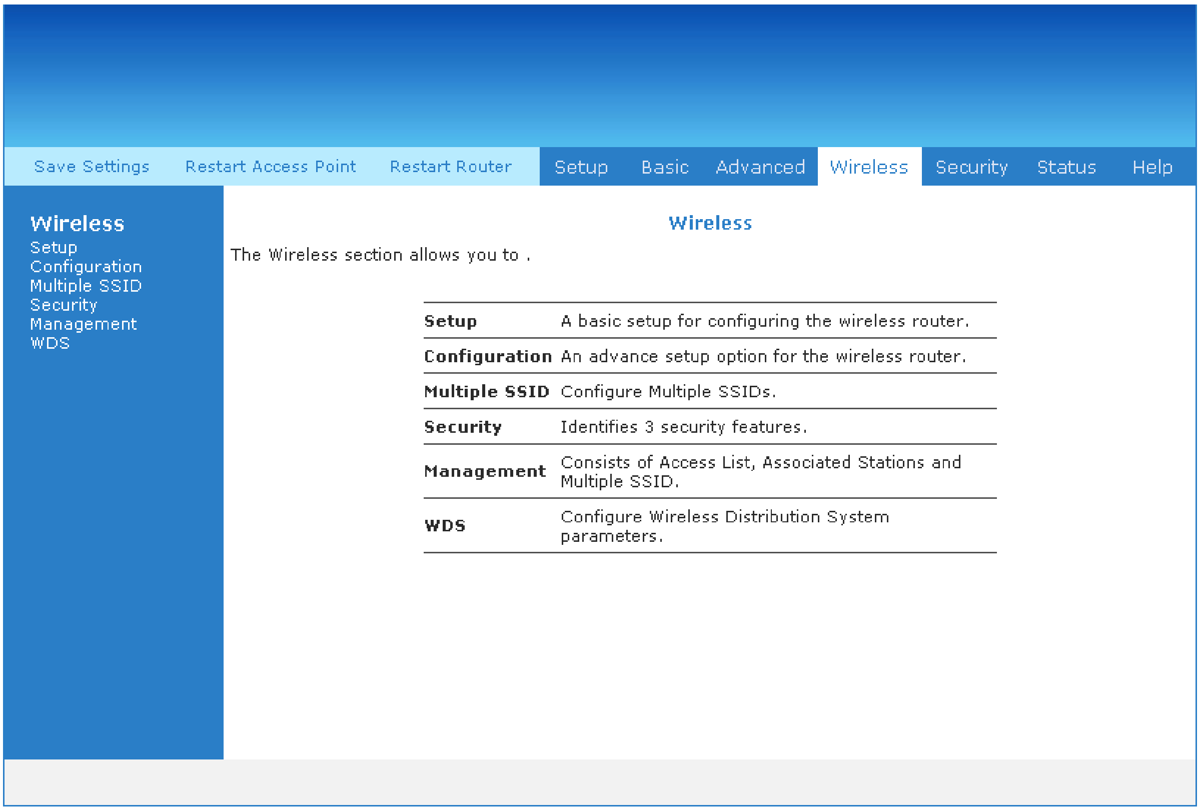
The Advanced section lets you configure advanced features like LAN Configuration, SNTP, IGMP, Bridge(MAC) Filters, LAN clients, etc.

Lan Configuration	Allows changes to be made to IP addresses and option to enable DHCP server.
LAN Clients	Allows user to join specified LAN groups.
UPnP	Enables computer to auto-detect and adapt to hardware changes.
SNTP	Short for Simple Network Time Protocol, a simplified version of NTP. Allows the user to synchronized with a specified time server.
SNMP	Allows user to manage 'SNMP' Agents and 'Traps'.
Port Forwarding	Configure Firewall and NAT pass-through to your hosted applications.
Bridge Filter	Allows user to enable / disable bridge filters to destination ports.
LAN Clients	Configure LAN Clients.
Easy Connect Configuration	Allow user to access Internet without changes to PC Network Settings
Bridge Filters	Select to setup Bridge Filters.
IGMP Proxy	Configure Multicast pass-through for different connections.
Web Access Control	Configure access control list for remote Web access.
SSH Access Control	Configure access control list for remote SSH access.
Policy Routing	Configure Policy Routing information.
Ingress	Configure Ingress information.
Egress	Configure Egress information.
Shaper	Configure Shaper information.
Routing	Consists of static and dynamic routing.

Advanced Menu

Wireless Menu

Wireless Menu allows you to configure the wireless settings.



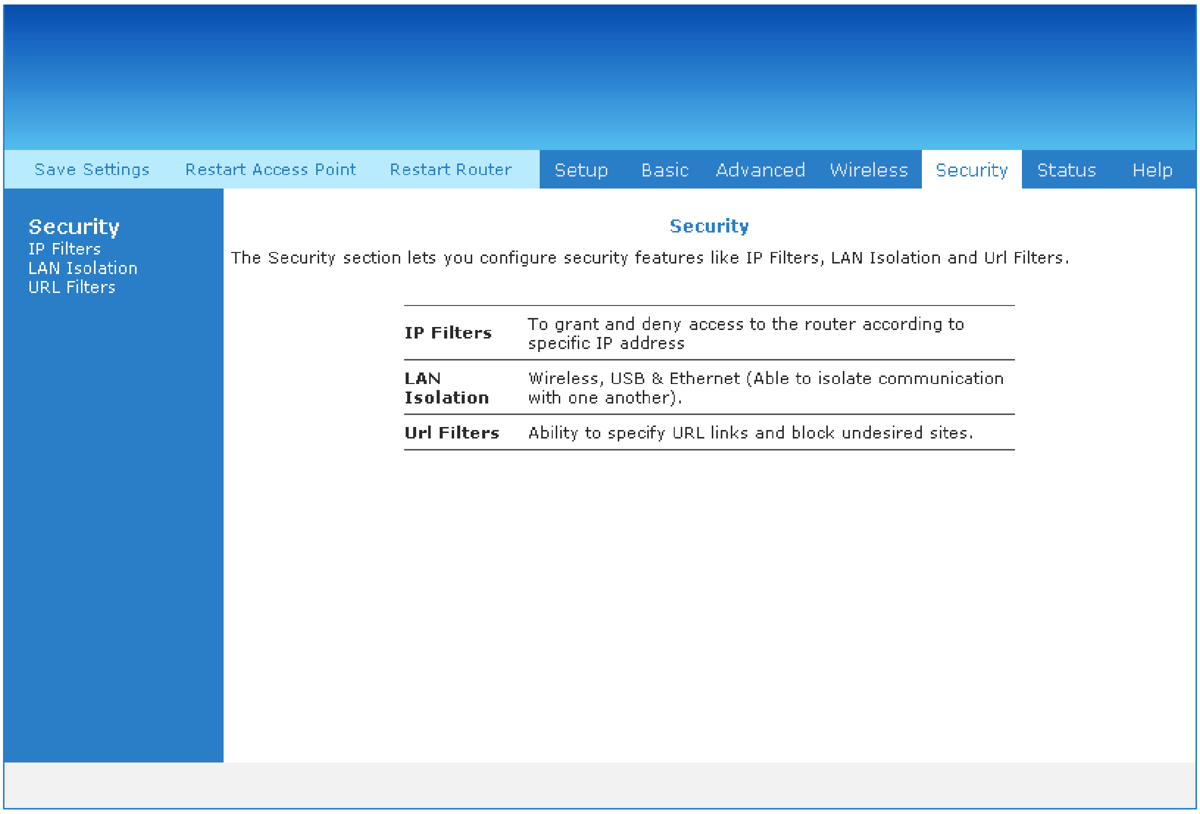
Wireless

The Wireless section allows you to .

Setup	A basic setup for configuring the wireless router.
Configuration	An advance setup option for the wireless router.
Multiple SSID	Configure Multiple SSIDs.
Security	Identifies 3 security features.
Management	Consists of Access List, Associated Stations and Multiple SSID.
WDS	Configure Wireless Distribution System parameters.

Security Menu

Security Menu allows you to configure security tools like IP Filters and LAN Isolation.



Security

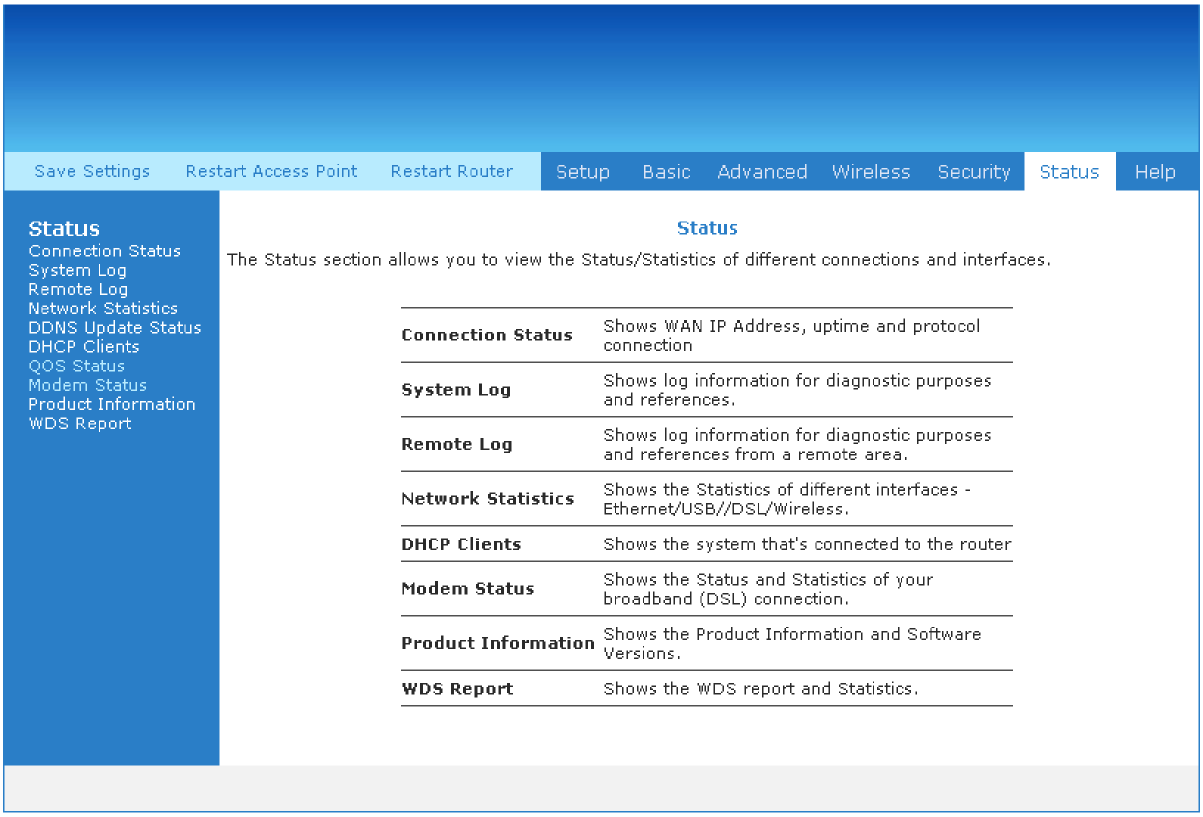
The Security section lets you configure security features like IP Filters, LAN Isolation and Url Filters.

IP Filters	To grant and deny access to the router according to specific IP address
LAN Isolation	Wireless, USB & Ethernet (Able to isolate communication with one another).
Url Filters	Ability to specify URL links and block undesired sites.

Security Menu

Status Menu

The Status Menu provides the status for different connections or interfaces.



Status

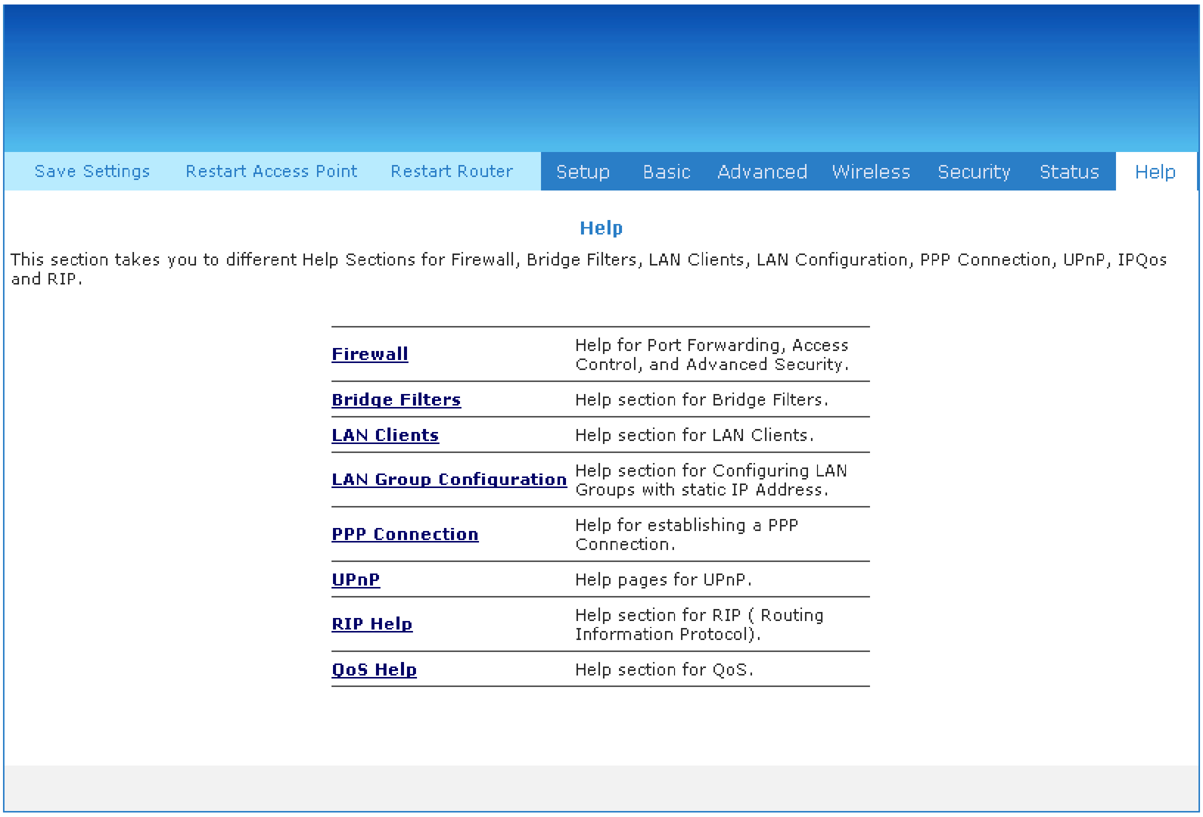
The Status section allows you to view the Status/Statistics of different connections and interfaces.

Connection Status	Shows WAN IP Address, uptime and protocol connection
System Log	Shows log information for diagnostic purposes and references.
Remote Log	Shows log information for diagnostic purposes and references from a remote area.
Network Statistics	Shows the Statistics of different interfaces - Ethernet/USB//DSL/Wireless.
DHCP Clients	Shows the system that's connected to the router
Modem Status	Shows the Status and Statistics of your broadband (DSL) connection.
Product Information	Shows the Product Information and Software Versions.
WDS Report	Shows the WDS report and Statistics.

Status Menu

Help Menu

The Help Menu provides documentation about various router features.



Help

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Configuration, PPP Connection, UPnP, IPQos and RIP.

Firewall	Help for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
LAN Group Configuration	Help section for Configuring LAN Groups with static IP Address.
PPP Connection	Help for establishing a PPP Connection.
UPnP	Help pages for UPnP.
RIP Help	Help section for RIP (Routing Information Protocol).
QoS Help	Help section for QoS.

Help Menu

Setup

This chapter provides information about removing conflicts and configuring device settings.

Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before you install and configure the router.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer’s instructions.

Internet Sharing Applications	Proxy Software	Security Software
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

Configuring TCP/IP Settings

After connecting the device, you need to set the TCP/IP Properties in your computer.

Note: These instructions apply to connections made using the Ethernet port.

To set the TCP/IP properties:

1. Select **Start** > **Run**. This opens the **Run** dialog box.
2. Enter **control** **ncpa.cpl** and then click **OK**. This opens the **Network Connections** in your computer.
3. Right-click **LAN** and then select **Properties**. This opens the **Local Area Connection Properties** dialog box.
4. Select **Internet Protocol (TCP/IP)** and then click **Properties**. This opens the **Internet Protocol (TCP/IP)** dialog box.
5. Select **Obtain an IP address automatically**.
6. Click **OK** to close the **Internet Protocol (TCP/IP)** dialog box.
7. Click **OK** to close the **Local Area Connection Properties** dialog box.

Configuring Internet Properties

To set the Internet Properties:

1. Select **Start** > **Run**. This opens the **Run** dialog box.
2. Enter **control** **inetcpl.cpl** and then click **OK**. This opens the **Internet Properties** dialog box.
3. Click **Connections** tab.
4. In the **Dial-up and Virtual Private Network settings** pane, select **Never dial a connection**.
5. Click **OK** to close the **Internet Properties** dialog box.

Removing Temporary Internet Files

To remove temporary Internet files:

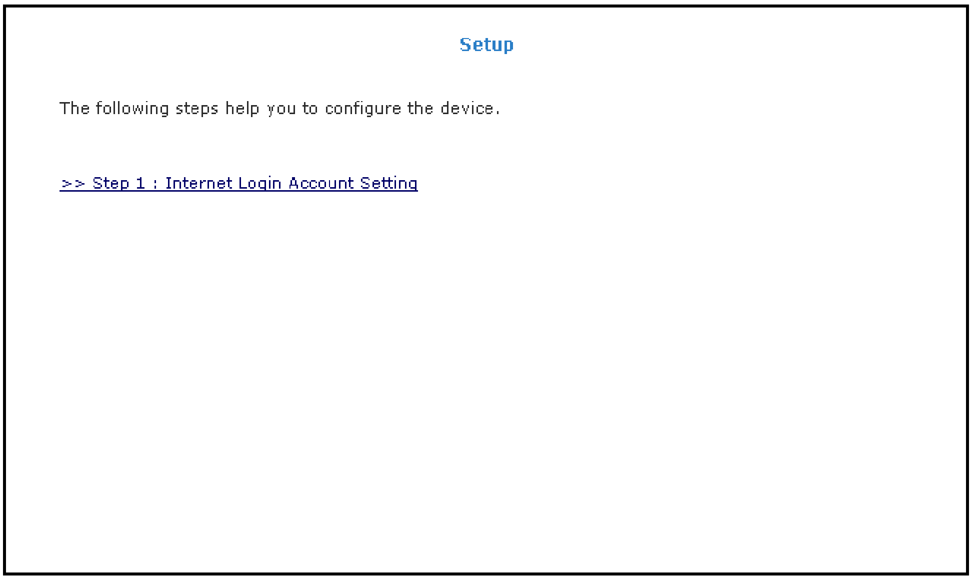
1. Select Start > Run. This opens the Run dialog box.
2. Enter **control** and then click OK. This opens the Control Panel.
3. Double-click Internet Options. This opens the Internet Options dialog box.
4. In the Temporary Internet Files pane, click Delete Cookies.
5. Click Delete Files.
6. Click OK to close the Internet Properties dialog box.

Using the Setup Menu

After connecting the devices, you need to configure the router settings via the web interface.

To open the web interface:

1. Open your browser.
2. Enter **192.168.1.1** in the address field and then press **Enter**. This opens the **Setup** page of the web interface.



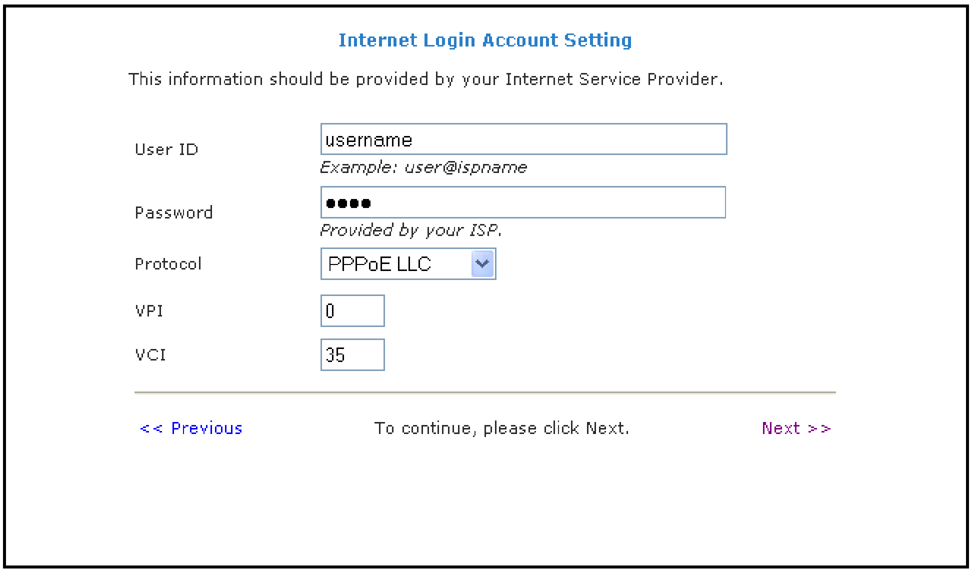
Setup

The following steps help you to configure the device.

>> Step 1 : Internet Login Account Setting

Setup Page

3. Click **Step 1: Internet Login Account Setting**. This opens the **Internet Login Account Setting** page.



Internet Login Account Setting

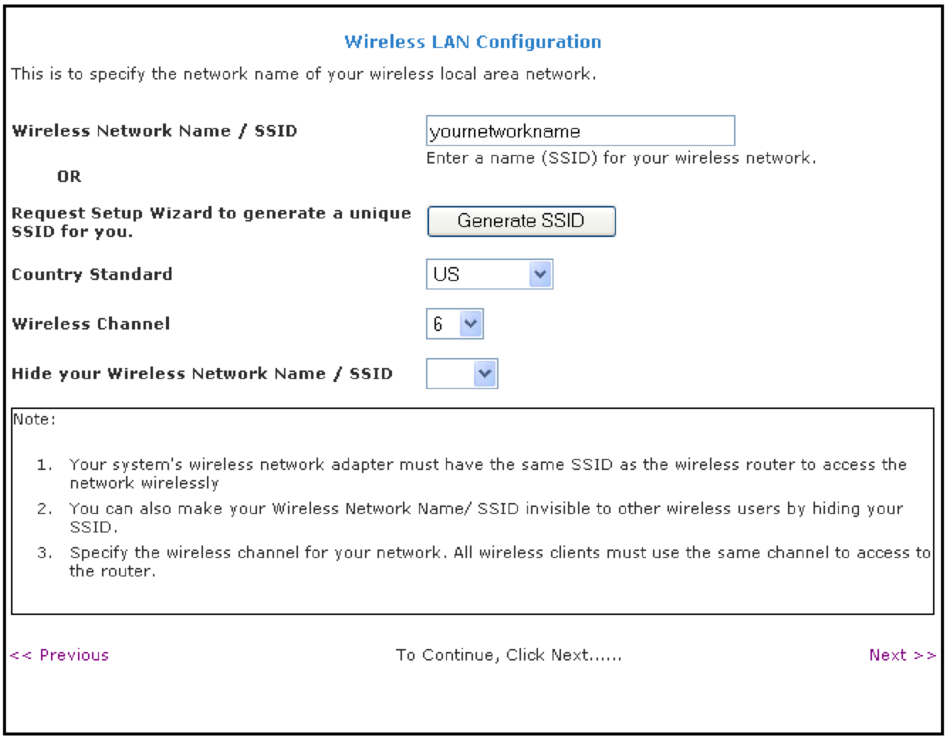
This information should be provided by your Internet Service Provider.

User ID	username *Example: user@ispname*
Password	●●●● *Provided by your ISP.*
Protocol	PPPoE LLC
VPI	0
VCI	35

Internet Login Account Setting page

4. Enter the **User ID**, **Password**, **Protocol**, **VP1**, and **VCI** for your account. These are the account information from your service provider.

5. Click **Next**. This opens the **Wireless LAN Configuration** page.



Wireless LAN Configuration

This is to specify the network name of your wireless local area network.

Wireless Network Name / SSID: yournetworkname

Enter a name (SSID) for your wireless network.

OR

Request Setup Wizard to generate a unique SSID for you. [Generate SSID]

Country Standard: US

Wireless Channel: 6

Hide your Wireless Network Name / SSID:

Note:

1. Your system's wireless network adapter must have the same SSID as the wireless router to access the network wirelessly
2. You can also make your Wireless Network Name/ SSID invisible to other wireless users by hiding your SSID.
3. Specify the wireless channel for your network. All wireless clients must use the same channel to access to the router.

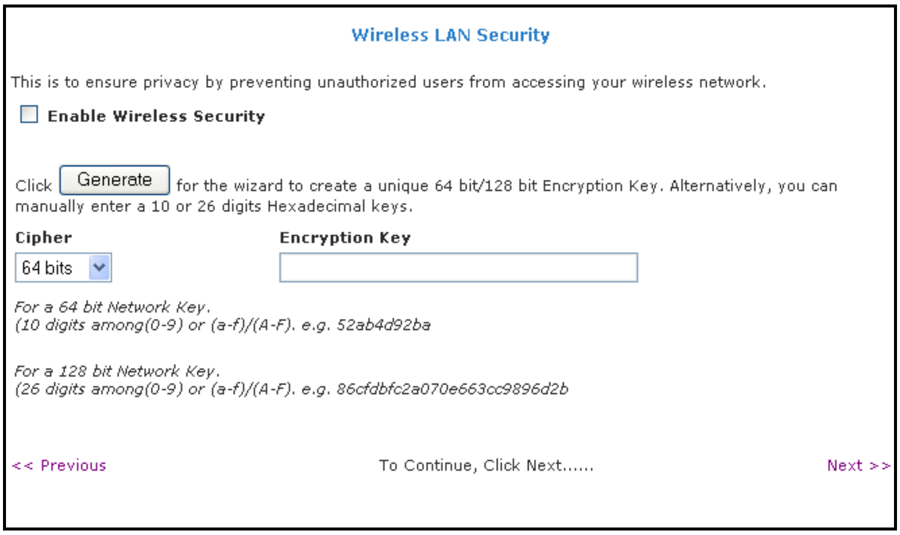
<< Previous To Continue, Click Next...... Next >>

Wireless LAN Configuration page

6. Enter an **SSID, Country Standard,** and **Wireless Channel**.

7. Select **Yes** or **No** to specify if you want to hide your wireless network name or not.

8. Click **Next**. This opens the **Wireless LAN Security** page.



Wireless LAN Security

This is to ensure privacy by preventing unauthorized users from accessing your wireless network.

☐ Enable Wireless Security

Click [Generate] for the wizard to create a unique 64 bit/128 bit Encryption Key. Alternatively, you can manually enter a 10 or 26 digits Hexadecimal keys.

Cipher: 64 bits

Encryption Key:

For a 64 bit Network Key.
(10 digits among(0-9) or (a-f)/(A-F). e.g. 52ab4d92ba

For a 128 bit Network Key.
(26 digits among(0-9) or (a-f)/(A-F). e.g. 86cfdbfc2a070e663cc9896d2b

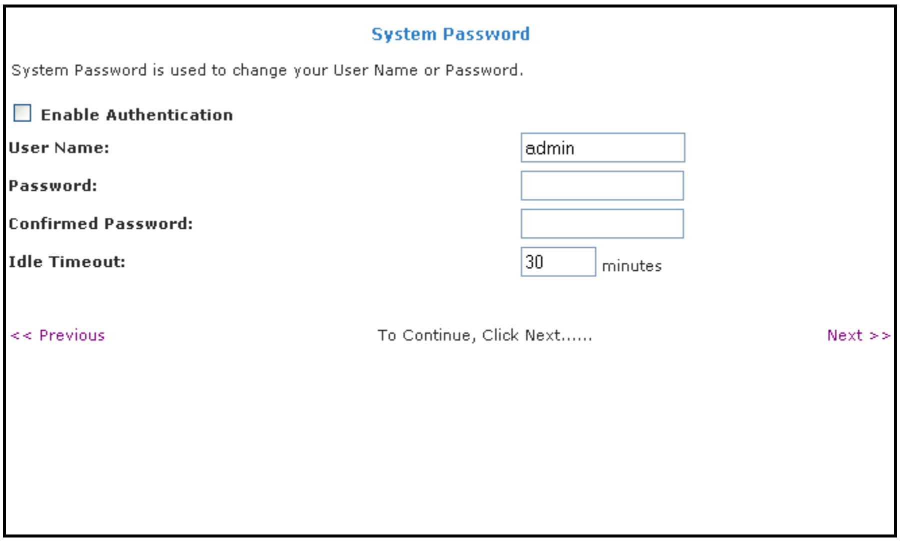
<< Previous To Continue, Click Next...... Next >>

Wireless LAN Security

9. Select **Enable Wireless Security**.

10. Enter an **Encryption Key** or click **Generate** to allow the router to create an alphanumeric encryption key for you. The Encryption key will be used to establish the wireless network connection of wireless devices.

11. Click **Next**. This opens the **System Password** page.



System Password

System Password is used to change your User Name or Password.

□ Enable Authentication

User Name:	admin
Password:	
Confirmed Password:	
Idle Timeout:	30 minutes

System Password page

12. Select **Enable Authentication**.

13. Enter **User Name, Password,** and **Confirm Password**.

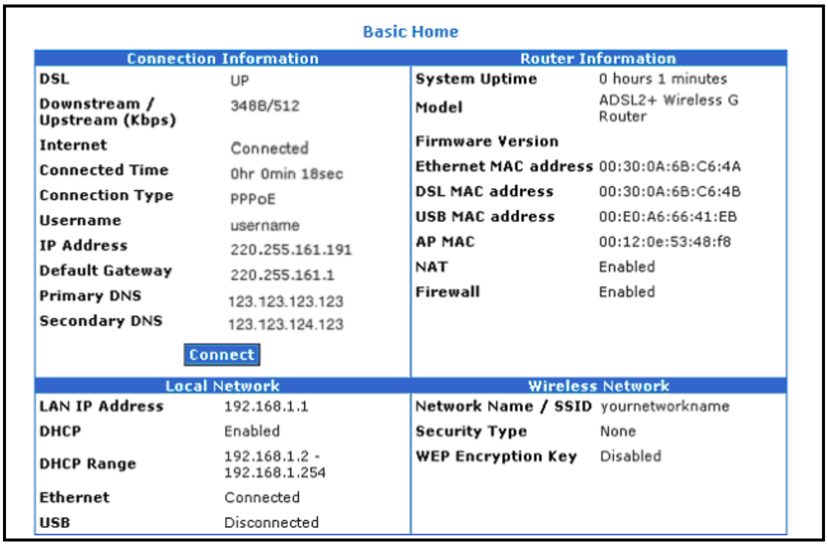
14. Enter the number of minutes for **Idle Timeout**.

15. Click **Next**. This opens the **Summary** page.

16. Click **Finish**.

17. This opens a dialog box asking if you want to save and restart the router. Click **OK**.

    The router will take about two minutes to save the settings and establish a connection with your Internet service provider. Afterwards, the Basic Home page opens to give you a summary of the account settings.



Basic Home

Connection Information	
DSL	UP
Downstream / Upstream (Kbps)	3488/512
Internet	Connected
Connected Time	0hr 0min 18sec
Connection Type	PPPoE
Username	username
IP Address	220.255.161.191
Default Gateway	220.255.161.1
Primary DNS	123.123.123.123
Secondary DNS	123.123.124.123

Router Information	
System Uptime	0 hours 1 minutes
Model	ADSL2+ Wireless G Router
Firmware Version	
Ethernet MAC address	00:30:0A:6B:C6:4A
DSL MAC address	00:30:0A:6B:C6:4B
USB MAC address	00:E0:A6:66:41:EB
AP MAC	00:12:0e:53:48:f8
NAT	Enabled
Firewall	Enabled

Local Network	
LAN IP Address	192.168.1.1
DHCP	Enabled
DHCP Range	192.168.1.2 - 192.168.1.254
Ethernet	Connected
USB	Disconnected

Wireless Network	
Network Name / SSID	yournetworkname
Security Type	None
WEP Encryption Key	Disabled

Basic Home page

Setting Up Via the Utility Wizard

The Setup Wizard can also be used to configure your router. However, this only runs on Windows operating systems.

Notes:

- Microsoft Windows 2000 users may be asked to confirm the installation. To confirm, click **Yes**.
- Microsoft Windows XP users may be asked to confirm the installation. To confirm, click **Continue Anyway**.

To use the Setup Wizard:

1. Insert the **Utility CD** into your CD-ROM.
2. If the utility does not launch automatically, select **Start** > **Run**, enter **D:\Setup.exe** (where **D:** is your CD-ROM drive), and then click **OK**. This opens the **Setup Utility**.
3. Select your router model and then follow the installation procedure.
4. After a successful connection, on the router's front panel, **INTERNET** lights up.

Setting the Administrator Account

Anyone who can access the web interface can be considered an Administrator. To restrict access to the web interface, you need to set the System Password.

Changing the System Password

To change the System Password:

1. Select **Advanced Menu**
2. Click **System Password**. This opens the **System Password** page.
3. Select **Enable Authentication**.
4. Enter your password.
5. Reenter your password in the **Confirm Password** text box.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

Note: Remember your account information. If you forget the User Name and System Password, you will need to reset the router to its default settings. To reset, press **RESET** at the router's back panel for 10 seconds.

Changing the Timeout Settings

To change the timeout settings:

1. Select **Advanced Menu**
2. Click **System Password**.
3. Select **Enable Authentication**.
4. Enter the number of minutes in the **Idle Timeout** text field.
5. To temporarily implement the settings, click **Apply**.

6. To make changes permanent, click **Save Settings**.

Network Setup

There are two types of network configuration for your router: WAN setup and LAN setup.

WAN Setup

Wide Area Network (WAN) is also referred to as the broadband connection. Connection settings differ for every service provider. Most of the configuration you perform is for the WAN connection.

LAN Setup

The router is preconfigured to automatically provide an IP address to all the computers in the Local Area Network (LAN). However, if you are familiar with your network setup, you can manually configure the LAN settings.

WAN Setup

Wide Area Network refers to the configurations you perform to establish an Internet connection. There are several types of WAN connections that require different settings.

New Connection

Your router supports the creation of new connections. If you have multiple virtual connections, you may need to utilize the static routing capabilities of the modem to pass data correctly.

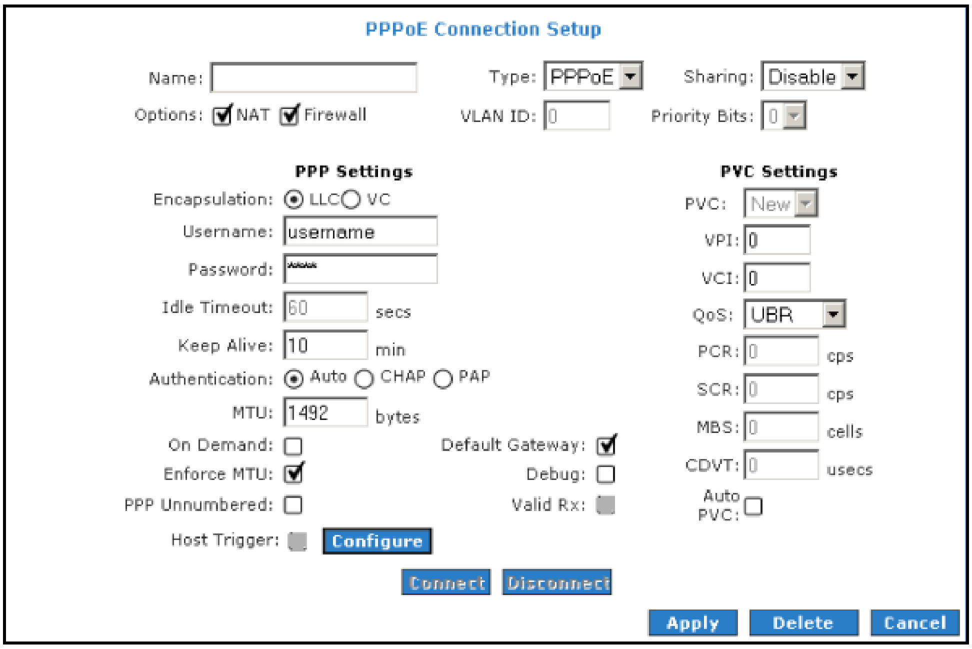
WAN connections types include:

- PPPoE Connection
- PPPoA Connection
- Static Connection
- DHCP Connection

- Bridge Connection
- CLIP Connection

PPPoE Connection

PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. PPPoE is a protocol for encapsulating PPP frames in Ethernet frames and is described in RFC 2516. PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each router uses its own PPP stack. Access control, billing, and type of service control can all be done on a per-user rather than per-site basis.



PPPoE Connection Setup

Name: | Type: PPPoE | Sharing: Disable
Options: ☑ NAT ☑ Firewall | VLAN ID: 0 | Priority Bits: 0

PPP Settings

Encapsulation: ● LLC ○ VC
Username: username
Password: *****
Idle Timeout: 60 secs
Keep Alive: 10 min
Authentication: ● Auto ○ CHAP ○ PAP
MTU: 1492 bytes
On Demand: □ | Default Gateway: ☑
Enforce MTU: ☑ | Debug: □
PPP Unnumbered: □ | Valid Rx: □
Host Trigger: □ Configure

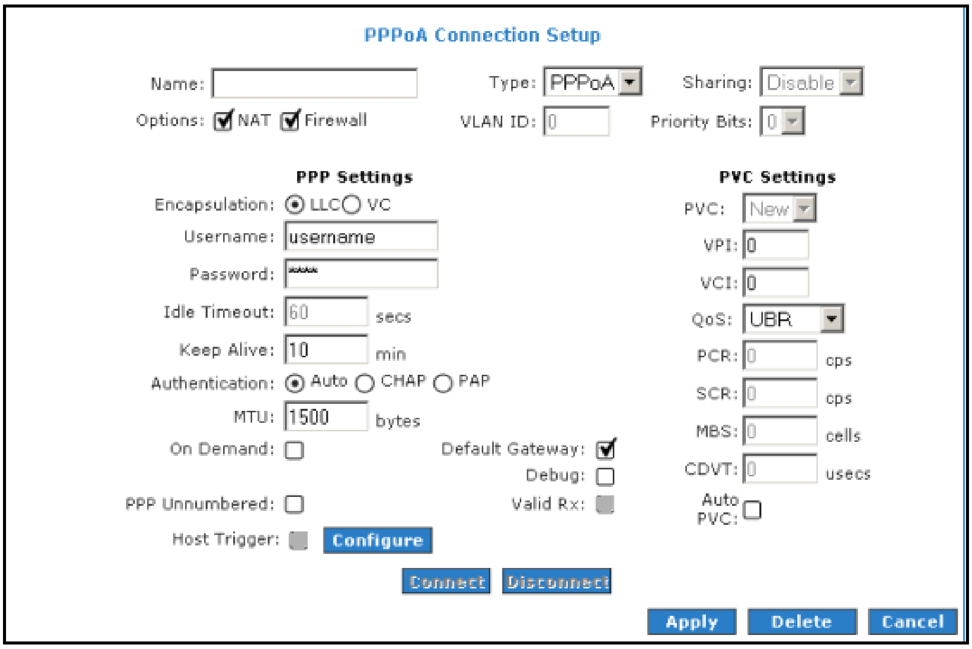
PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

New PPPoE Connection Setup

PPPoA Connection

PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets in ATM cells that are carried over the DSL line. PPP, or point-to-point protocol, is a method of establishing a network connection/session between network hosts. It usually provides a mechanism of authenticating users. Logical link control (LLC) and virtual circuit (VC) are two different methods of encapsulating the PPP packet. Contact your service provider to determine which encapsulation is being used on your Internet connection.



PPPoA Connection Setup

Name: Type: PPPoA Sharing: Disable

Options: ☑ NAT ☑ Firewall VLAN ID: 0 Priority Bits: 0

PPP Settings

Encapsulation: ● LLC ○ VC

Username: username

Password: ****

Idle Timeout: 60 secs

Keep Alive: 10 min

Authentication: ● Auto ○ CHAP ○ PAP

MTU: 1500 bytes

On Demand: □ Default Gateway: ☑

Debug: □

PPP Unnumbered: □ Valid Rx: □

Host Trigger: □

PVC Settings

PVC: New

VPI: 0

VCI: 0

QoS: UBR

PCR: 0 cps

SCR: 0 cps

MBS: 0 cells

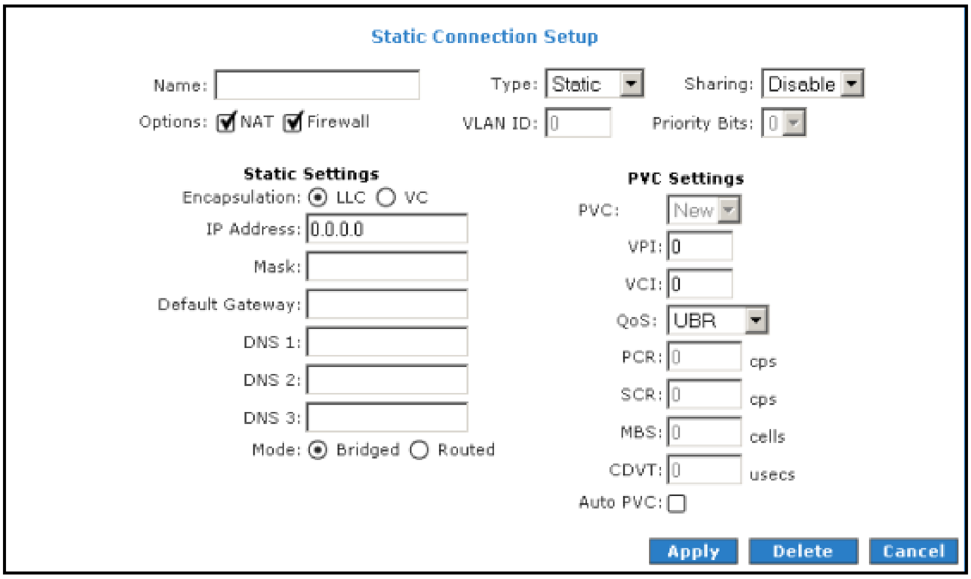
CDVT: 0 usecs

Auto PVC: □

New PPPoA Connection Setup

Static Connection

Static connection type is used whenever a known static IP address is assigned to the router. Additional addressing information such as the subnet mask and the default gateway must also be specified. Up to three domain name server (DNS) addresses can be identified. These servers resolve the name of the computer to the IP address mapped to it and thus enable you to access other web servers by typing the symbolic name (host name).



Static Connection Setup

Name:
Type: Static
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

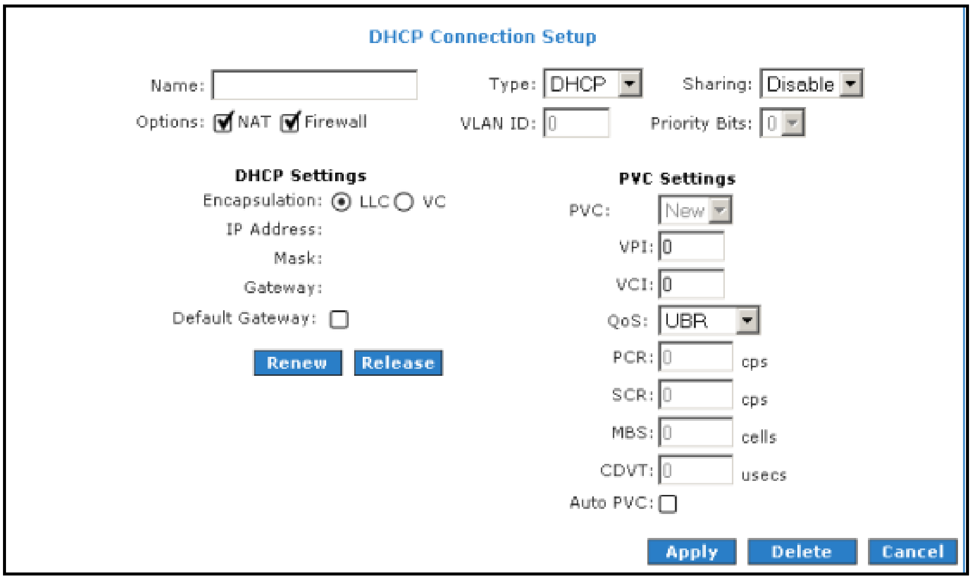
Static Settings
Encapsulation: ● LLC ○ VC
IP Address: 0.0.0.0
Mask:
Default Gateway:
DNS 1:
DNS 2:
DNS 3:
Mode: ● Bridged ○ Routed

PVC Settings
PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

New Static Connection Setup

DHCP Connection

DHCP allows the router to automatically obtain the IP address from the server. This option is commonly used in when the IP is dynamically assigned and is not known prior to assignment.



DHCP Connection Setup

Name:
Type: DHCP
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

DHCP Settings

Encapsulation: ● LLC ○ VC
IP Address:
Mask:
Gateway:
Default Gateway: □

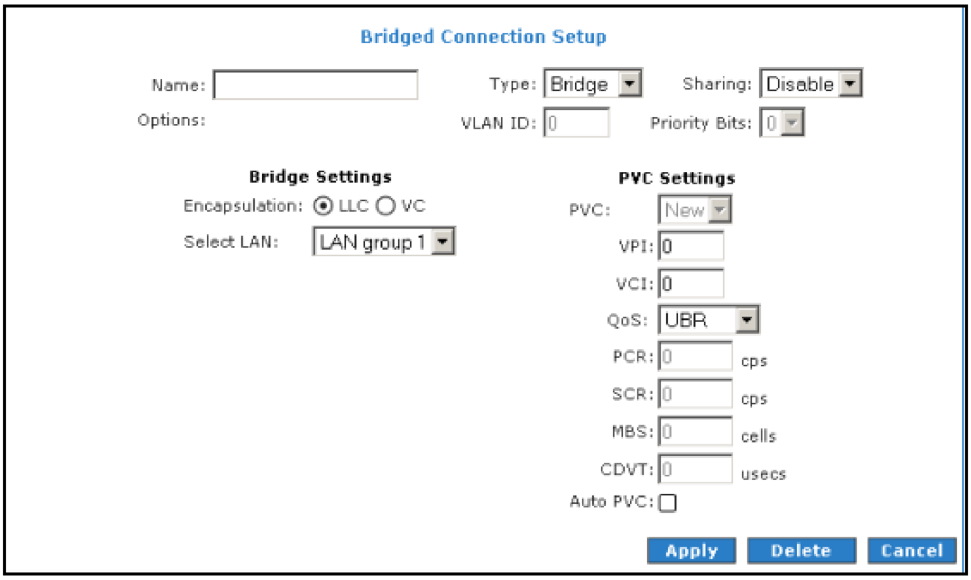
PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

New DHCP Connection Setup

Bridge Connection

A pure bridged connection does not assign any IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the router act as a bridge for passing packets between the WAN interface and the LAN interface.



Bridged Connection Setup

Name:
Type: Bridge
Sharing: Disable
Options:
VLAN ID: 0
Priority Bits: 0

Bridge Settings

Encapsulation: ● LLC ○ VC
Select LAN: LAN group 1

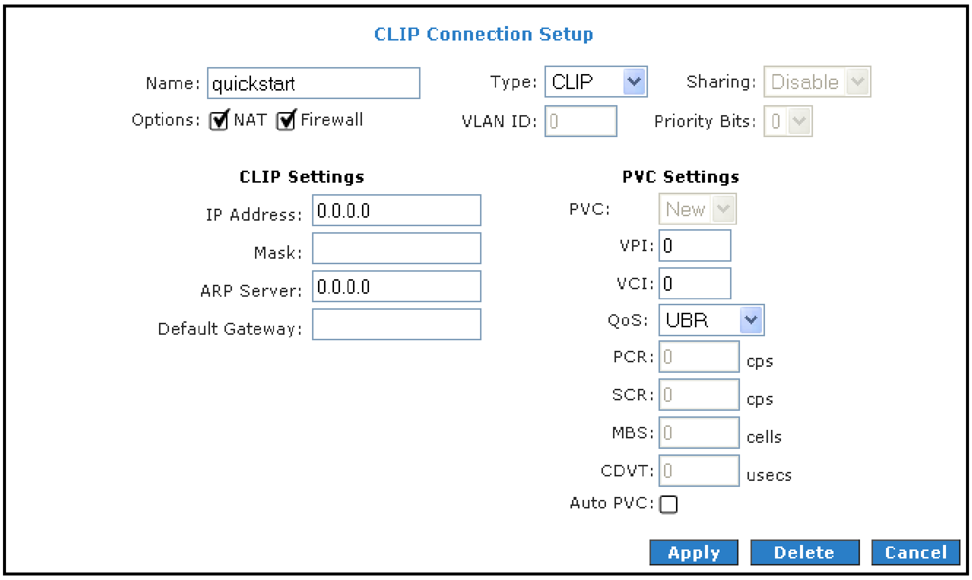
PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

New Bridge Connection Setup

CLIP Connection

Classical IP over ATM (CLIP) Connection Setup page (CLIP) provides the ability to transmit IP packets over an ATM network. CLIP support encapsulates an IP datagram in an AAL5 PDU frame using RFC 2225 and it uses an ATM-aware version of the address resolution protocol (ATMARP).



CLIP Connection Setup

Name: quickstart
Type: CLIP
Sharing: Disable
Options: ☑ NAT ☑ Firewall
VLAN ID: 0
Priority Bits: 0

CLIP Settings

IP Address: 0.0.0.0
Mask:
ARP Server: 0.0.0.0
Default Gateway:

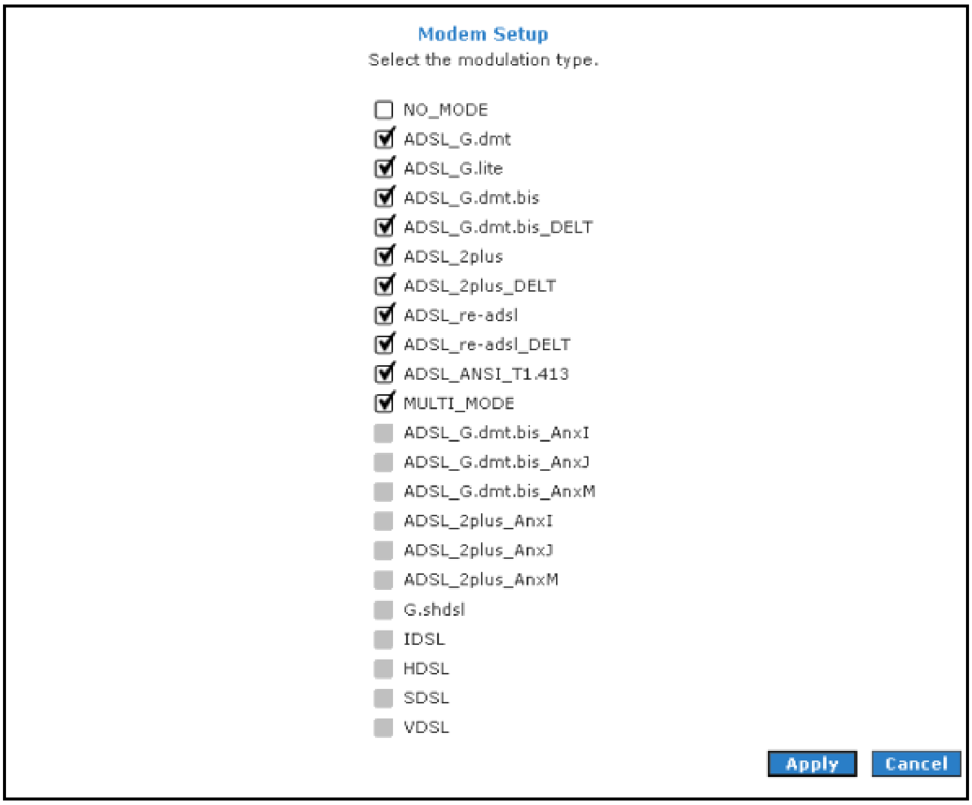
PVC Settings

PVC: New
VPI: 0
VCI: 0
QoS: UBR
PCR: 0 cps
SCR: 0 cps
MBS: 0 cells
CDVT: 0 usecs
Auto PVC: □

CLIP Connection Setup

ADSL Modulation

ADSL Modulation allows you to select any combination of DSL training modes. Leave the default value if you are unsure or the service provider did not provide this information. In most cases, this screen should not be modified.



Modem Setup

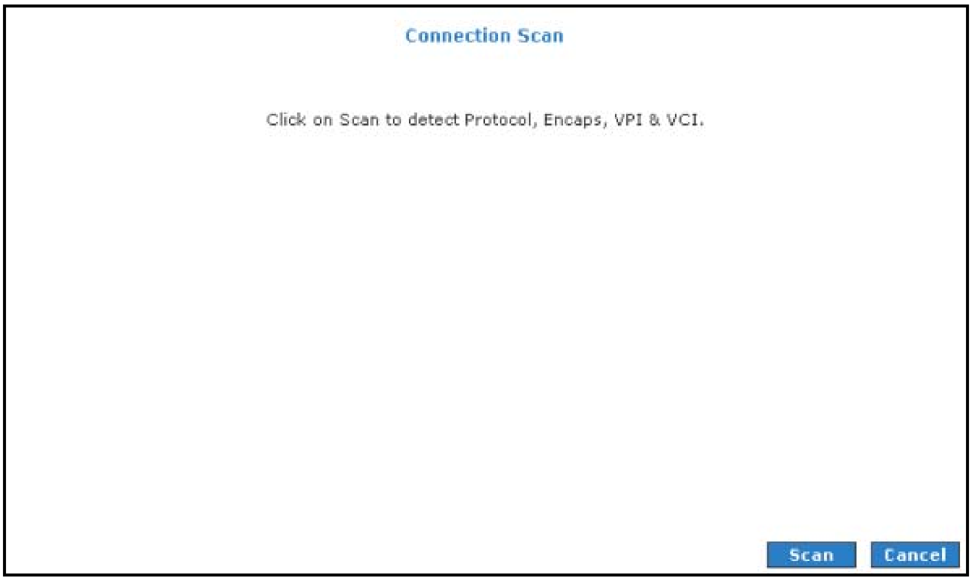
Select the modulation type.

- □ NO_MODE
- ☑ ADSL_G.dmt
- ☑ ADSL_G.lite
- ☑ ADSL_G.dmt.bis
- ☑ ADSL_G.dmt.bis_DELT
- ☑ ADSL_2plus
- ☑ ADSL_2plus_DELT
- ☑ ADSL_re-adsl
- ☑ ADSL_re-adsl_DELT
- ☑ ADSL_ANSI_T1.413
- ☑ MULTI_MODE
- □ ADSL_G.dmt.bis_AnxI
- □ ADSL_G.dmt.bis_AnxJ
- □ ADSL_G.dmt.bis_AnxM
- □ ADSL_2plus_AnxI
- □ ADSL_2plus_AnxJ
- □ ADSL_2plus_AnxM
- □ G.shdsl
- □ IDSL
- □ HDSL
- □ SDSL
- □ VDSL

ADSL Modulation

Connection Scan

This feature helps users to detect the PVC settings provided by the service provider. Before the router can begin scanning the connection, the telephone line has to be plugged into the router.



Click on Scan to detect Protocol, Encaps, VPI & VCI.

Connection Scan

To perform connections scan:

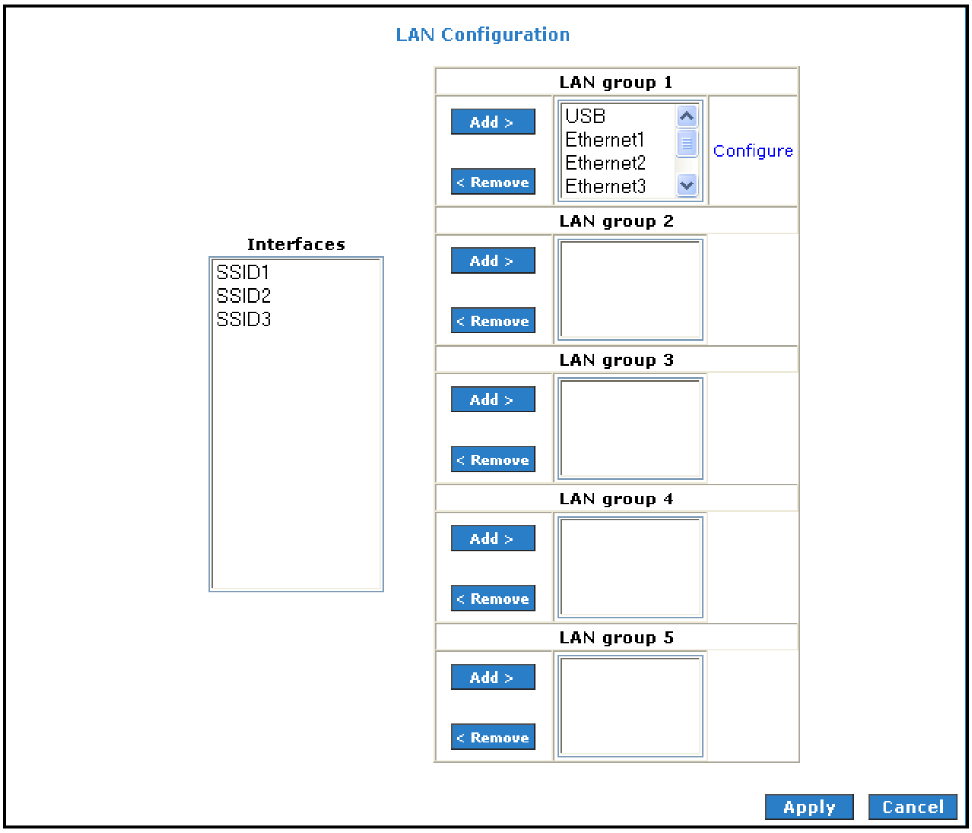
1. Select the Advanced Menu.
2. Select WAN > Connection Scan.
3. Click Scan.

LAN Setup

The router is preconfigured to automatically provide IP addresses to all the computers in the Local Area Network (LAN). Your router allows you to create and configure LAN groups.

LAN Configuration

Your router's default IP address and subnet mask are 192.168.1.1 and 255.255.255.0, respectively. This subnet mask allows the router to support 254 users. If you want to support more users, you need to edit the subnet mask but remember that the DHCP server is defaulted to only give out 255 IP addresses. If you change your gateways' IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet. The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway Address.



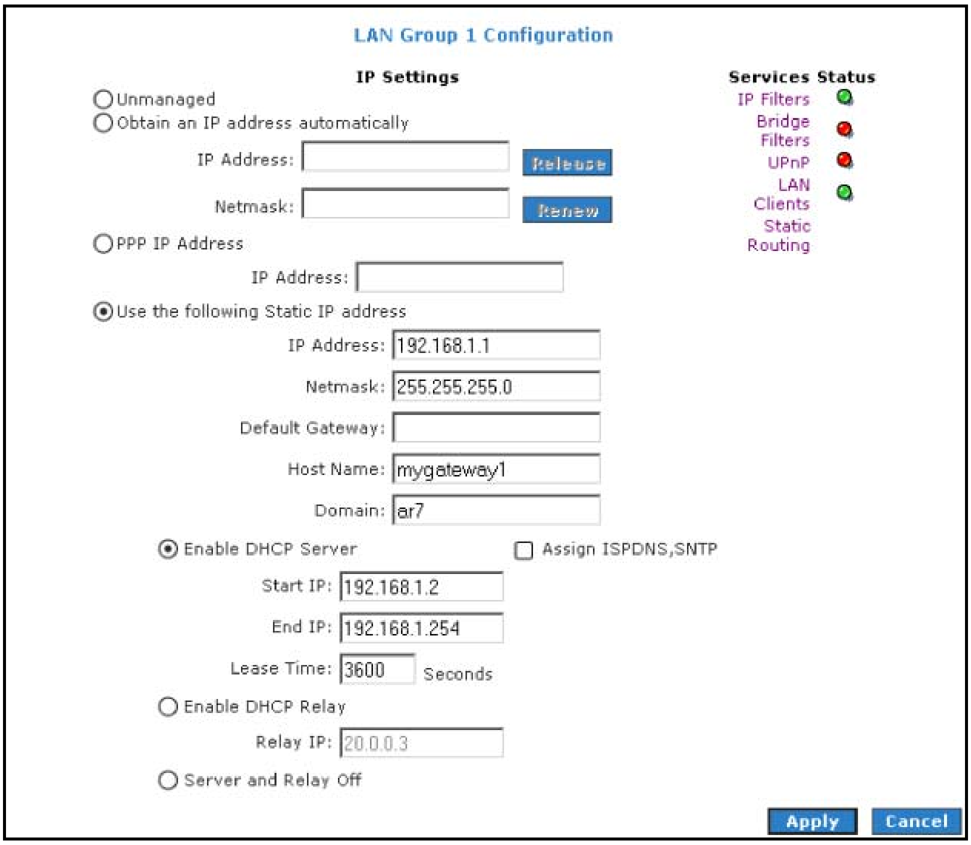
LAN Configuration

To configure the LAN groupings:

1. Select the Advanced Menu.
2. Select LAN > LAN Configuration.
3. Select ETHERNET in LAN group 1 and then click < Remove. No packets will be sent to the ETHERNET interface because it does not belong to any LAN group.
4. Select ETHERNET from Interfaces and then click Add > under LAN group 2. Just like in LAN group 1, Configure will appear in LAN group 2 to allow the definition of additional configurations.
5. To temporarily activate the settings, click Apply.
6. To make changes permanent, click Save Settings.

LAN Group Configuration

LAN Group Configuration allows you to configure settings for each LAN group. Notice that you can also view the status of advanced services that can be applied to a LAN group. Green indicates that the service is enabled, while red indicates that the service is disabled.



LAN Group 1 Configuration

IP Settings

○ Unmanaged

○ Obtain an IP address automatically

IP Address:

Netmask:

○ PPP IP Address

IP Address:

● Use the following Static IP address

IP Address: 192.168.1.1

Netmask: 255.255.255.0

Default Gateway:

Host Name: mygateway1

Domain: ar7

● Enable DHCP Server □ Assign ISPDNS,SNTP

Start IP: 192.168.1.2

End IP: 192.168.1.254

Lease Time: 3600 Seconds

○ Enable DHCP Relay

Relay IP: 20.0.0.3

○ Server and Relay Off

Services Status

IP Filters	🟩
Bridge Filters	🟥
UPnP	🟥
LAN Clients	🟩
Static Routing	

LAN Group Configuration

Category	Field	Description
Unmanaged		Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
Obtain an IP address automatically		When this function is enabled, your router acts like a client and requests an IP address from the DHCP server on the LAN side.
	IP Address	You can retrieve/renew an IP address from the DHCP server using the Release and Renew buttons.
	Netmask	The subnet mask of your router.

PPP IP Address		Enables/disables PPP unnumbered feature.
	IP Address	The IP address should be different but within the same subnet as the WAN-side IP address.
Use the following Static IP address		This field enables you to change the IP address of the router.
	IP Address	The default IP address of the router (as shown) is 192.168.1.1.
	Netmask	The default subnet mask of your router is 255.255.255.0. This subnet allows the router to support 254 users. If you want to support a larger number of users you can change the subnet mask.
	Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
	Host Name	The host name is used in conjunction with the domain name to uniquely identify the router. It can be any alphanumeric word that does not contain spaces.
	Domain	The domain name is used in conjunction with the host name to uniquely identify the router. To access the web pages of the router you can type 192.168.1.1 (the IP address) or mygateway1.ar7 (Host Name.Domain).
Enable DHCP Server		Enables/disables DHCP. By default, your router has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers.
	Assign ISP DNS, SNTP	Enable/disables the Assign ISP DNS, SNTP feature when the DHCP server of your router has been enabled. To learn more, please refer to Assign ISP DNS, SNTP.
	Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the router. For example, if the IP address of the router is 192.168.1.1 (default), then the starting IP address must be 192.168.1.2 (or higher). Note: If you change the start or end values, make sure the values are still within the same subnet as the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate

		with the router if your host has DHCP enabled.
	End IP	The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254; hence the max value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time. Note: If you change the start or end values, make sure the values are still within the same subnet as the IP address of the router. In other words, if the IP address of the router is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate with the router if your host has DHCP enabled.
	Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the router using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or the DHCP server issues a new IP. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (About 278 hours).
Enable DHCP Relay		In addition to the DHCP server feature, the router supports the DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server.
	Relay IP	The IP address of the DHCP relay server.
Server and Relay Off		When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your router must reside on the same subnet as all the other hosts.

Assign ISP DNS, SNTP

When you enable the DHCP server, the router dynamically assigns IP addresses to computers in the local network. The router provides its own LAN IP address (192.168.1.1) as both the gateway and the DNS server.

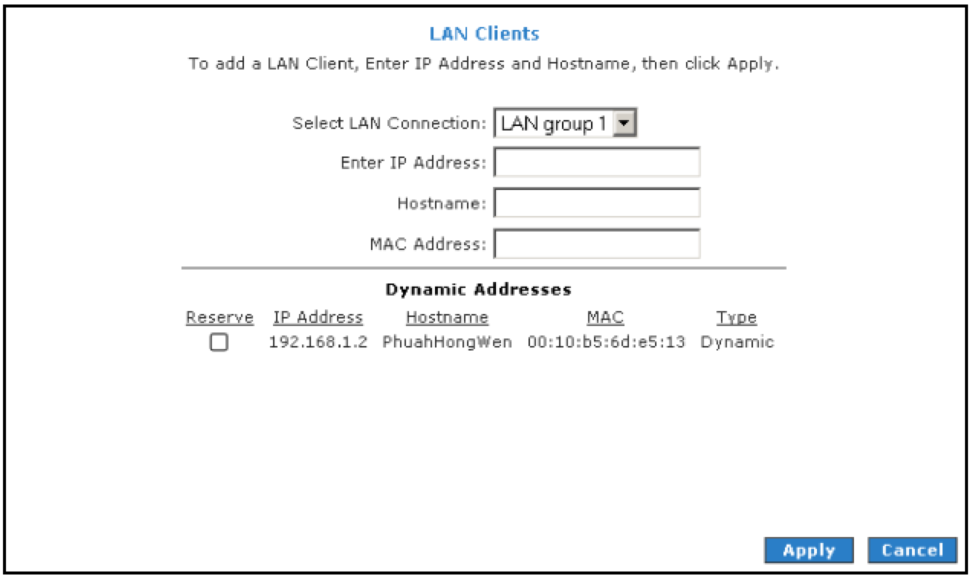
The router has a choice of advertising its own IP address (192.168.1.1) as the DNS server or providing the DNS that was received from the WAN. This can be configured by enabling/disabling **Assign ISP DNS SNTP** on the **LAN Group Configuration** page.

Note: ISP DNS, SNTP only applies when the DHCP server is enabled on the LAN Group Configuration page.

LAN Clients

LAN Clients allows you to view and add computers in a LAN group. Each computer either has a dynamic or static (manually-configured) IP address.

You can add a static IP address (belonging to the router's LAN subnet) using the LAN Clients page. Any existing static entry falling within the DHCP server's range can be deleted.



LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
□	192.168.1.2	PhuahHongWen	00:10:b5:6d:e5:13	Dynamic

LAN Clients

To add LAN Clients:

1. Select Advanced Menu.

2. Select LAN > LAN Clients. This opens the LAN Clients page.

3. Select a LAN Connection, and enter IP Address, Hostname, and MAC Address.

4. Click Apply.

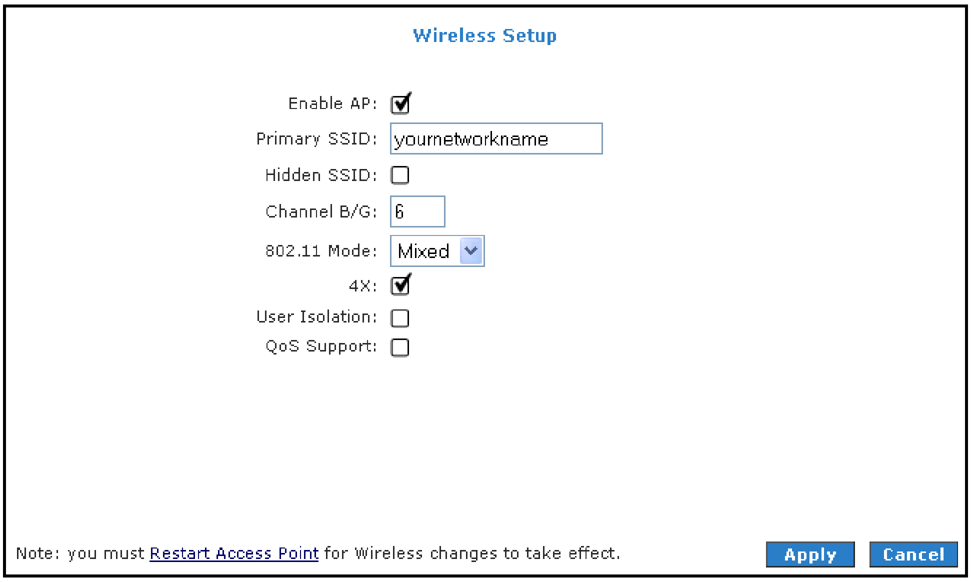
5. You can convert the dynamic into a static entry by clicking Reserve, and then click Apply.

6. To temporarily implement the settings, click Apply.

7. To make changes permanent, click Save Settings.

Wireless Setup

The SSID default is yournetworkname. SSID is wireless network name for the wireless router. Your wireless client needs this name to establish wireless connection. The wireless setup allows the user to enable or disable the Access Point (AP). Disabling Access Point will prevent the wireless router from emitting any wireless signal.



Enable AP: ☑
Primary SSID: yournetworkname
Hidden SSID: □
Channel B/G: 6
802.11 Mode: Mixed
4X: ☑
User Isolation: □
QoS Support: □

Note: you must Restart Access Point for Wireless changes to take effect.

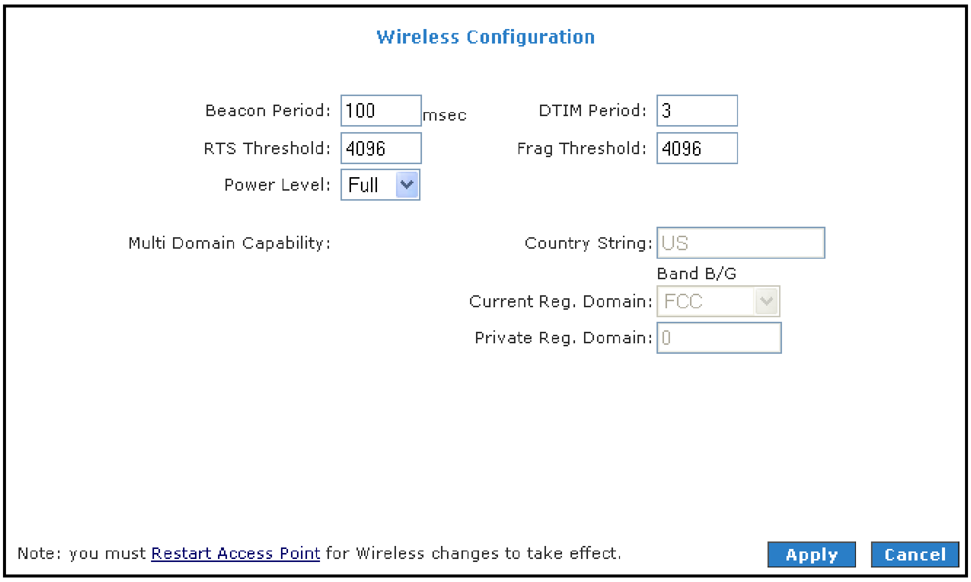
Wireless Setup

To access Wireless Setup:

1. Select the **Wireless Menu.**
2. Select **Setup**.

Wireless Configuration

For users who want to explore the advanced features, you can click on the Advanced button. The options listed can be changed to cater for advance users.



Beacon Period: 100 msec

DTIM Period: 3

RTS Threshold: 4096

Frag Threshold: 4096

Power Level: Full

Multi Domain Capability:

Country String: US

Band B/G

Current Reg. Domain: FCC

Private Reg. Domain: 0

Note: you must Restart Access Point for Wireless changes to take effect.

Wireless Configuration

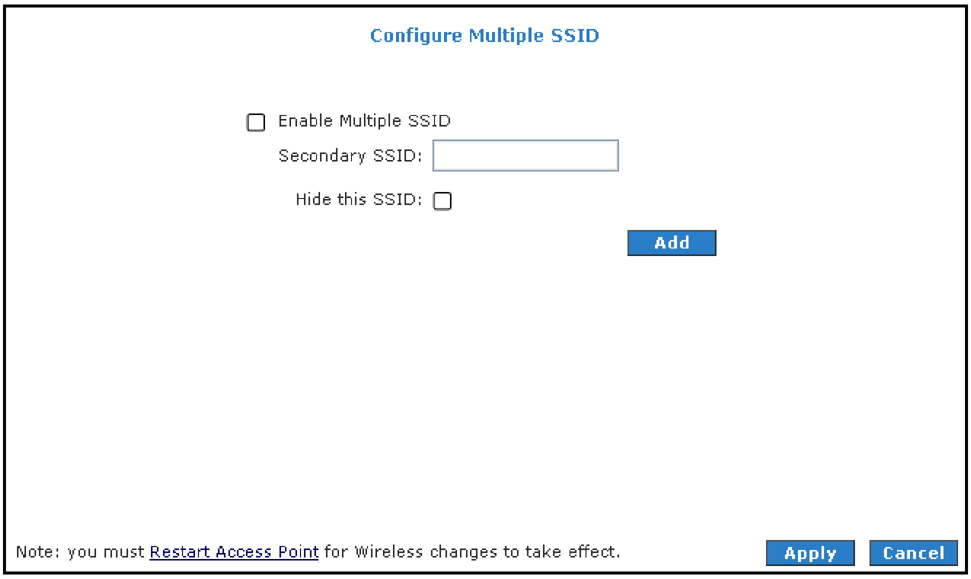
To access Wireless Setup:

1. Select the **Wireless Menu.**

2. Select **Configuration**.

Multiple SSID

Multiple SSID allows you to use a primary and a secondary SSID. The SSID field takes up to 32 alphanumeric characters. Change the VLAN ID to a number different from zero (between 1 to 4095).



Multiple SSID

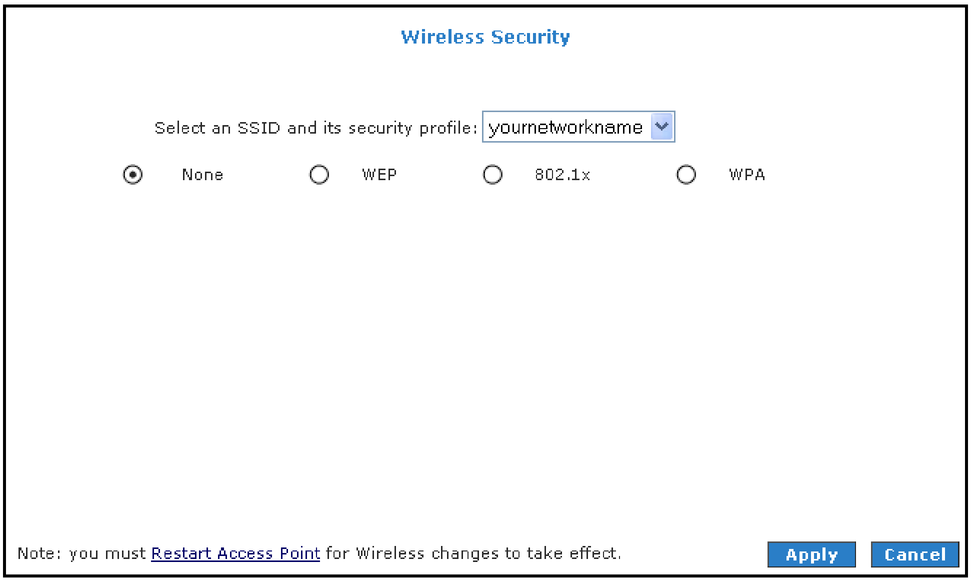
To access Wireless Setup:

1. Select the **Wireless Menu.**

2. Select **Multiple SSID**.

Wireless Security

It is important for user to enforce security in wireless LAN environment. This is to prevent unauthorized wireless users from accessing your router. By default, **None** is selected.



Select an SSID and its security profile: yournetworkname

● None ○ WEP ○ 802.1x ○ WPA

Note: you must Restart Access Point for Wireless changes to take effect.

Wireless Security

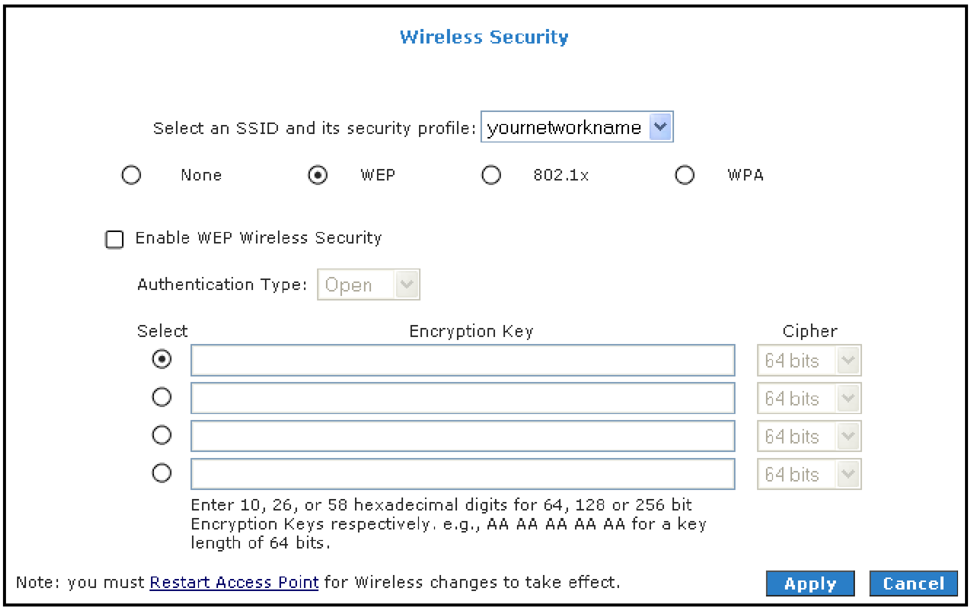
WEP

WEP is a security protocol for WLAN. WEP provides security by encrypting the data that is sent over the WLAN. You can configure up to 4 sets of keys for your wireless client.

The router supports three levels of WEP encryption:

- 64-bit encryption
- 128-bit encryption
- 256-bit encryption

With WEP, the receiving station must use the same key for decryption. Each radio network interface card (NIC) and router must be manually to use the same key.



Wireless Security

Select an SSID and its security profile: yournetworkname

○ None ● WEP ○ 802.1x ○ WPA

□ Enable WEP Wireless Security

Authentication Type: Open

Select	Encryption Key	Cipher
●		64 bits
○		64 bits
○		64 bits
○		64 bits

Enter 10, 26, or 58 hexadecimal digits for 64, 128 or 256 bit Encryption Keys respectively. e.g., AA AA AA AA AA for a key length of 64 bits.

Note: you must Restart Access Point for Wireless changes to take effect.

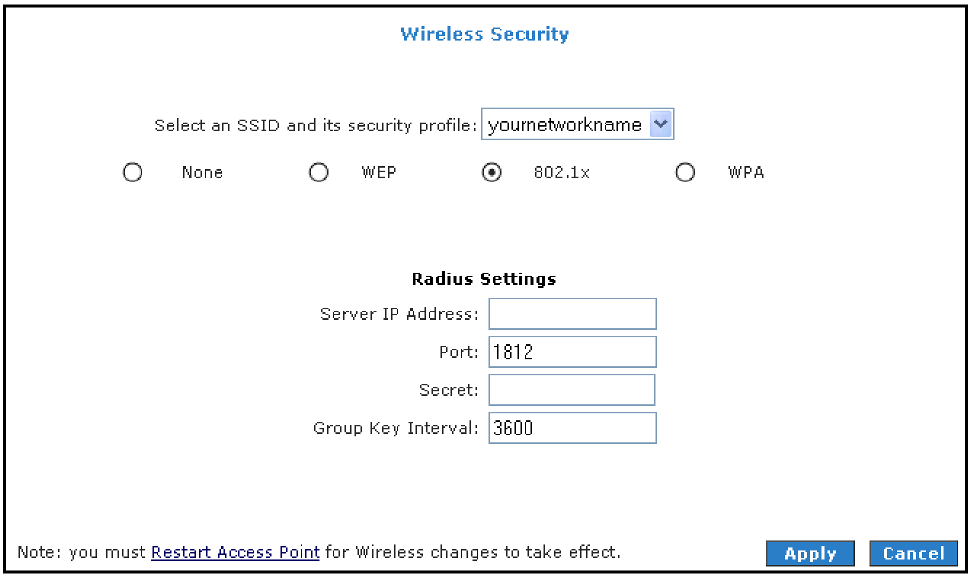
Wireless Security - WEP

To configure WEP:

1. Select the **Wireless Menu.**
2. Select **Security**. This opens the **Wireless Security** page.
3. Select **WEP**.
4. Select **Enable WEP Wireless Security.**
5. Enter an **Encryption Key**.
6. Select a **Cipher** option.
7. To temporarily implement changes, click **Apply**.
8. To make changes permanent, click **Save Settings**.

802.1x

802.1x is a security protocol for WLAN. It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on extensible authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the remote authentication dial-in user service (RADIUS) protocol.



Wireless Security

Select an SSID and its security profile: yournetworkname

○ None ○ WEP ● 802.1x ○ WPA

Radius Settings

Server IP Address:

Port: 1812

Secret:

Group Key Interval: 3600

Note: you must Restart Access Point for Wireless changes to take effect.

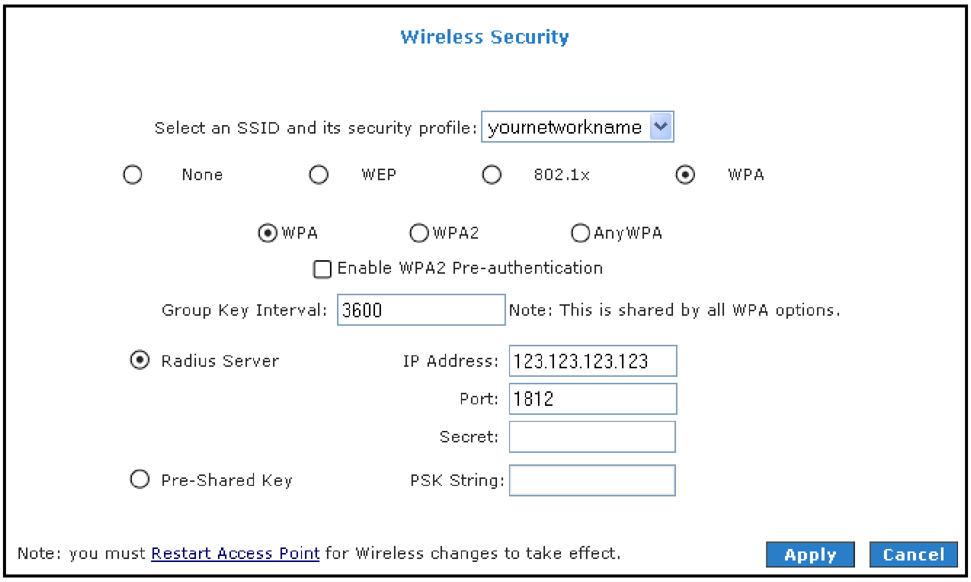
Wireless Security – 802.1x

To configure 802.1z:

1. Select the **Wireless Menu**.
2. Select **Security**. This opens the **Wireless Security** page.
3. Select **802.1x**.
4. Enter the IP address of your RADIUS server.
5. To temporarily implement changes, click **Apply**.
6. To make changes permanent, click **Save Settings**.

WPA

WPA is the short term for WiFi Protected Access. WPA is an industry-supported, pre-standard version of 802.11i that utilizes the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, which includes using dynamic keys. WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an Access Point. Protocols including 802.1X, EAP, and RADIUS are used for strong authentication. Like WEP, keys can still be entered manually (pre-shared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. WPA uses temporal key integrity protocol (TKIP) for data encryption. WPA2, also known as 802.11i, uses advanced encryption standard counter mode CBC-MAC protocol (AES-CCMP) for data encryption.



Wireless Security

Select an SSID and its security profile: yournetworkname

○ None ○ WEP ○ 802.1x ● WPA

● WPA ○ WPA2 ○ AnyWPA

□ Enable WPA2 Pre-authentication

Group Key Interval: 3600 Note: This is shared by all WPA options.

● Radius Server IP Address: 123.123.123.123

Port: 1812

Secret:

○ Pre-Shared Key PSK String:

Note: you must Restart Access Point for Wireless changes to take effect.

Wireless Security – WPA

To access Wireless Setup:

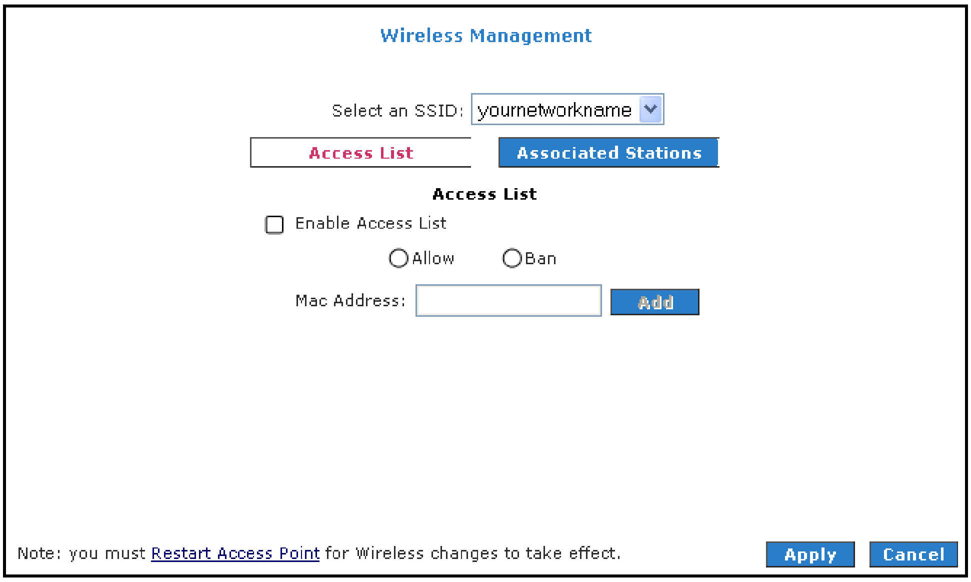
1. Select the **Wireless Menu.**
2. Select **Security**.
3. Select **WPA**.

Wireless Management

The wireless management function gives another level of security to your router. It allows you to permit or ban devices by entering the MAC address or selecting devices that are currently connected.

Access List

This feature permits you to permit or ban wireless clients by using the MAC address.



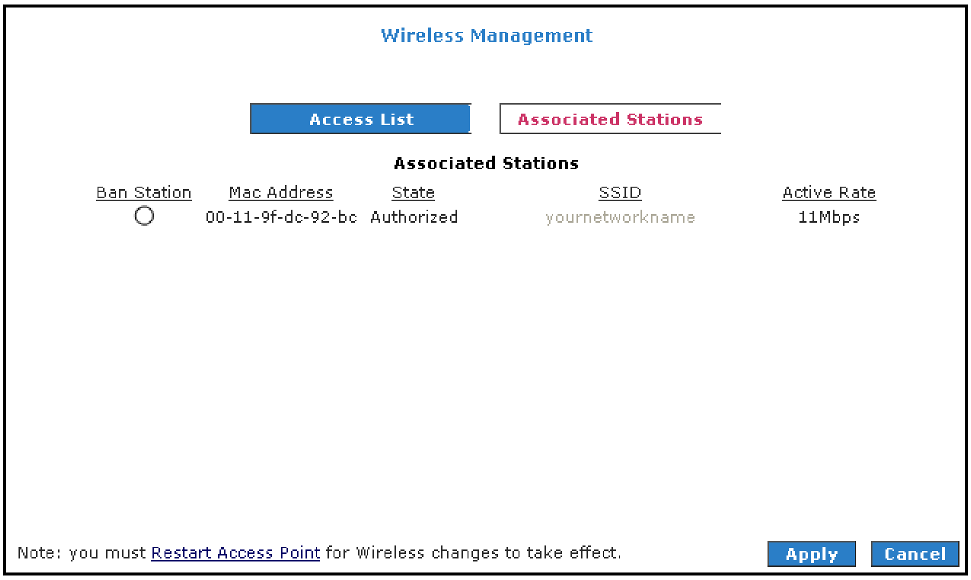
Wireless Management – Access List

To permit or ban a client through the Access List page:

1. Select the **Wireless Menu**.
2. Select **Wireless Management**. This opens the **Wireless Management** page.
3. Select **Enable Access List**.
4. Enter the **MAC address**.
5. Select **Allow** or **Ban**.
6. To temporarily implement the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

Associated Stations

Clients connected to the wireless router are displayed in this page.



Associated Stations

Ban Station	Mac Address	State	SSID	Active Rate
○	00-11-9f-dc-92-bc	Authorized	yournetworkname	11Mbps

Note: you must Restart Access Point for Wireless changes to take effect.

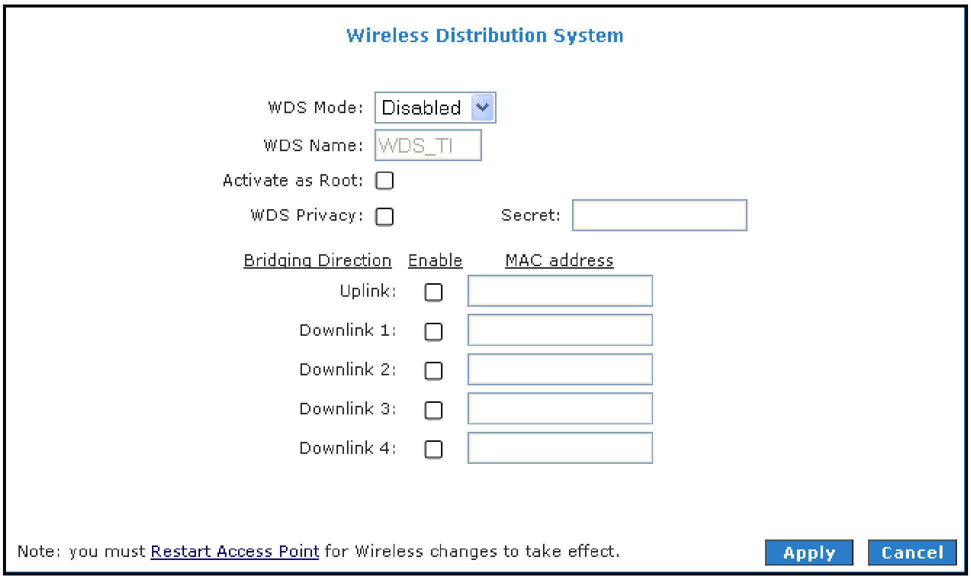
Wireless Management – Associated Stations

To permit or ban a client through the Access List page:

1. Select the **Wireless Menu**.
2. Select **Wireless Management**. This opens the **Wireless Management** page.
3. Select **Associated Stations**.
4. Select **Allow or Ban** beside the wireless client.
5. To temporarily implement the settings, click **Apply**.
6. To make changes permanent, click **Save Settings**.

Wireless Distribution System

Wireless distribution system (WDS) is a system that interconnects BSS to build a premise wide network. WDS network allows users of mobile equipment to roam and stay connected to the available network resources.



Wireless Distribution System

WDS Mode: Disabled

WDS Name: WDS_TI

Activate as Root: □

WDS Privacy: □ Secret:

Bridging Direction	Enable	MAC address
Uplink:	□	
Downlink 1:	□	
Downlink 2:	□	
Downlink 3:	□	
Downlink 4:	□	

Note: you must Restart Access Point for Wireless changes to take effect.

Wireless Distribution System

Field	Description
WDS Mode	The following WDS mode are available: Bridge: In Bridge mode, the Access Point basic service set (BSS) service is enabled. Repeater: In Repeater mode, the Access Point BSS is disabled when connection to the upper layer Access Point is established Crude: In Crude mode, the Access Point BSS is always enabled; however the links between Router are configured statically and are not maintained. Disabled (Default): WDS inactive. In both Bridge and Repeater modes, WDS uses management protocol to establish and maintain links between Router.
WDS Name	The WDS name is used to identify WDS network. The field takes up to eight characters. Two or more WDS networks may exist in the same area.
Activate as Root	This field must be checked for the root device in WDS hierarchy. Only one WDS root device may exist in WDS network. This field is not applicable for Crude mode.
WDS Privacy	Checking this field commands WDS manager to use a secured connection between Router in the WDS network. Security settings must be the same in all Router in the WDS network. Note: WDS privacy is not supported in Crude mode.

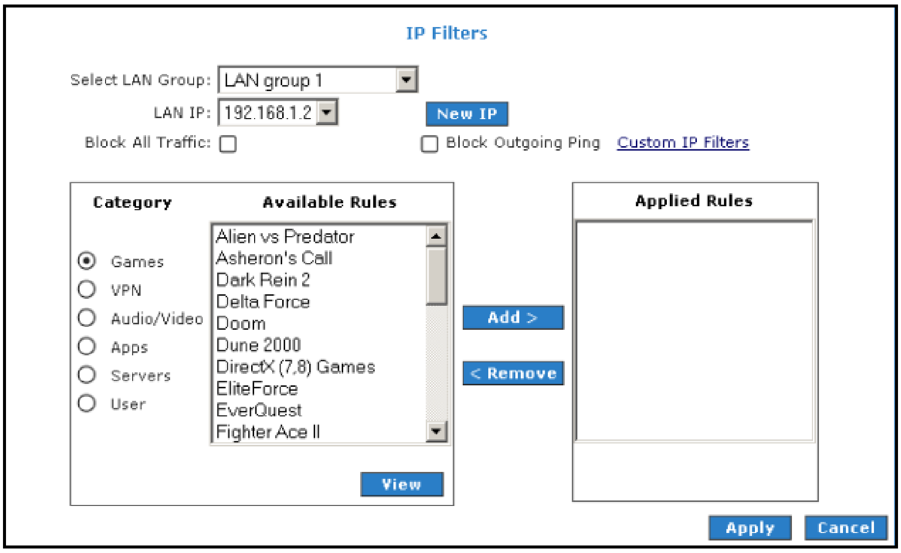
Secret	The 32-character alphanumeric privacy key.
Auto Channel Selection	Auto channel selection is not supported in the current version.
Auto Configuration	Auto configuration is not supported in the current version.
Uplink Connection	The BSS ID of the upper device in the WDS hierarchy. This uplink cannot be configured if root is enabled.
Downlink Connection	The BSS ID of the lower device in the WDS hierarchy connected to this Access Point. Up to four downlinks can be configured.

Security Settings

Configuring IP Filters

IP filtering allows you to block specific applications/services based on the IP address of the LAN device. In this page, you can block specific traffic (for example, block web access) or any traffic from a host on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.



IP Filters

Select LAN Group: LAN group 1

LAN IP: 192.168.1.2

Block All Traffic: □

□ Block Outgoing Ping

Category: ● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User

Available Rules:
Alien vs Predator
Asheron's Call
Dark Rein 2
Delta Force
Doom
Dune 2000
DirectX (7,8) Games
EliteForce
EverQuest
Fighter Ace II

Applied Rules:

IP Filters

To configure IP Filters:

1. Select the **Security Menu** and then click **IP Filters**.

2. On the **IP Filters** page, select **LAN Group** and **LAN IP**. If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the **LAN Client** page, which is accessed by clicking **New IP**.

3. Select the available rules for a given category. Click **View** to view the rule associated with a predefined filter. Click **Add** to apply the rule for this category.

4. If a rule is not in the list, you can create your own rule in the **User category**. Select **User**, and then click **New**.

5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map**, and then click **Apply**.

   The rules you create will appear in the **Available Rules** pane in the User category. You can view or delete the rules you create.

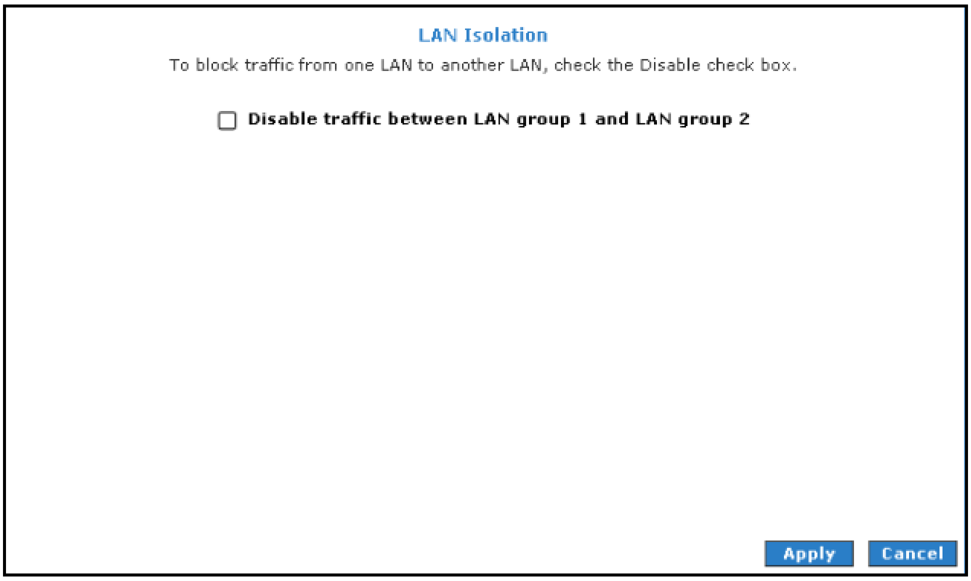
6. Continue to add rules as they apply from each category using the **Add** button.

7. To temporarily implement the changes, click **Apply**.

8. To make the change permanent, click **Save Settings**.

LAN Isolation

LAN isolation allows you to disable the flow of packets between two LAN groups. This allows you to secure information in private portions of the LAN from other publicly accessible LAN segments.



LAN Isolation

To block traffic from one LAN to another LAN, check the Disable check box.

□ Disable traffic between LAN group 1 and LAN group 2

LAN Isolation

To enable LAN Isolation:

1. Select the **Security Menu** and then click **LAN Isolation**.

2. On the **LAN Isolation** page, select the checkbox for **Disable traffic between LAN group 1 and LAN group 2**.

3. To temporarily implement the changes, click **Apply**.

4. To make changes permanent, click **Save Settings**.

URL Filters

URL Filtering allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied.

To apply URL filters:

1. Select the **Security Menu** and then click **URL Filters**.

2. In the **URL Filters** page, select **Enable**.

3. Enter the keyword and then click **Add**.

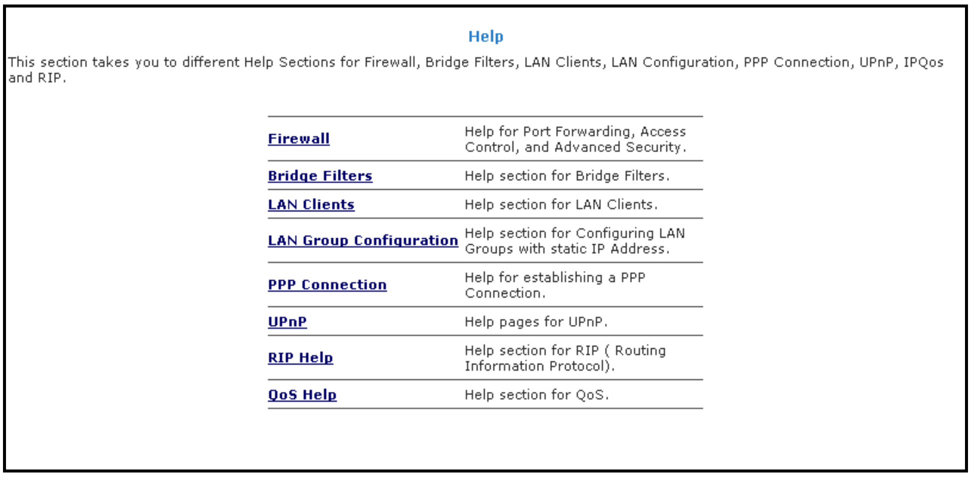
4. To remove keywords, select the keyword and then click **Remove**.

5. To temporarily implement the changes, click **Apply**.

6. To make changes permanent, click **Save Settings**.

Help

The Help page provides documentation for various topics like Firewall, Bridge Filters, LAN Clients, LAN Group Configuration, PPP Configuration, UPnP, IP QoS, and Routing Information Protocol. To access Help, select the **Help Menu**.



Help

This section takes you to different Help Sections for Firewall, Bridge Filters, LAN Clients, LAN Configuration, PPP Connection, UPnP, IPQos and RIP.

Firewall	Help for Port Forwarding, Access Control, and Advanced Security.
Bridge Filters	Help section for Bridge Filters.
LAN Clients	Help section for LAN Clients.
LAN Group Configuration	Help section for Configuring LAN Groups with static IP Address.
PPP Connection	Help for establishing a PPP Connection.
UPnP	Help pages for UPnP.
RIP Help	Help section for RIP (Routing Information Protocol).
QoS Help	Help section for QoS.

Help

Advanced Settings

This chapter provides advanced configuration options for your router.

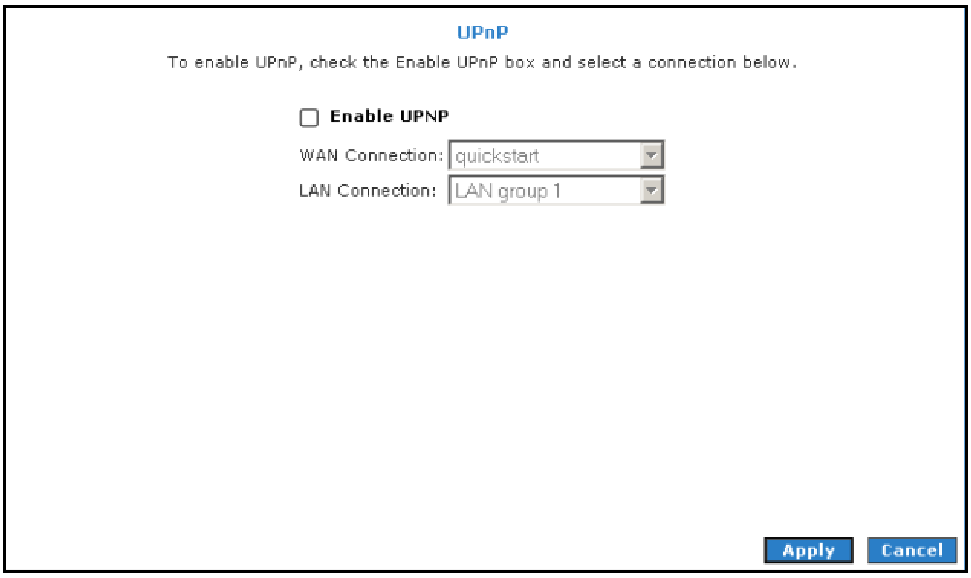
Applications

Applications include:

- Universal Plug and Play (UPnP)
- Simple Network Timing Protocol (SNTP)
- Simple Network Management Protocol
- Internet Group Management Protocol (IGMP) Proxy
- TR-068 WAN Access
- TR-069
- NAT Services
- DNS Proxy
- Dynamic DNS Client
- Easy Connect Configuration
- Prot Triggering
- Port Forwarding
- Bridge Filters
- Web Access Control
- SSH Access Control

Universal Plug and Play

Universal plug and play (UPnP), NAT, and firewall traversal allow traffic to pass through the router for applications using the UPnP protocol. This feature requires one active WAN connection. In addition, the computer should support this feature. In the presence of multiple WAN connections, select a connection on which the incoming traffic is present, for example, the default WAN connection.



UPnP

To enable UPnP, check the Enable UPnP box and select a connection below.

□ Enable UPNP

WAN Connection: quickstart

LAN Connection: LAN group 1

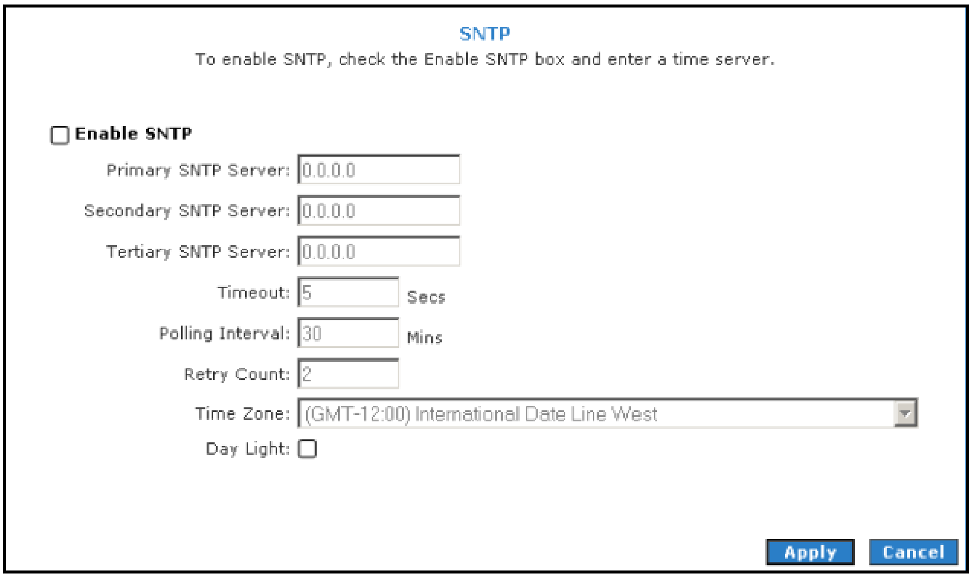
UPnP

To configure UPnP:

1. Select **Advanced**.
2. Select **Application** > **Enable UPnP**.
3. Select the **WAN Connection** and **LAN Connection** that will use UPnP from the drop-down lists.
4. Click **Apply** to temporarily apply the settings.
5. To make changes permanent, click **Save Settings**.

Simple Network Timing Protocol

Simple network timing protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers.



SNTP

To enable SNTP, check the Enable SNTP box and enter a time server.

□ Enable SNTP

Primary SNTP Server:	0.0.0.0
Secondary SNTP Server:	0.0.0.0
Tertiary SNTP Server:	0.0.0.0
Timeout:	5 Secs
Polling Interval:	30 Mins
Retry Count:	2
Time Zone:	(GMT-12:00) International Date Line West
Day Light:	□

SNTP

To enable SNTP:

1. Check **Enable SNTP**.

2. Configure the following fields:

   - **Primary SNTP Server** The IP address or the host name of the primary SNTP server. This can be provided by ISP or defined by user.

   - **Secondary SNTP Server** The IP address or the host name of the secondary SNTP server. This can be provided by ISP or defined by user.

   - **Tertiary SNTP Server** The IP address or the host name of the tertiary SNTP server. This can be provided by ISP or defined by user.

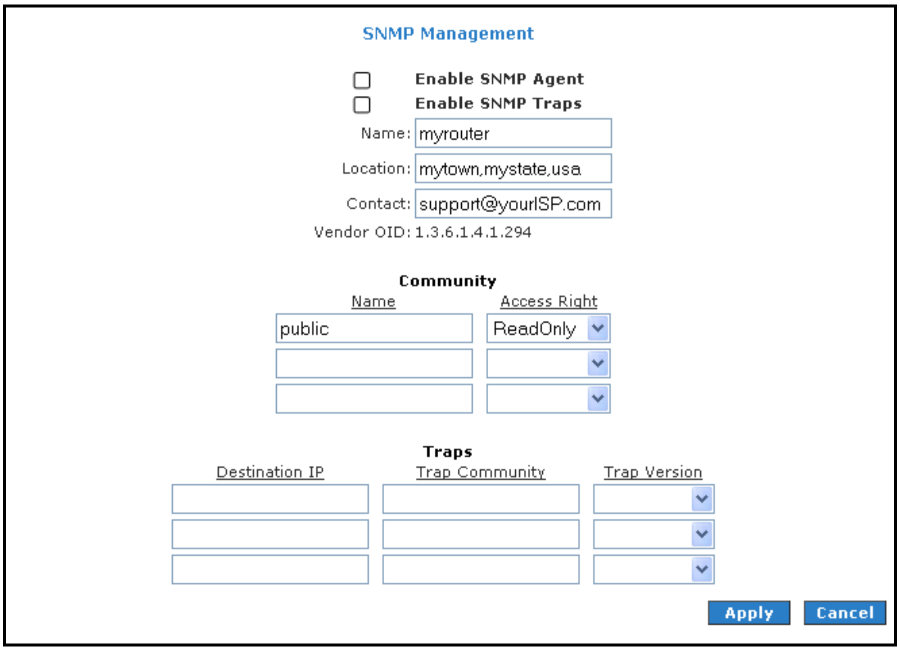
   - **Timeout** If the router failed to connect to an SNTP server within the Timeout period, it retries the connection.

- **Polling Interval** The amount of time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
- **Retry Count** The number of times the router tries to connect to an SNTP server before it tries to connect to the next server in line.
- **Time Zone** The time zone in which the router resides.
- **Day Light** Select this option to enable/disable daylight saving time (DST). DST is not automatically enabled or disabled. You need to manually enable and disable it.

3. Click **Apply** to temporarily apply the settings.
4. To make changes permanent, click **Save Settings**.

Simple Network Management Protocol

SNMP (Simple Network Management Protocol) is a troubleshooting and management protocol, which uses the UDP protocol on port 161 to communicate between clients and servers. SNMP uses a manager MIB (management information base) agent solution to fulfill the network management needs. The agent is a separate station that can request data from an SNMP agent in each of the different system in the network. The agent uses MIBs as dictionaries of manageable objects. Each SNMP-managed device has at least one agent that can respond to the queries from the NMS. The SNMP agent supports GETS, SETS, and TRAPS for 4 groups with MIB-II: System, Interface, IP, and ICMP. The SNMP agent supports three-community names authentication.



SNMP Management

□ Enable SNMP Agent
□ Enable SNMP Traps

Name: myrouter
Location: mytown,mystate,usa
Contact: support@yourISP.com
Vendor OID: 1.3.6.1.4.1.294

Community

Name	Access Right
public	ReadOnly

Traps

Destination IP	Trap Community	Trap Version

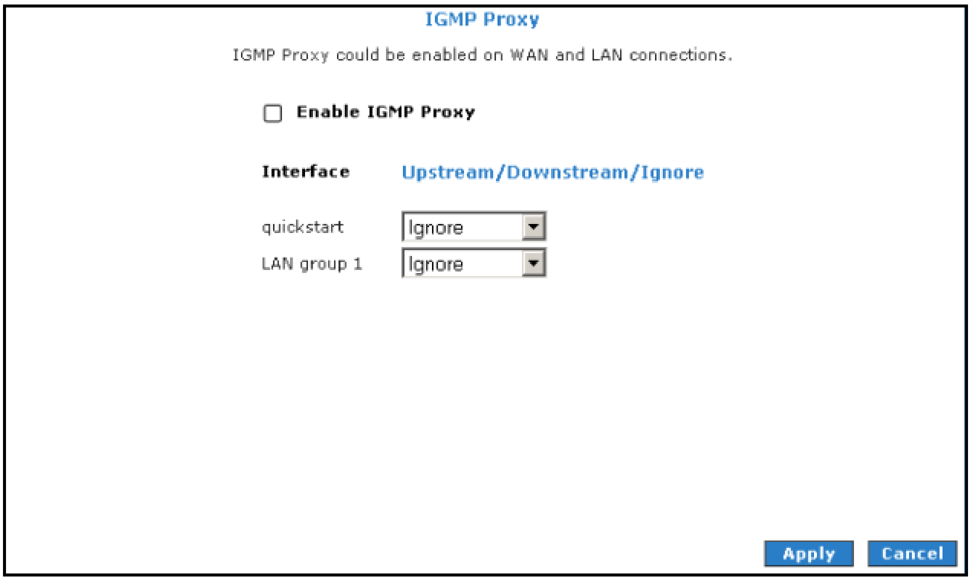
SNMP Management

To access SNMP:

1. Select the Advanced Menu.
2. Select Application > SNMP.

IGMP Proxy

IP hosts use Internet group management protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your router supports IGMP proxy that handles IGMP messages. When enabled, your router acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.



IGMP Proxy

IGMP Proxy could be enabled on WAN and LAN connections.

□ Enable IGMP Proxy

Interface	Upstream/Downstream/Ignore
quickstart	Ignore
LAN group 1	Ignore

IGMP Proxy

Multicasting is a form of limited broadcast. UDP is used to send datagram's to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. The following statements apply to host groups:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.

- Non-group members may send UDP datagram's to the host group.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

The IGMP Proxy page allows you to enable multicast on available WAN and LAN connections. You can configure the WAN or LAN interface as one of the following:

- Upstream The interface that IGMP requests from hosts are sent to the multicast router.
- Downstream The interface data from the multicast router are sent to hosts in the multicast group database.
- Ignore No IGMP request nor data multicast are forwarded.

You can perform one of the two options:

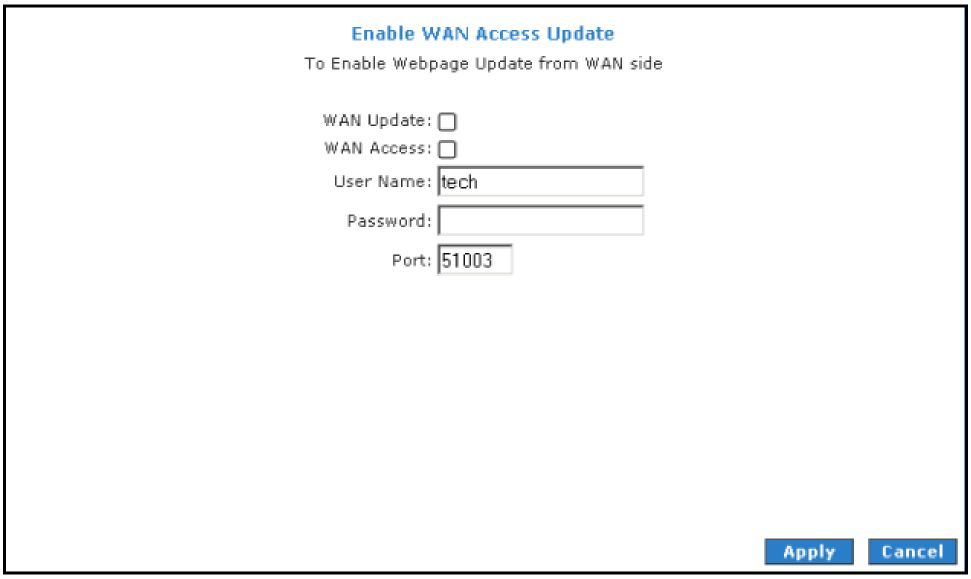
1. Configure one or more WAN interface as the upstream interface.
2. Configure one or more LAN interface as the upstream interface.

To configure the IGMP Proxy:

1. Select Advanced.
2. Select Application > IGMP Proxy.
3. Configure the following interfaces:
    - Quickstart
    - LAN group 1
4. Click Apply to temporarily apply the settings.
5. To make changes permanent, click Save Settings.

TR-068 WAN Access

The TR-068 WAN Access page enables you to give temporary permission to someone (such as technical support staff) to be able to access your router from the WAN side. From the moment the account is enabled the user is expected to log in within 20 minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.



Enable WAN Access Update

To Enable Webpage Update from WAN side

WAN Update: □

WAN Access: □

User Name: tech

Password:

Port: 51003

Enable WAN Access Update

To create a temporary user account for remote access:

1. Select the Advanced Menu.
2. Select Application > TR-068 WAN Access.
3. Select WAN Update.
4. Select WAN Access.
5. Enter a user name and password in the User Name and Password fields.
6. Enter a port number In the Port field (for example, 51003).

   To access your router remotely, enter the following URL:

   - http(s)://10.10.10.5:51003

- **Syntax**: http(s)://WAN IP of router:Port Number

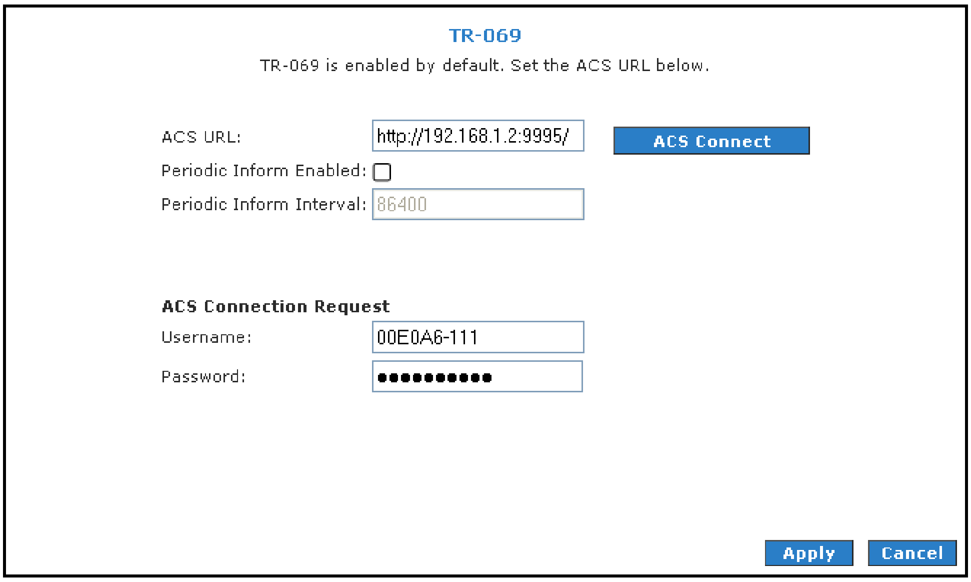
7. Click **Apply** to temporarily apply the settings.
8. To make changes permanent, click **Save Settings**.

TR-069

The TR-069 page allows you to set up connection parameters that cannot be seen by end users. TR-069 is CPE Management Protocol from WAN side, intended for communication between a CPE and Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines a mechanism that encompasses secure auto-configuration of a CPE, and also incorporates other CPE management functions into a common framework.

The CPE WAN Management Protocol is intended to support a variety of functionalities to manage a collection of CPE, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software/firmware image management
- Status and performance monitoring
- Diagnostics



TR-069

TR-069 is enabled by default. Set the ACS URL below.

ACS URL: http://192.168.1.2:9995/

Periodic Inform Enabled: □

Periodic Inform Interval: 86400

ACS Connection Request

Username: 00E0A6-111

Password: ●●●●●●●●●●●

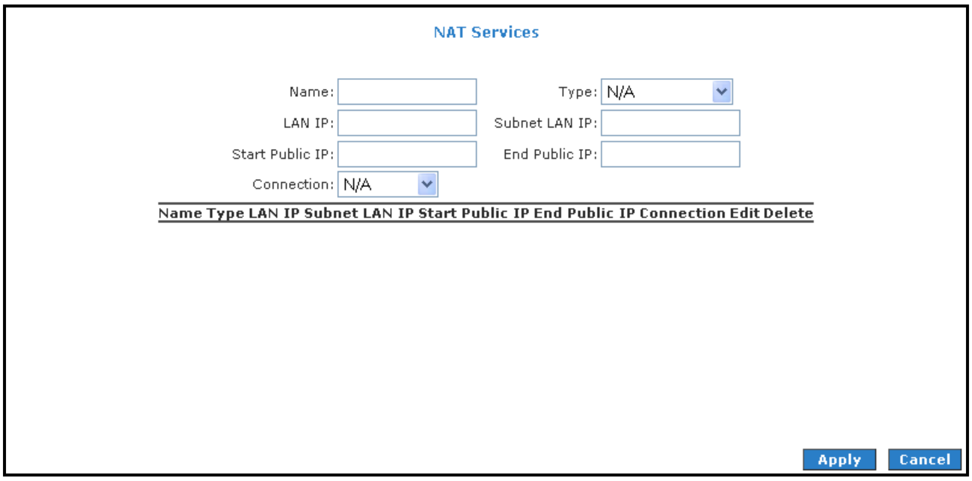
TR0069

To set TR-069:

1. Select the **Advanced Menu**.
2. Select **Application** > **TR-069**.
3. Leave ACS URL.
4. Select **Periodic Inform Enabled** and then enter the **Periodic Inform Interval**.
5. Click ACS Connect to connect to the ACS. When a connection is established, the AVS updates the **ACS URL**, **Periodic Inform Enabled**, and **Periodic Inform Interval**.
6. To temporarily apply the settings, click **Apply**.
7. To make changes permanent, click **Save Settings**.

NAT Services

If the user has more than one public IP address assigned by the ISP, these additional IP addresses can be used to map to servers on the LAN. One public IP address will be used to provide Internet access to the LAN computers via NAT, serving as the primary IP address of the router. The rest will be mapped to servers on the LAN.



NAT Services

Name:
Type: N/A
LAN IP:
Subnet LAN IP:
Start Public IP:
End Public IP:
Connection: N/A

Name	Type	LAN IP	Subnet LAN IP	Start Public IP	End Public IP	Connection	Edit	Delete

NAT Services

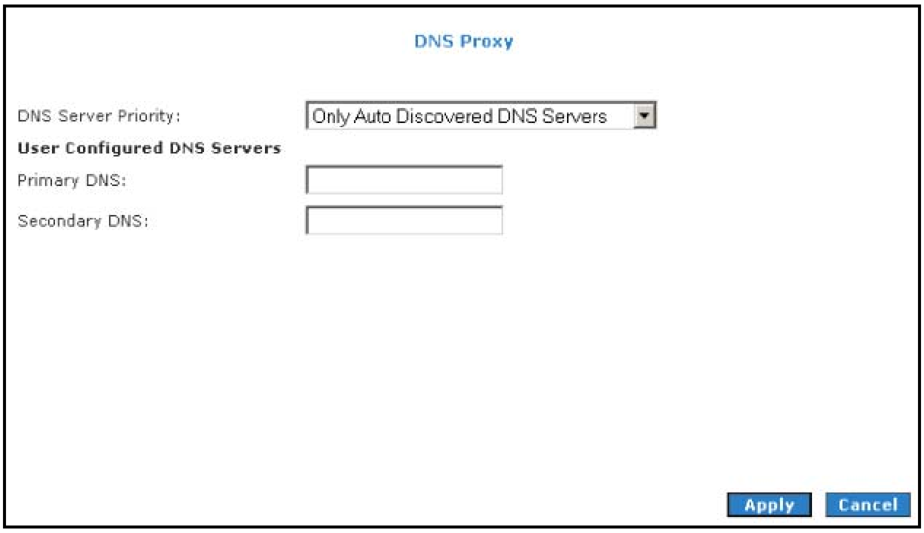
To access NAT:

1. Select the Advanced Menu.

2. Select Application > NAT Services.

DNS Proxy

DNS Proxy determines the primary Domain Name Server and secondary DNS to be used.


DNS Proxy

DNS Server Priority: Only Auto Discovered DNS Servers

User Configured DNS Servers

Primary DNS:

Secondary DNS:

DNS Proxy

To select the DNS Server Priority:

1. Select Advanced.

2. Select Application > DNS Proxy.

3. Select the DNS Server Priority:

    - Only Auto Discovered DNS Servers

    - Only User Configured DNS Servers

    - Auto Discovered then User Configured

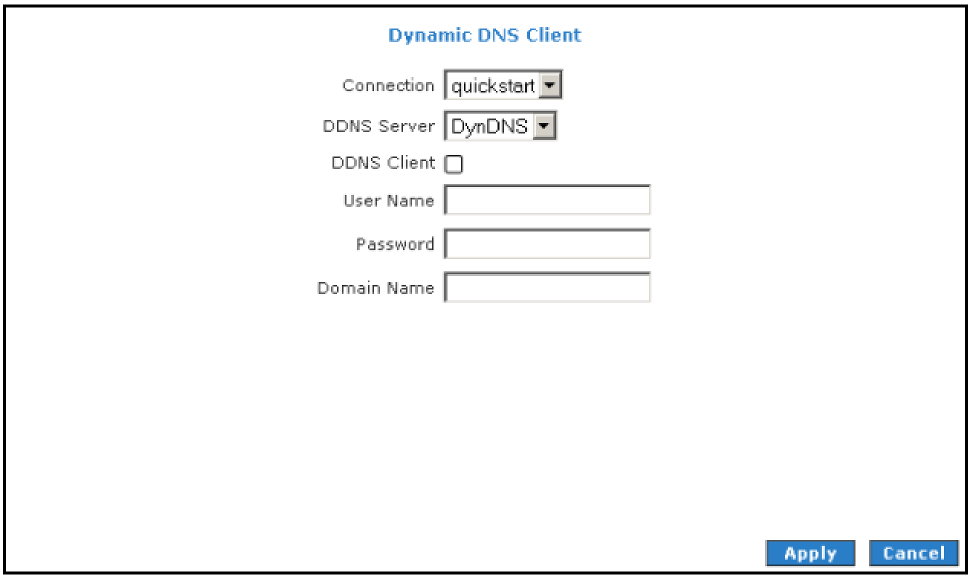
    - User Configured then Auto Discovered

4. Click Apply to temporarily apply settings.

5. To make changes permanent, click Save Settings.

Dynamic DNS Client

Dynamic DNS allows the user to register with a Dynamic DNS Provider. The Dynamic DNS will be linked with the WAN IP of the router even after the ISP update the WAN IP to another IP address. It can be useful in web hosting and FTP services.



Dynamic DNS Client

Connection: quickstart
DDNS Server: DynDNS
DDNS Client: □
User Name:
Password:
Domain Name:

Dynamic DNS Client

Note: The User Name/Password entered should be similar to the User Name/Password you have specified during the registration of the DNS hostname.

To enable Dynamic DNS:

1. Select Advanced.
2. Select Application > Dynamic DNS Client.
3. Configure the following fields:
   - Connection
   - DDNS Server
   - DDNS Client
   - User Name
   - Password

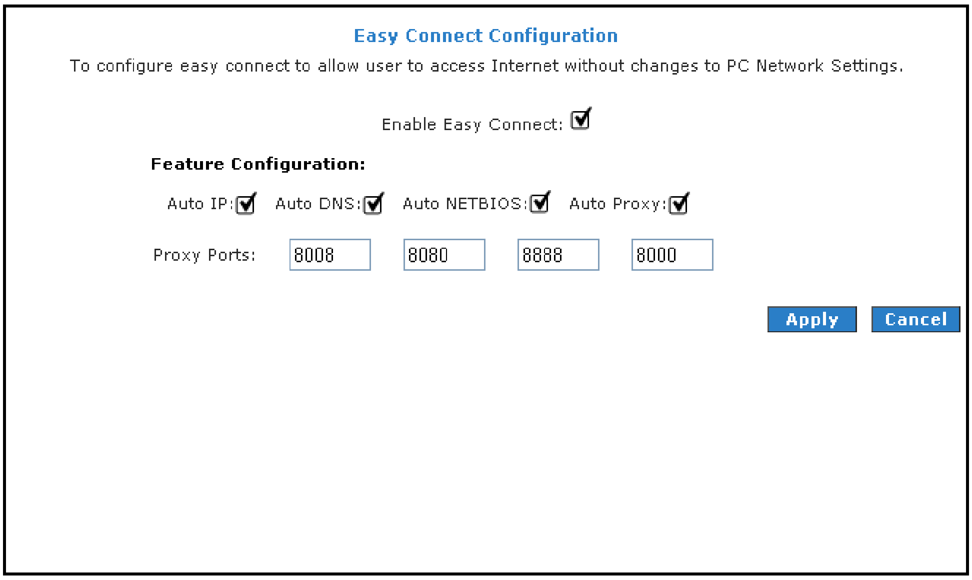
- Domain Name

4. Click **Apply** to temporarily apply the settings.

5. To make changes permanent, click Save **Settings**.

Easy Connect Configuration

Easy Connect feature allow user to surf web with ease without the need to changes default configuration setting, i.e. TCP/IP, Proxy, DNS of user's computer.



Easy Connect Configuration

To configure easy connect to allow user to access Internet without changes to PC Network Settings.

Enable Easy Connect: ☑

Feature Configuration:

Auto IP:☑ Auto DNS:☑ Auto NETBIOS:☑ Auto Proxy:☑

Proxy Ports: 8008 8080 8888 8000

Easy Connect Configuration

Easy Connect features include:

- **Auto IP** All valid TCP/IP setting on user's computer can surf web via the router without the need to change the IP address

- **Auto DNS** Any DNS IP address set at user's computer irregardless whether the address is valid or invalid DNS, Auto DNS still allow user's computer to surf the web.

- **Auto Proxy** Refers to any valid Private IP proxy setting with any port number. For example, when you enter 1234 on the browser, Auto Proxy will still allow the computer to surf the web. Any Public IP proxy setting will assume the proxy is valid and hence Auto Proxy function will not take place.

Note: The port number to be used must be specified in both the browser and the Auto Proxy Ports.

Private IP Ranges

Class A: 10.0.0.0 ~ 10.255.255.255

Class B: 172.16.0.0 ~ 172.31.255.255

Class C: 192.168.0.0 ~ 192.168.255.255

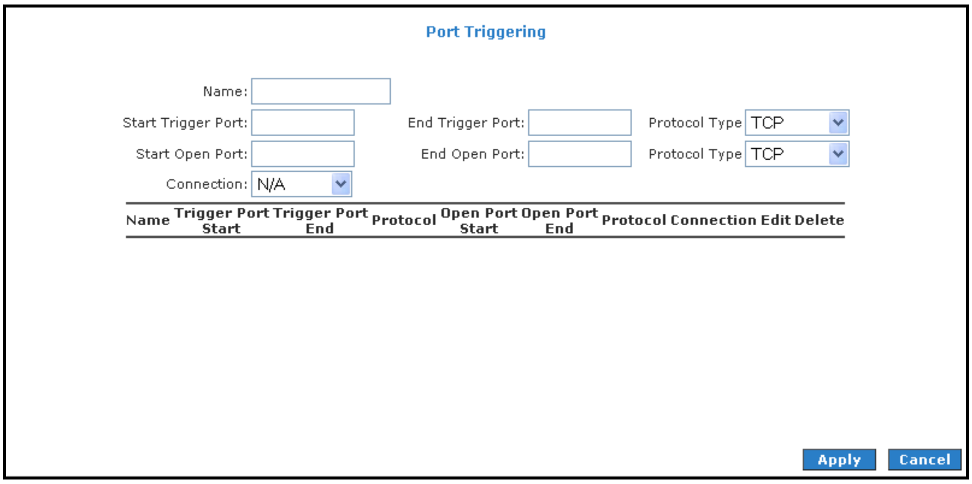
- **Auto NetBIOS** It allows proxy server to use any NetBIOS name which the Auto NetBIOS still allow computer to surf the web with a condition that the router gateway MUST be in Private IP Ranges.

To access Easy Connect:

1. Select **Advanced Menu**.
2. Select **Application** > **Easy Connect Configuration**.

Port Triggering

Port triggering is a specialized form of port forwarding which enables computers behind NAT to be accessed. It triggers open an incoming port when a client on the LAN makes an outgoing connection to a predetermined port on a server.



Port Triggering

Name:

Start Trigger Port: End Trigger Port: Protocol Type TCP

Start Open Port: End Open Port: Protocol Type TCP

Connection: N/A

Name	Trigger Port Start	Trigger Port End	Protocol	Open Port Start	Open Port End	Protocol	Connection	Edit	Delete

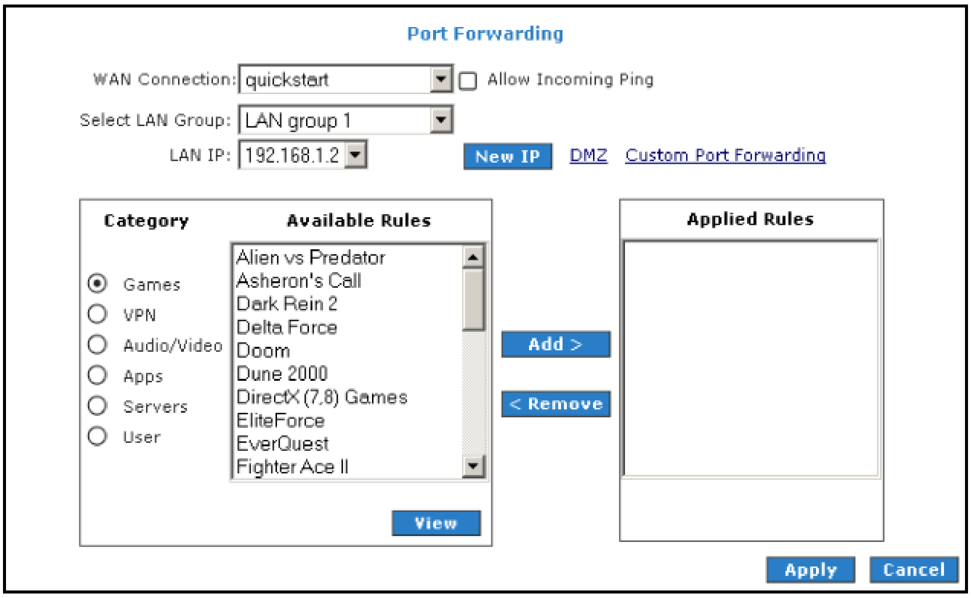
Port Trigegering

To access port triggering:

1. Select **Advanced Menu**.
2. Select **Application** > **Port Triggering**.

Port Forwarding

Port forwarding (or virtual server) allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the Port Forwarding page, you can provide local services (for example, web hosting) for people on the Internet or play Internet games. Port forwarding is configurable per LAN group.



Port Forwarding

WAN Connection: quickstart

□ Allow Incoming Ping

Select LAN Group: LAN group 1

LAN IP: 192.168.1.2

Category: ● Games ○ VPN ○ Audio/Video ○ Apps ○ Servers ○ User

Available Rules: Alien vs Predator, Asheron's Call, Dark Rein 2, Delta Force, Doom, Dune 2000, DirectX (7,8) Games, EliteForce, EverQuest, Fighter Ace II

Applied Rules

Port Forwarding

A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.

To configure port forwarding:

1. Select **Advanced**.
2. Select **Application** > **Port Forwarding**.

3. Select **WAN Connection**, **LAN Group**, and **LAN IP**. If the desired LAN IP is not available in the **LAN IP** drop-down menu, you can add it using the **LAN Client page**, which is accessed by clicking **New IP**.

4. Select the available rules for a given category and click **Add** to apply the rule for this category. If a rule is not in the list, you can create your own rule in the **User** category. Select **User**, and then click **New**.

5. The Rule Management page opens for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map**, and then click **Apply**.

6. Continue to add rules as they apply from each category.

7. Click **Apply** to temporarily activate the settings.

8. To make changes permanent, click **Save Settings**.

DMZ Settings

Setting a host on your local network as demilitarized zone (DMZ) forwards any network traffic that is not redirected to another host via the port forwarding feature to the IP address of the host. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.

To enable DMZ Settings:

1. On the **Port Forwarding** page, select **Enable DMZ**. This opens the DMZ Settings page.

2. Select the **WAN Connection**, **LAN Group**, and **LAN IP Address**.

3. Click **Apply** to temporarily apply the settings.

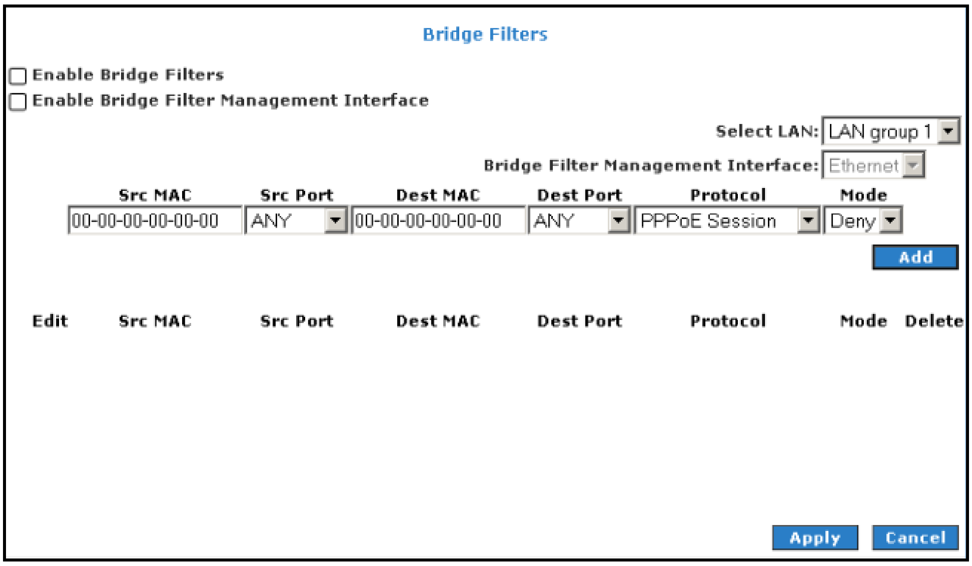
4. To make changes permanent, click **Save Settings**.

Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom port forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operation.

Bridge Filters

The Bridge Filters allows you to enable, add, edit, or delete the filter rules. When bridge filtering is enabled, each frame is examined against every defined filter rule in sequence. When a match is found, the appropriate filtering action (allow or deny) is performed. Up to 20 filter rules are supported with bridge filtering.



Bridge Filters

□ Enable Bridge Filters
□ Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Edit	Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode	Delete

Bridge Filters

To configure Bridge Filters:

1. Select **Advanced**.
2. Select **Application** > **Bridge Filters**. This opens the Bridge Filters page.
3. Select **Enable Bridge Filters**.
4. To add a rule, enter the source **MAC address**, **Destination MAC address**, and **Protocol** with desired filtering type, then click **Add**.

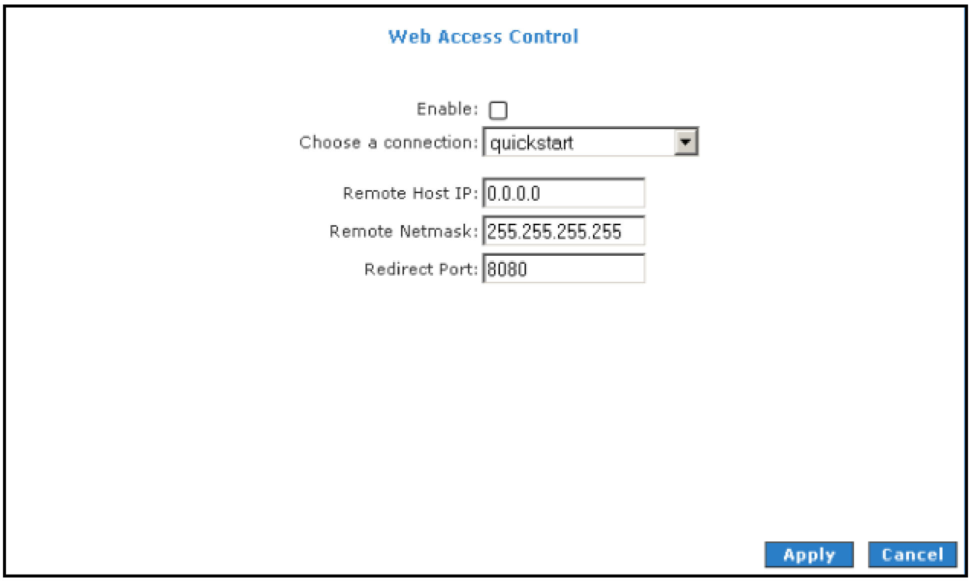
Note: You can also edit a rule that you created using the **Edit** checkbox. You can delete using **Delete**.

5. Click **Apply** to temporarily activate the settings.

6. To make changes permanent, click **Save Settings**.

Web Access Control

The Web Access Control page allows you to access the router via the web from a remote location like your home or office.



Web Access Control

Enable: □

Choose a connection: quickstart

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

Redirect Port: 8080

Web Access Control

To configure Web Access:

1. Select **Advanced Menu**.

2. Select **Application > Web Access Control**.

3. Select **Enable**.

4. Select the connection used in **Choose a connection**.

5. Configure the following fields:

   - Remote Host IP

   - Remote Netmask

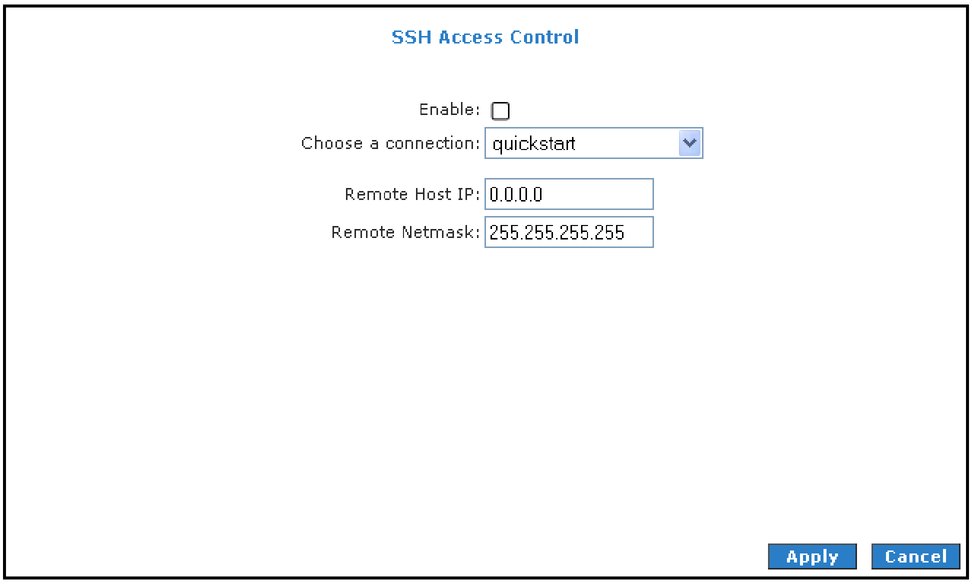
- Redirect Port

6. Click **Apply** to temporarily activate the settings on the page. The WAN address is now added into the IP Access List. This allows you to access you router remotely.

7. To make changes permanent, click **Save Settings**.

SSH Access Control

SSH Access control allows you to access the router remotely via SSH from the WAN side.



SSH Access Control

Enable: □

Choose a connection: quickstart

Remote Host IP: 0.0.0.0

Remote Netmask: 255.255.255.255

SSH Access Control

To configure SSH Access Control:

1. Select **Advanced** Menu.

2. Select **Application > SSH Access Control**. This opens the **SSH Access Control** page.

3. Select **Enable**.

4. Enter the IP address of the remote computer you want to use in **Remote Host IP**.

5. Enter the **Remote Netmask**.

6. To temporarily implement the settings, click **Apply**.

7. To make changes permanent, click **Save Settings**.

Quality of Service

Quality of service allows network administrators to configure the routers to meet the real time requirements for voice and video.

Different networks use different QoS markings like:

- ToS network: ToS bits in the IP header
- VLAN network: priority bits in the VLAN header
- DSCP network: uses only 5 bits of the CoS
- WLAN: WLAN QoS header.

The QoS framework is supported on all the above domains. How do you make them talk to each other? How can you make sure the priority from one network is carried over to another network? Class of service (CoS) is introduced as the common language for the QoS mappings. When QoS is enabled, the router has full control over packets from the time they enter the router till they leave the router. This is how it works: The domain mapping (ToS bits, priority bits, etc.) of a packet needs to be translated to CoS when the packet enter the router, and vice versa, the CoS of a packet needs to be translated back to the domain mapping when the packet leaves the router.

There are 6 types of CoS (in descending priority):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

The rules are:

1. CoS1 has absolute priority and is used for expedited forwarding (EF) traffic. This is always serviced till completion.
2. CoS2-CoS5 are used for assured forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme:

   CoS2 > CoS3 > CoS4 > CoS5
3. CoS6 is for best effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your router, all traffic will be treated as best effort.

There are some additional terms you should get familiarize with:

- Ingress: Packets arriving into the router from a WAN/LAN interface.
- Egress: Packets sent from the router to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.
- Traffic Conditioning Agreement (TCA): The TCA needs to be defined for each interface:
  - Ingress mappings (Domain =>CoS)
  - Egress Mappings (CoS => Domain)
  - Untrusted mode (default)
- Shaper

Egress

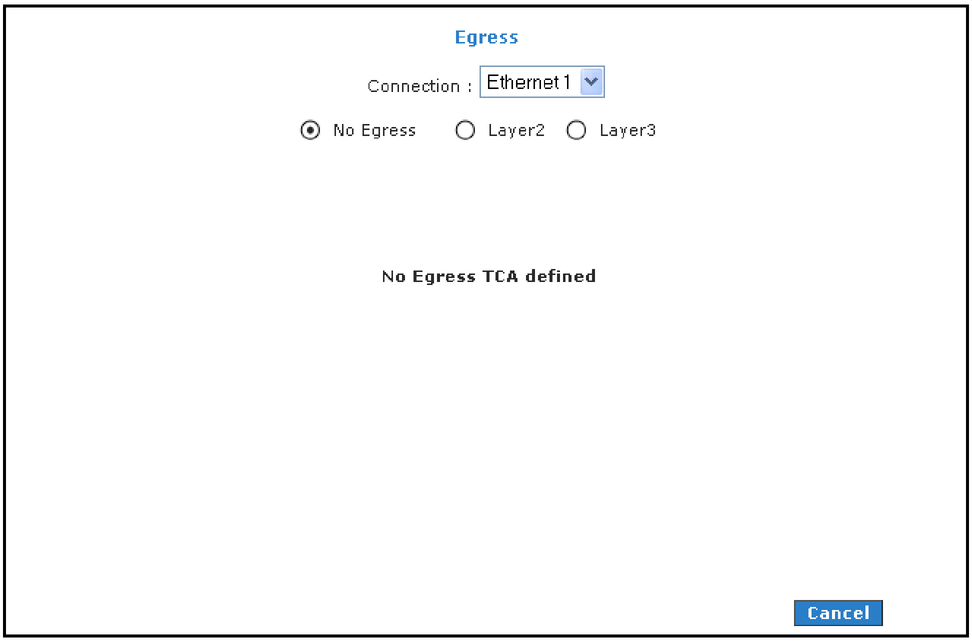
For packets going out of the router, the markings (CoS) need to be translated to the mappings understood by the network domains. The reverse CoS and domain mapping is configured using the Egress. To access **Egress**, select the **Advanced Menu** and then select **QoS > Egress**.

There are three Egress modes:

- No Egress mode
- Layer 2
- Layer 3

No Egress Mode

The default Egress page setting for all interfaces is No Egress. In this mode, the domain mappings of the packets are untouched.



Egress

Connection : Ethernet 1

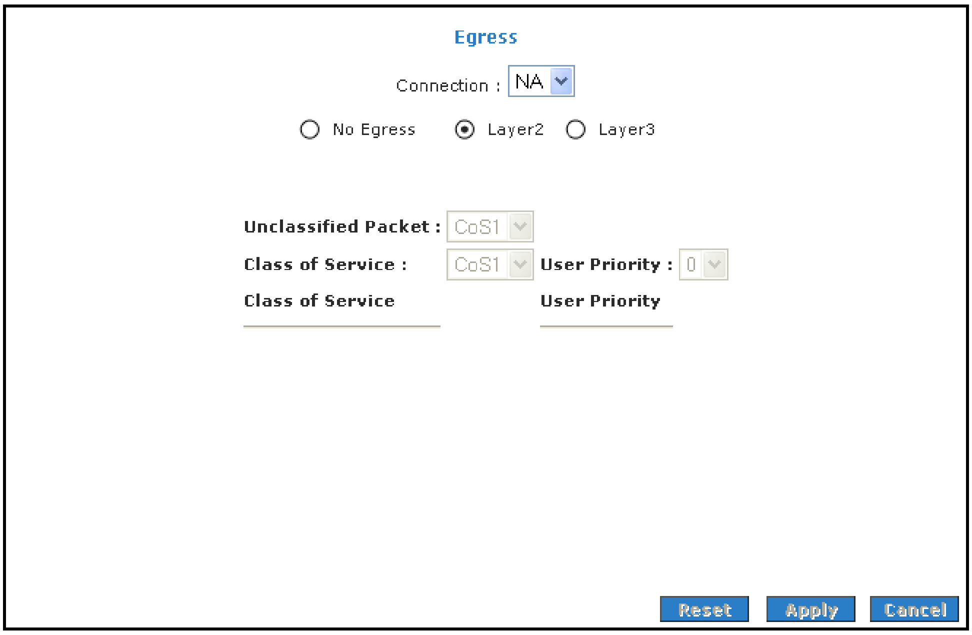
● No Egress ○ Layer2 ○ Layer3

No Egress TCA defined

Egress

Layer 2

The Egress Layer 2 page allows you to map the CoS of an outgoing packet to user priority bits, which is honored by the VLAN network. Again, this feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current release.



Egress

Connection : NA

○ No Egress ● Layer2 ○ Layer3

Unclassified Packet : CoS1

Class of Service : CoS1 User Priority : 0

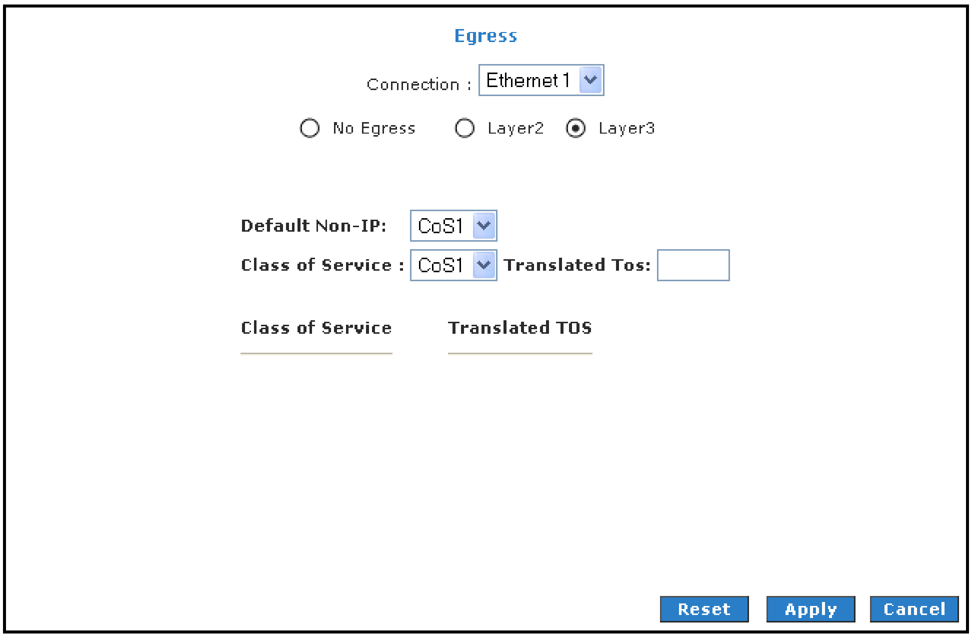
Class of Service	User Priority

Layer 2

Field	Description
Interface	Select the WAN interface to configure the QoS for outgoing packets; LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
Unclassified Packet	Some locally generated packets might not have been classified and thus do not have a CoS value, such as PPP control packet and ARP packet. You can define the CoS for all unclassified outgoing packets on layer 2 using this field, which will then pick up the user priority bits based on the mapping rules you create. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.

Layer 3

Egress Layer 3 enables you to map CoS to ToS so that the priority marking of outgoing packets can be carried over to the IP network.



Egress

Connection : Ethernet 1

○ No Egress ○ Layer2 ● Layer3

Default Non-IP: CoS1

Class of Service : CoS1 Translated Tos:

Class of Service	Translated TOS

Layer 3

Field	Description
Interface	Select the WAN interface to configure the QoS for outgoing packets, LAN interface cannot be selected as VLAN is currently supported on the WAN side only.
Default Non-IP	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
Translated TOS	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6, 7.

Ingress

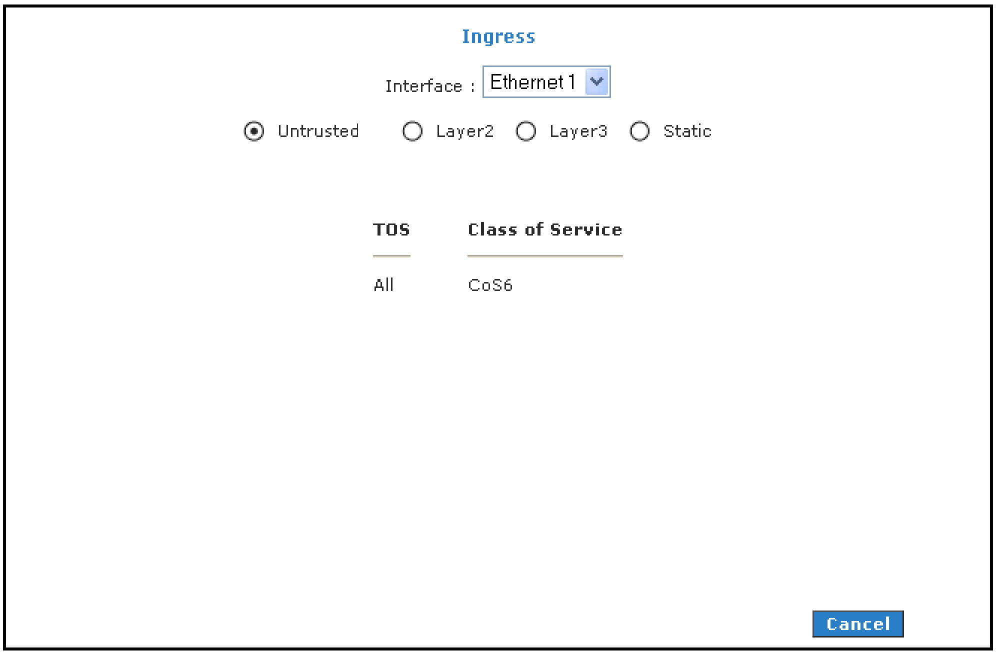
Ingress enables you to configure QoS for packets as soon as they come into the router. The domain mappings are converted to CoS (the common language) so that the priority marking is carried over.

There are four Ingress modes:

- Untrusted mode
- Layer 2
- Layer 3
- Static

Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honored in the router. All packets are treated as CoS6 (best effort).



Ingress

Interface : Ethernet 1

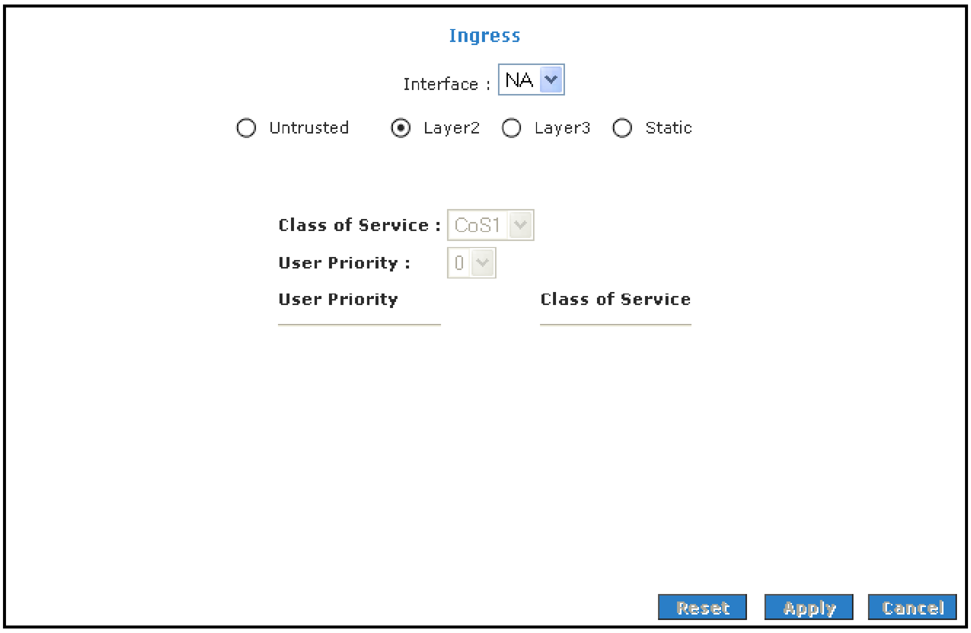
● Untrusted ○ Layer2 ○ Layer3 ○ Static

TOS	Class of Service
All	CoS6

Untrusted mode

Layer 2

Layer 2 allows you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.



Ingress

Interface : NA

○ Untrusted ● Layer2 ○ Layer3 ○ Static

Class of Service : CoS1

User Priority : 0

User Priority	Class of Service

Layer 2

Field	Description
Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.

To configure Ingress Layer 2:

1. Select Advanced Menu.
2. Select QoS > Ingress.
3. Select the **quickstart** interface.
4. Select Layer 2.

5. Select **CoS1** in **Class of Service** and enter **5** in **Priority Bits**. Any packet with priority marking 5 is mapped to CoS1, the highest priority that is normally given to the voice packets.

6. Click **Apply** to temporarily the settings.

7. Select **CoS2** in the **Class of Service** and **1** in **Priority Bits**. Any packet that has a priority bit of 1 is mapped to CoS2, which is the second highest priority. This is given to the high priority packets such as video.

8. Click **Apply** to temporarily activate the settings.

9. Repeat steps 5-7 to add more rules. Up to eight rules can be configured for each interface.

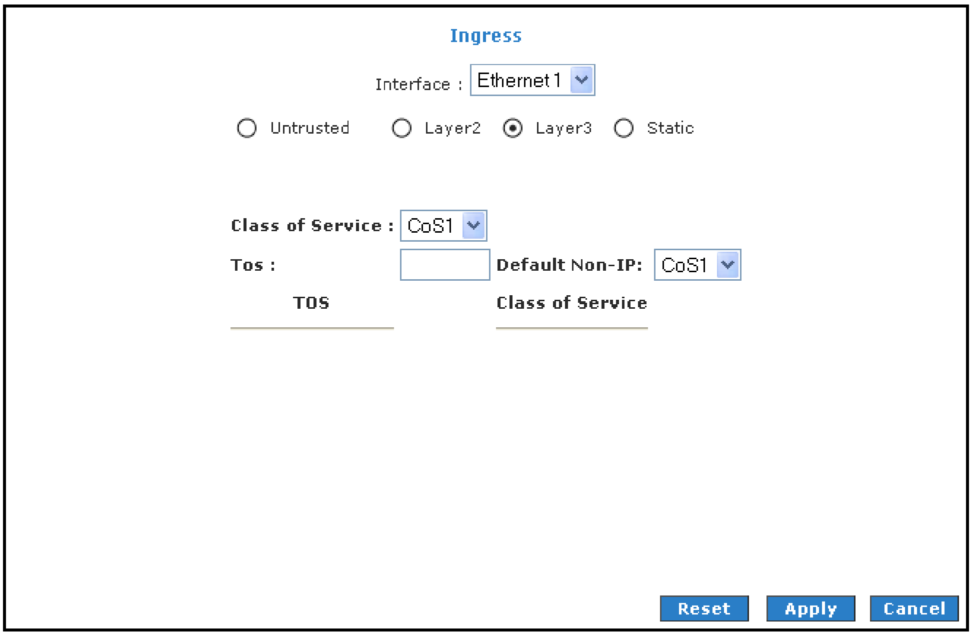
10. To make changes permanent, click **Save Settings**.

Notes:

- Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority.
- Any WAN interface that is not configured has the default Untrusted mode.

Layer 3

The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.



Ingress

Interface : Ethernet1

○ Untrusted ○ Layer2 ● Layer3 ○ Static

Class of Service : CoS1

Tos : Default Non-IP: CoS1

TOS	Class of Service

Layer 3

Field	Description
Interface	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
Class of Service	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
ToS	The Type of Service field takes values from 0 to 255.
Default Non-IP	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have an IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).

To configure Ingress Layer 3:

1. Select **Advanced Menu**.
2. Select **QoS** > **Ingress**.
3. Select the **quickstart** interface.
4. Select **Layer 3**.

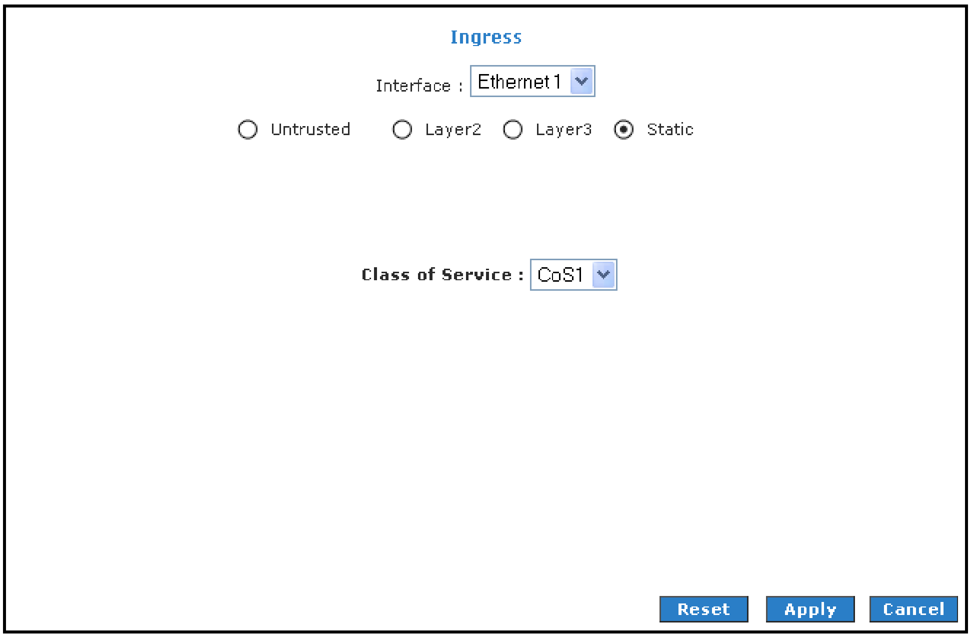
5. Select **CoS1** in **Class of Service** and enter **22** in **Type of Service** (ToS). Any incoming packet from LAN Group 1 (layer 3) with a ToS of 22 is mapped to CoS1, the highest priority, which is normally given to the voice packets.
6. Leave the default value CoS1 in Default Non-IP. Any incoming packet from LAN Group 1 without an IP is mapped to CoS1, the highest priority.
7. Click **Apply** to temporarily activate the settings.
8. Repeat step 5-7 to add more rules to LAN Group 1. Up to 255 rules can be configured for each interface.
9. To make changes permanent, click **Save Settings**.

Notes:

- Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority.
- Any WAN interface that is not configured has the default Untrusted mode.

Static

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.



Static

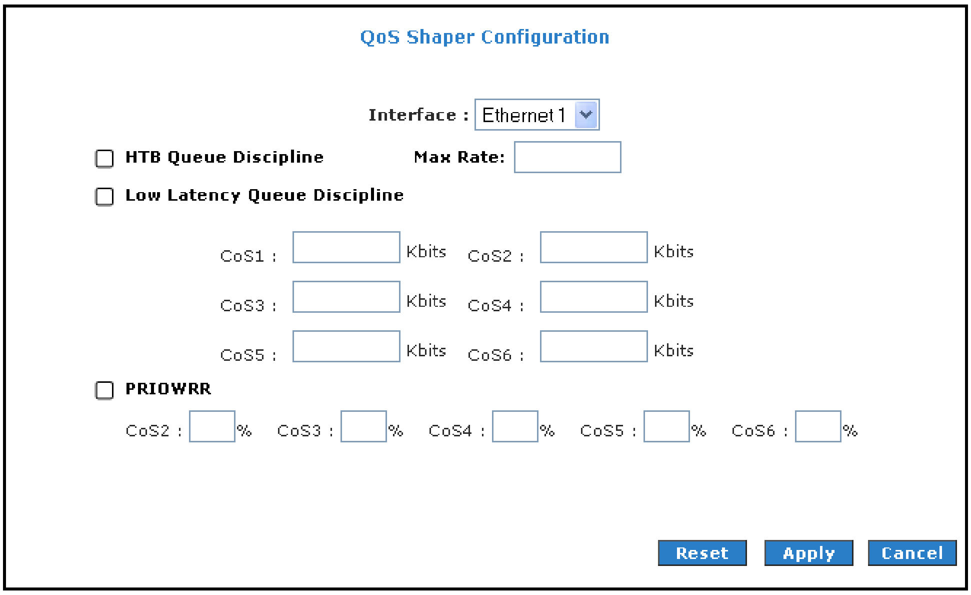
To configure Ingress Layer 3:

1. Select Advanced Menu.
2. Select QoS > Ingress.
3. Select the quickstart interface.
4. Select Static.
5. At the ETHERNET Interface. You are configuring QoS on this interface only. Any WAN/LAN interface that is not configured has the default Untrusted mode.
6. Select CoS1 in Class of Service. All incoming traffic from the ETHERNET interface receives CoS1, the highest priority.
7. Click Apply to temporarily activate the settings.
8. To make changes permanent, click Save Settings.

QoS Shaper Configuration

The Shaper Configuration page is accessed by selecting Shaper on the Advanced main page. Three shaper algorithms are supported:

- HTB
- Low Latency Queue Discipline
- PRIOWRR



QoS Shaper Configuration

Interface : Ethernet 1

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

QoS Shaper Configuration

Note: Egress TCA is required if shaper is configured for that interface.

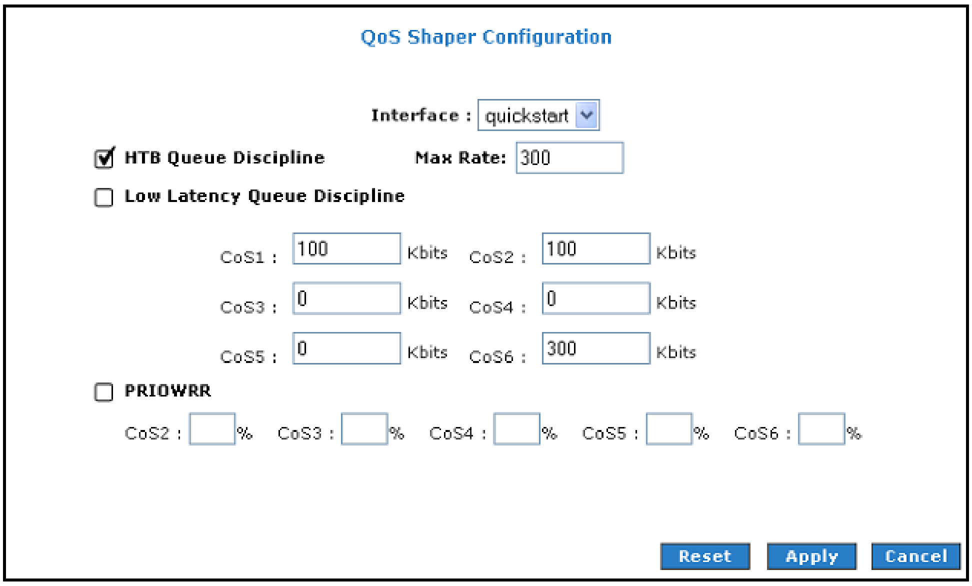
Field	Description
Interface	The selections are WAN/LAN interfaces except WLAN, which does not support Shaper feature. This field needs to be selected before shaper configuration.
Max Rate	This field is applicable for the HTB Queue Discipline and Low Latency Queue Discipline, both are rate-based shaping algorithms.
HTB Queue Discipline	The hierarchical token bucket queue discipline is a rate-based shaping algorithm. This algorithm rate shapes the traffic of a class over a specific interface. All CoSx traffic uses a specific rate to which data will be shaped. For example: If CoS1 is configured to 100Kbps then even if 300Kbps of CoS1 data is being transmitted to the interface only 100Kbps will be sent out.

Low Latency Queue Discipline	This is similar to the above algorithm except that CoS1 is not rate limited. So in the example above CoS1 data is not rate limited to 100Kbps but instead all 300Kbps is transmitted. The side effect is that a misconfigured stream can potentially take all bandwidth.
PRIOWRR	This is a priority based weighted round robin algorithm operating on CoS2-CoS6. CoS1 queues have the highest priority and are not controlled by the WRR algorithm.

Of the three shaping algorithms available on the Shaper Configuration page, only one can be enabled at a time. An example of each configuration is given as follows.

Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300 Kbps of bandwidth, of which 100 Kbps is given to CoS1 and another 100 Kbps is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 Kbps of bandwidth.



QoS Shaper Configuration

Interface : quickstart

☑ HTB Queue Discipline Max Rate: 300

□ Low Latency Queue Discipline

CoS1 : 100 Kbits CoS2 : 100 Kbits

CoS3 : 0 Kbits CoS4 : 0 Kbits

CoS5 : 0 Kbits CoS6 : 300 Kbits

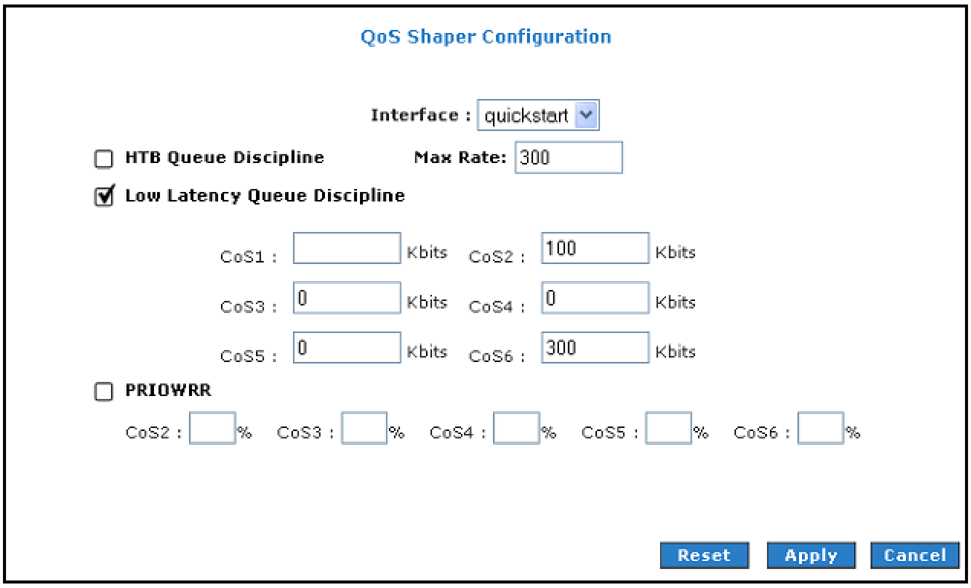
□ PRIOWRR

CoS2 : % CoS3 : % CoS4 : % CoS5 : % CoS6 : %

HTB Queue Discipline enabled

Example 2: Low Latency Queue Discipline Enabled

In this second example, Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 Kbps when there is no CoS1 packets. CoS6 has 300 Kbps when there is no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.



QoS Shaper Configuration

Interface : quickstart

□ HTB Queue Discipline   Max Rate: 300

☑ Low Latency Queue Discipline

CoS1 : [ ] Kbits   CoS2 : 100 Kbits

CoS3 : 0 Kbits   CoS4 : 0 Kbits

CoS5 : 0 Kbits   CoS6 : 300 Kbits

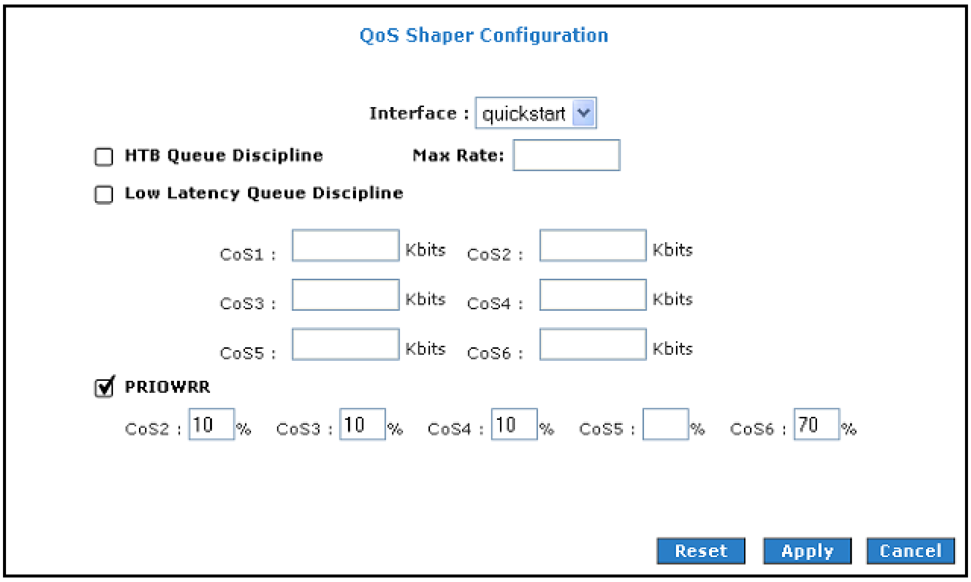
□ PRIOWRR

CoS2 : [ ] %   CoS3 : [ ] %   CoS4 : [ ] %   CoS5 : [ ] %   CoS6 : [ ] %

Low Latency Queue Discipline enabled

Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there is no CoS1 packets, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the Low Latency Queue discipline, except that one is packet-based, and the other is rate-based.



QoS Shaper Configuration

Interface : quickstart

□ HTB Queue Discipline Max Rate:

□ Low Latency Queue Discipline

CoS1 : Kbits CoS2 : Kbits

CoS3 : Kbits CoS4 : Kbits

CoS5 : Kbits CoS6 : Kbits

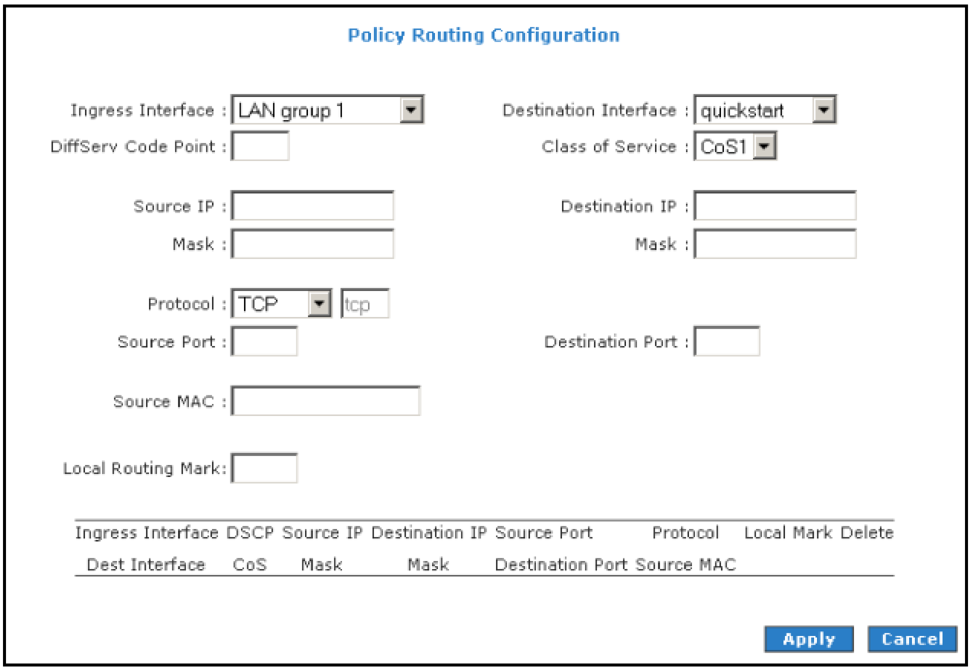
☑ PRIOWRR

CoS2 : 10 % CoS3 : 10 % CoS4 : 10 % CoS5 : % CoS6 : 70 %

PRIOWRR enabled

Policy Routing Configuration

The Policy Routing Configuration enables you to configure policy routing and QoS.



Policy Routing Configuration

Ingress Interface : LAN group 1

Destination Interface : quickstart

DiffServ Code Point :

Class of Service : CoS1

Source IP :

Mask :

Destination IP :

Mask :

Protocol : TCP tcp

Source Port :

Destination Port :

Source MAC :

Local Routing Mark:

Ingress Interface	DSCP	Source IP	Destination IP	Source Port	Protocol	Local Mark	Delete
Dest Interface	CoS	Mask	Mask	Destination Port	Source MAC		

Policy Routing Configuration

Field	Description
Ingress Inter face	The incoming traffic interface for a Policy Routing rule. Selections include LAN interfaces, WAN interfaces, Locally generated (traffic), and not applicable. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP, etc.
Destination Interface	The outgoing traffic interfaces for a Policy Routing rule. Selections include LAN Interfaces and WAN interfaces.
DiffServ Code Point	The diffServ code point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone, additional fields like IP, Source MAC, and/or Ingress Interface should be configured.
Class of Service	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.
Source IP	The IP address of the traffic source.
Mask	The source IP Netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Mask	The Netmask of the destination. This field is required if the destination IP has been entered.

Protocol	The selections are TCP, UDP, ICMP, Specify, and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone, additional fields like IP, Source MAC, and/or Ingress Interface should be configured. This field is also required if the source port or destination port has been entered.
Source Port	The source protocol port. You cannot configure this field without entering the protocol first.
Destination Port	The destination protocol port or port range. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing MAC	This field is enabled only when Locally Generated is selected in the Ingress Interface field. The mark for DNS traffic generated by different applications are described below: ▪ Dynamic DNS: 0xE1 ▪ Dynamic Proxy: 0xE2 ▪ Web Server: 0xE3 ▪ MSNTP: 0xE4 ▪ DHCP Server: 0xE5 ▪ IP tables Utility: 0xE6 ▪ PPP Deamon: 0xE7 ▪ IP Route: 0xE8 ▪ ATM Library: 0xE9 ▪ NET Tools: 0xEA ▪ RIP: 0xEB ▪ RIP v2: 0xEC ▪ UPNP: 0xEE ▪ Busybox Utility: 0xEF ▪ Configuration Manager: 0xF0 ▪ DropBear Utility: 0xF1 ▪ Voice: 0

Currently routing algorithms make decision based on destination address, i.e. only Destination IP address and subnet mask is supported. The Policy Routing page enables you to route packets on the basis of various fields in the packet.

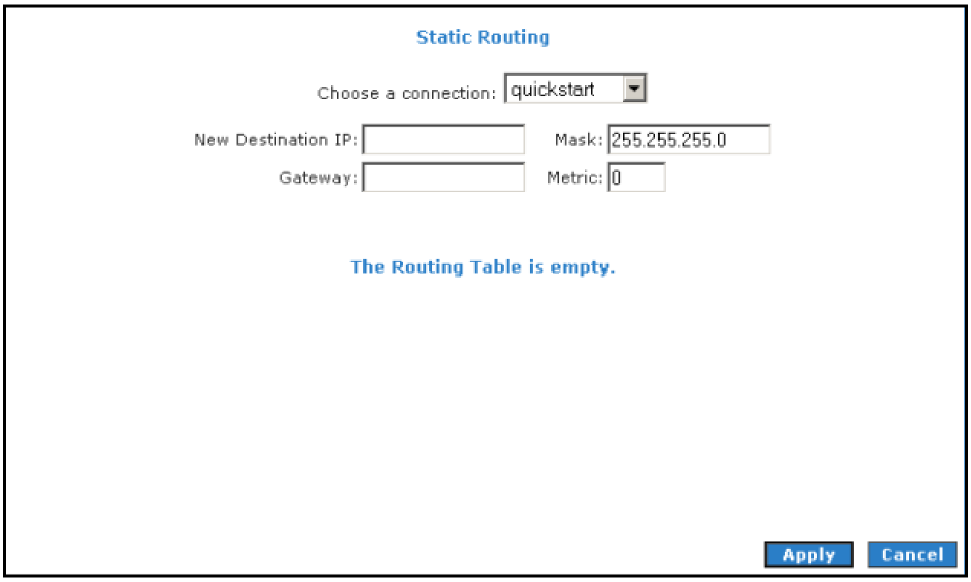
The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

Routing

Static Routing

If the router is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the router.



Static Routing

Choose a connection: quickstart

New Destination IP:
Mask: 255.255.255.0

Gateway:
Metric: 0

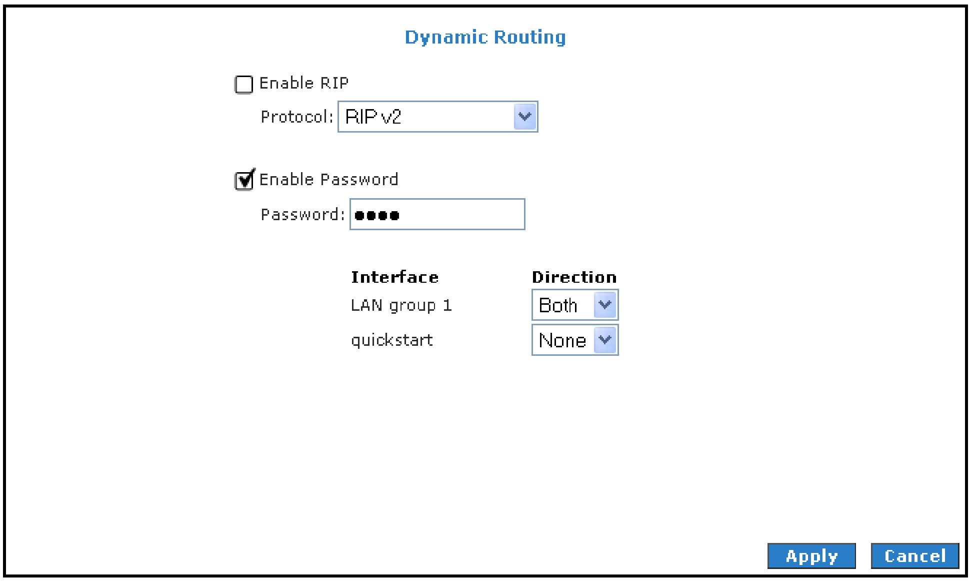
The Routing Table is empty.

Static Routing

The New Destination IP is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0. The Gateway IP address should be the IP address of the gateway device that allows for contact between the Gateway and the remote network or host

Dynamic Routing

Dynamic Routing allows the router to automatically adjust to physical changes in the network. The router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network. The Direction determines the direction that RIP routes will be updated. Selecting In means that the router will only incorporate received RIP information. Selecting Out means that the router will only send out RIP information. Selecting both means that the router will incorporate received RIP information and send out updated RIP information.



Dynamic Routing

□ Enable RIP

Protocol: RIP v2

☑ Enable Password

Password: ●●●●

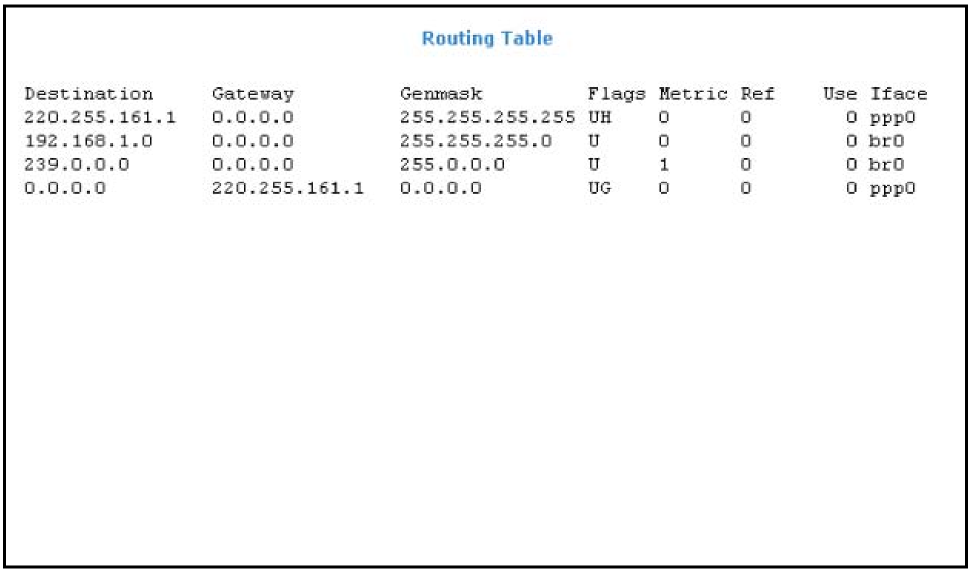
Interface	Direction
LAN group 1	Both
quickstart	None

Dynamic Routing

The protocol is dependent upon the entire network. Most networks support RIP v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If RIP v2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If RIP v1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting.

Routing Table

Routing Table displays the information used by routers when making packet-forwarding decisions. Packets are routed according to the packet's destination IP address.



Routing Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
220.255.161.1   0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 br0
239.0.0.0       0.0.0.0         255.0.0.0       U     1      0        0 br0
0.0.0.0         220.255.161.1   0.0.0.0         UG    0      0        0 ppp0
```

Routing Table

Diagnostics

This chapter provides information about monitoring the router status and viewing product information.

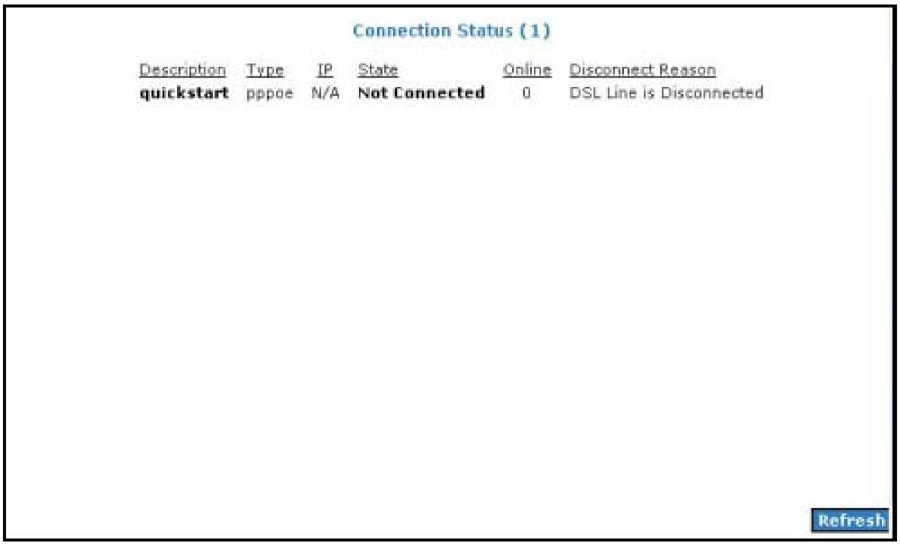
Viewing Status and Product Information

Your router allows you to view the following status and product information:

- Connection Status
- System Log
- Remote Log
- Network Statistics
- DDNS Update Status
- DHCP Clients
- QoS Status
- Modem Status
- Product Information
- DWS Report

Connection Status

Connection Status displays the type of protocol, the WAN IP address, the connection state and the duration of your Internet connection. To view the Connection Status, select the **Status Menu** and then click **Connection Status**.



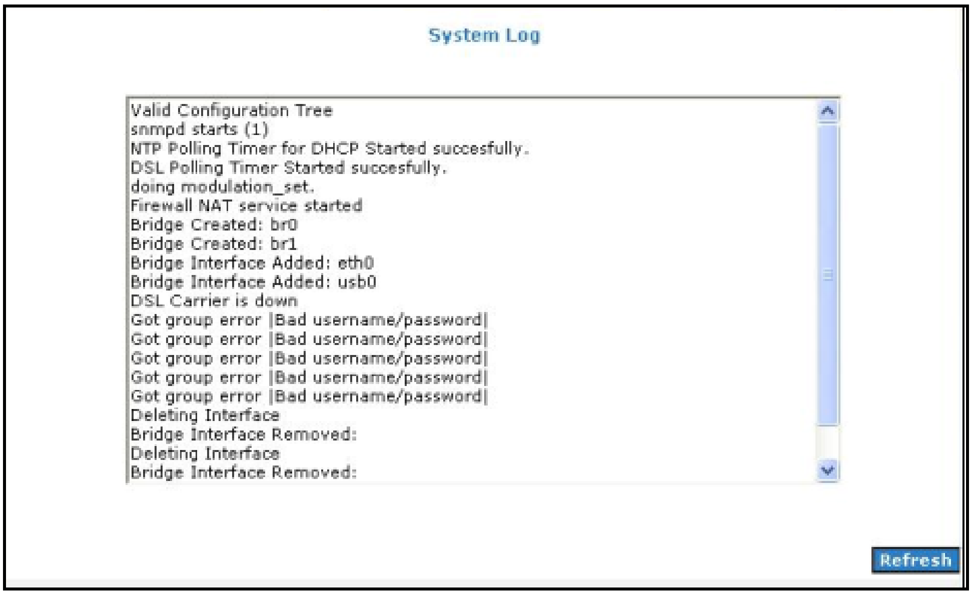
Connection Status (1)

Description	Type	IP	State	Online	Disconnect Reason
quickstart	pppoe	N/A	**Not Connected**	0	DSL Line is Disconnected

Connection Status

System Log

System Log displays the router log. Depending on the severity level, the information log will generate log reports to a remote host if remote logging is enabled. To view the System Log, select the **Status Menu** and then click **System Log**.



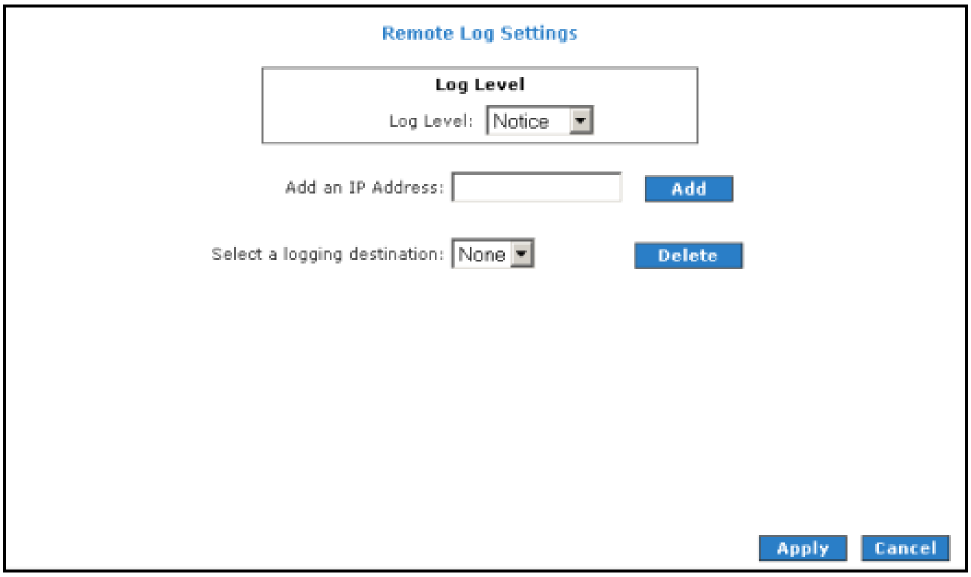
```
Valid Configuration Tree
snmpd starts (1)
NTP Polling Timer for DHCP Started succesfully.
DSL Polling Timer Started succesfully.
doing modulation_set.
Firewall NAT service started
Bridge Created: br0
Bridge Created: br1
Bridge Interface Added: eth0
Bridge Interface Added: usb0
DSL Carrier is down
Got group error |Bad username/password|
Got group error |Bad username/password|
Got group error |Bad username/password|
Got group error |Bad username/password|
Got group error |Bad username/password|
Deleting Interface
Bridge Interface Removed:
Deleting Interface
Bridge Interface Removed:
```

System Log

Remote Log

Remote Log allows you to forward all logged information to one (or more) remote computer. The type of information forwarded to the remote computer depends on the Log level. Each log message belongs to a certain log level, which indicates the severity of the event.

When you configure remote logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the log server and can be viewed using the server log application, which can be downloaded from the web.



Remote Log Settings

Log Level

Log Level: Notice

Add an IP Address:

Select a logging destination: None

Remote Log Settings

To enable remote logging:

1. Select the **Status Menu** and then click **Remote Log**.
2. Select a **Log Level**. There are 8 log levels listed below in order of severity.
   - **Panic** System panic or other condition that causes the router to stop functioning.
   - **Alert** Conditions that require immediate correction, such as a corrupted system database.
   - **Critical** Critical conditions such as hard drive errors.

- **Error** Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- **Warning** Conditions that warrant monitoring.
- **Notice** (Default) Conditions that are not errors but might warrant special handling.
- **Info** Events or non-error conditions of interest.
- **Debug** Software debugging message. Specify this level only when directed by a technical support representative.

3. Enter the **IP Address** where the log will be sent to and then click **Add**.
4. Click **Apply**. The IP address will appear in the **Select a logging destination** drop-down menu.
5. To make changes permanent, click **Save Settings**.

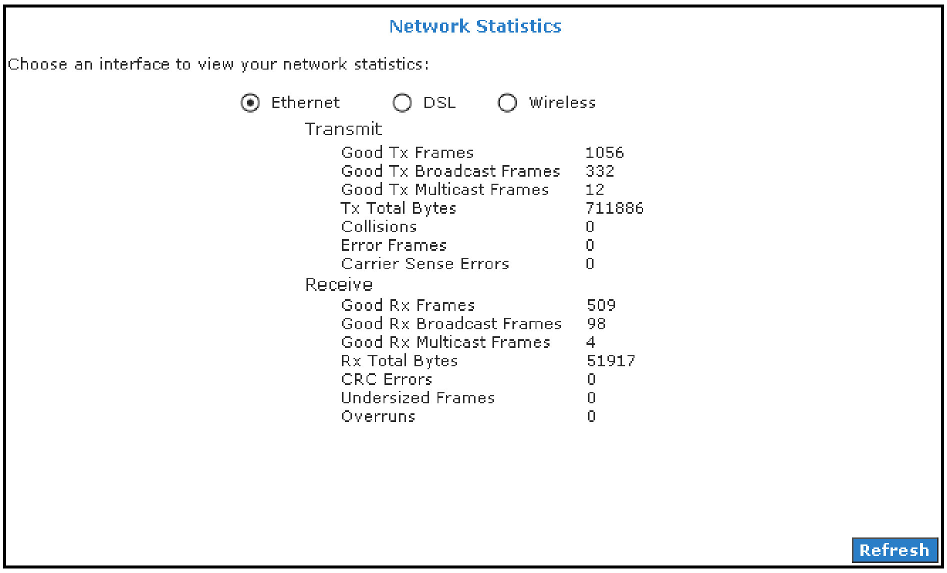
Note: When you select a log level, all log information within this severity level and levels above (meaning, more severe levels) will be sent to the remote host.

To disable a remote log:

1. Select the IP address to be deleted from the **Select a logging destination** drop-down menu.
2. To temporarily implement the changes, click **Apply**.
3. To make changes permanent, click **Save Settings**.

Network Statistics

The Ethernet and DSL line statuses are displayed in this page. To view the Network Statistics, select the **Status Menu** and then click **Network Statistics**.



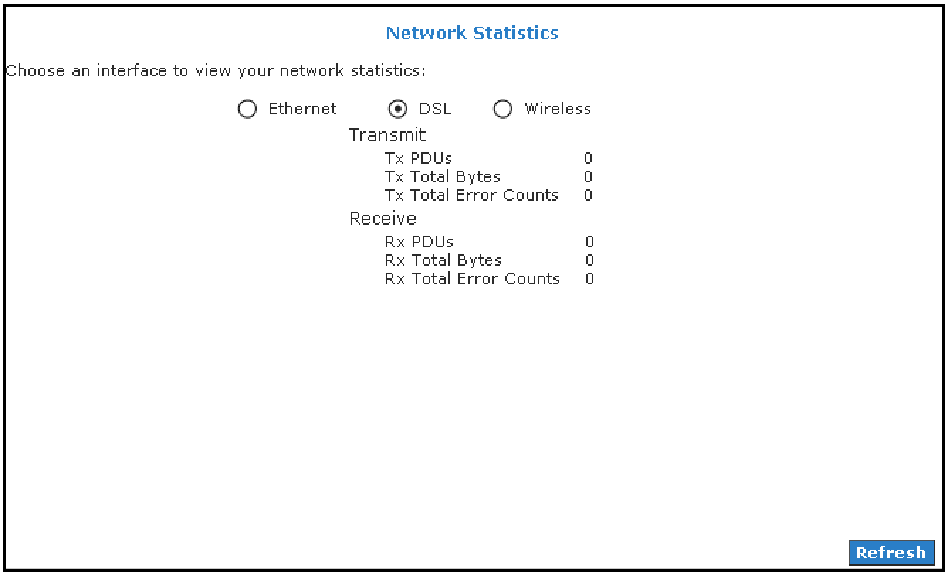
Network Statistics

Choose an interface to view your network statistics:

● Ethernet ○ DSL ○ Wireless

```
Transmit
     Good Tx Frames              1056
     Good Tx Broadcast Frames    332
     Good Tx Multicast Frames    12
     Tx Total Bytes              711886
     Collisions                  0
     Error Frames                0
     Carrier Sense Errors        0
Receive
     Good Rx Frames              509
     Good Rx Broadcast Frames    98
     Good Rx Multicast Frames    4
     Rx Total Bytes              51917
     CRC Errors                  0
     Undersized Frames           0
     Overruns                    0
```

Network Statistics – Ethernet



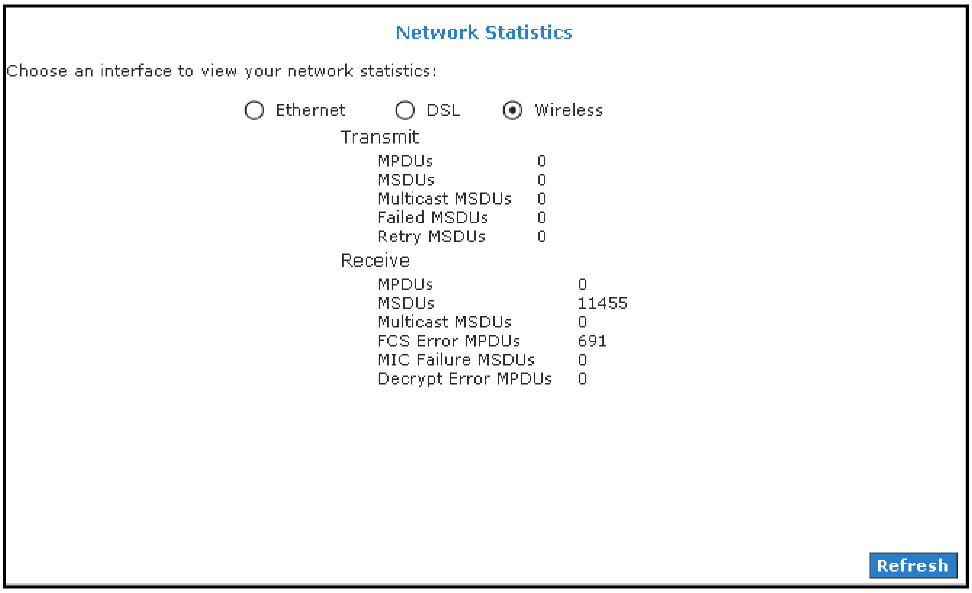
Network Statistics

Choose an interface to view your network statistics:

○ Ethernet ● DSL ○ Wireless

```
Transmit
     Tx PDUs               0
     Tx Total Bytes        0
     Tx Total Error Counts 0
Receive
     Rx PDUs               0
     Rx Total Bytes        0
     Rx Total Error Counts 0
```

Network Statistics – DSL



Network Statistics

Choose an interface to view your network statistics:

○ Ethernet ○ DSL ● Wireless

Transmit

MPDUs	0
MSDUs	0
Multicast MSDUs	0
Failed MSDUs	0
Retry MSDUs	0

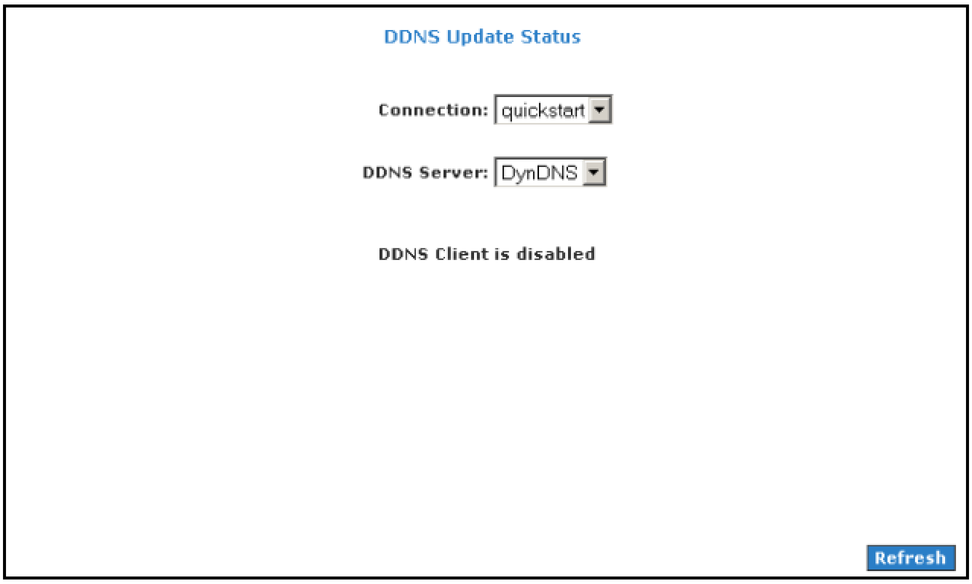
Receive

MPDUs	0
MSDUs	11455
Multicast MSDUs	0
FCS Error MPDUs	691
MIC Failure MSDUs	0
Decrypt Error MPDUs	0

Network Statistics - Wireless

DDNS Update Status

DDNS Update Status displays the WAN connection status. By default, DDNS is disabled. When the DDNS is enabled, the DDNS client updates every time the router gets a new IP address. To view the DDNS Update Status, select the **Status Menu** and then click **DDNS Update Status**.



DDNS Update Status

Connection: quickstart

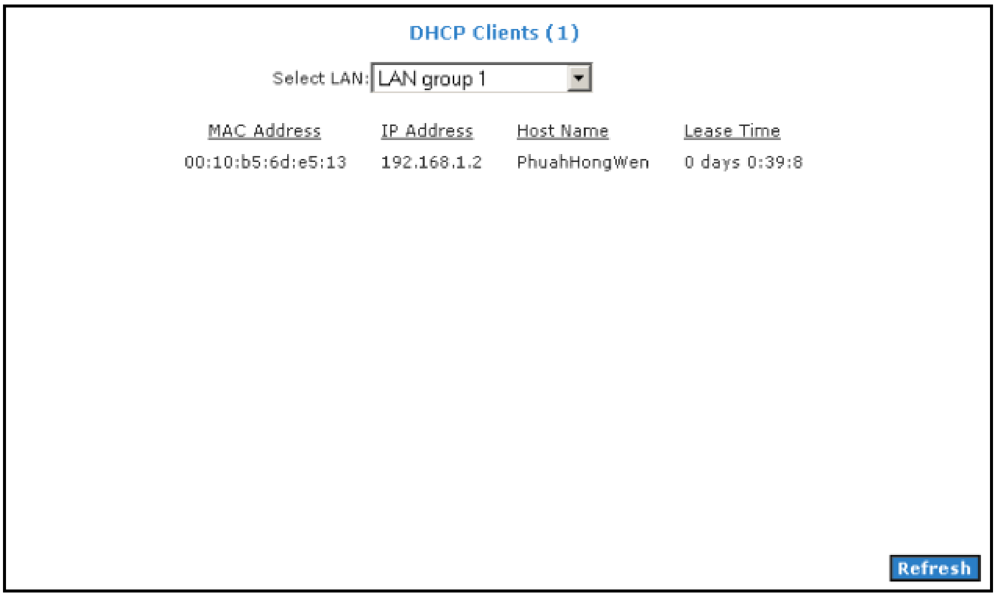
DDNS Server: DynDNS

DDNS Client is disabled

DDNS Update Status

DHCP Clients

DHCP Clients displays the MAC address, IP address, host name, and lease time. To view the DHCP Clients, select the **Status Menu** and then click **DHCP Clients**.



DHCP Clients (1)

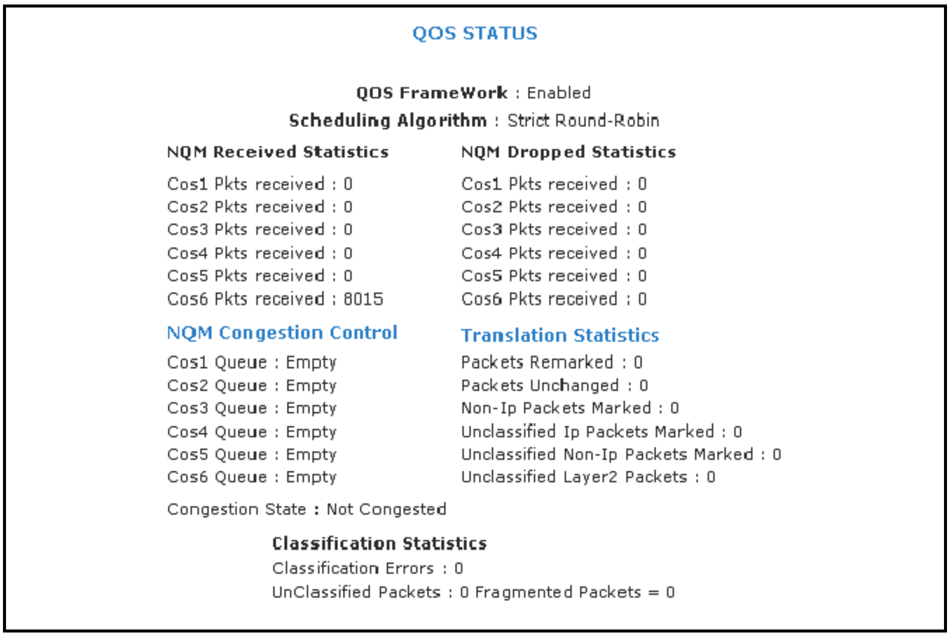
Select LAN: LAN group 1

MAC Address	IP Address	Host Name	Lease Time
00:10:b5:6d:e5:13	192.168.1.2	PhuahHongWen	0 days 0:39:8

DHCP Clients

QoS Status

This page displays the Quality of Service and the packet statistics. To view the QoS Status, select the **Status Menu** and then click **QoS Status**.



QOS STATUS

QOS FrameWork : Enabled

Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics

Cos1 Pkts received : 0
Cos2 Pkts received : 0
Cos3 Pkts received : 0
Cos4 Pkts received : 0
Cos5 Pkts received : 0
Cos6 Pkts received : 8015

NQM Dropped Statistics

Cos1 Pkts received : 0
Cos2 Pkts received : 0
Cos3 Pkts received : 0
Cos4 Pkts received : 0
Cos5 Pkts received : 0
Cos6 Pkts received : 0

NQM Congestion Control

Cos1 Queue : Empty
Cos2 Queue : Empty
Cos3 Queue : Empty
Cos4 Queue : Empty
Cos5 Queue : Empty
Cos6 Queue : Empty

Translation Statistics

Packets Remarked : 0
Packets Unchanged : 0
Non-Ip Packets Marked : 0
Unclassified Ip Packets Marked : 0
Unclassified Non-Ip Packets Marked : 0
Unclassified Layer2 Packets : 0

Congestion State : Not Congested

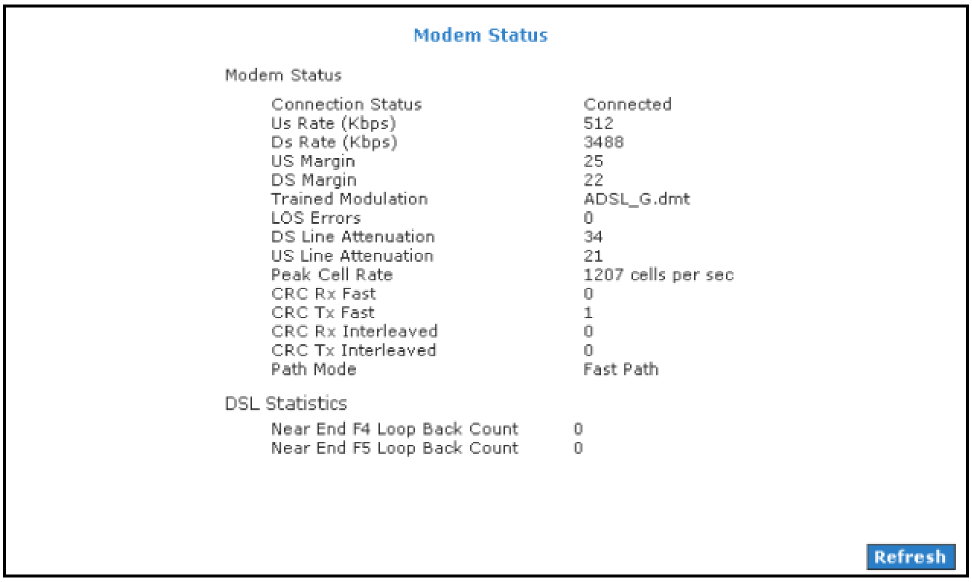
Classification Statistics

Classification Errors : 0
UnClassified Packets : 0 Fragmented Packets = 0

QoS Status

Modem Status

This page displays the model status. To view the Modem Status, select the **Status Menu** and then click **Modem Status**.



Modem Status

Modem Status

Connection Status	Connected
Us Rate (Kbps)	512
Ds Rate (Kbps)	3488
US Margin	25
DS Margin	22
Trained Modulation	ADSL_G.dmt
LOS Errors	0
DS Line Attenuation	34
US Line Attenuation	21
Peak Cell Rate	1207 cells per sec
CRC Rx Fast	0
CRC Tx Fast	1
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path

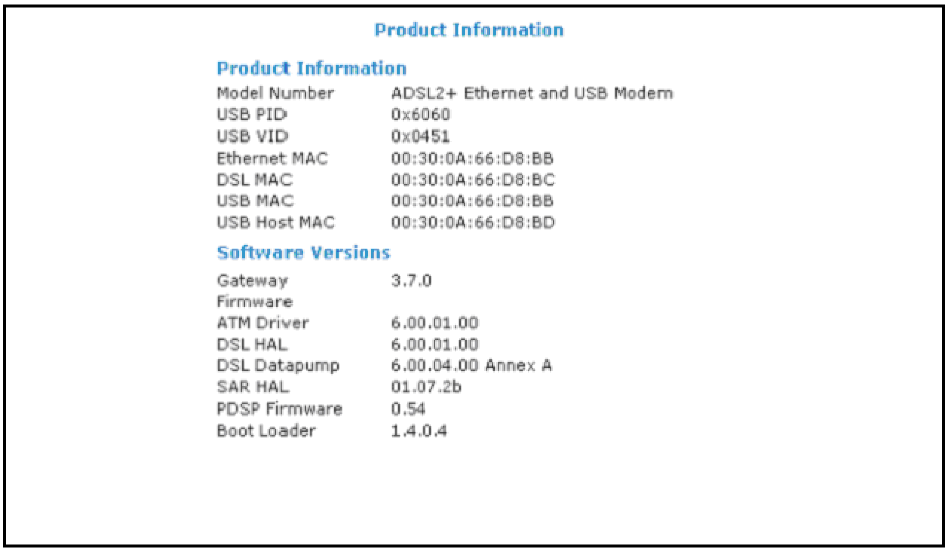
DSL Statistics

Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

Modem Status

Product Information

This page displays the product information and software versions. To view the Product Information, select the **Status Menu** and then click **Product Information**.



Product Information

Product Information

Model Number	ADSL2+ Ethernet and USB Modem
USB PID	0x6060
USB VID	0x0451
Ethernet MAC	00:30:0A:66:D8:BB
DSL MAC	00:30:0A:66:D8:BC
USB MAC	00:30:0A:66:D8:BB
USB Host MAC	00:30:0A:66:D8:BD

Software Versions

Gateway	3.7.0
Firmware	
ATM Driver	6.00.01.00
DSL HAL	6.00.01.00
DSL Datapump	6.00.04.00 Annex A
SAR HAL	01.07.2b
PDSP Firmware	0.54
Boot Loader	1.4.0.4

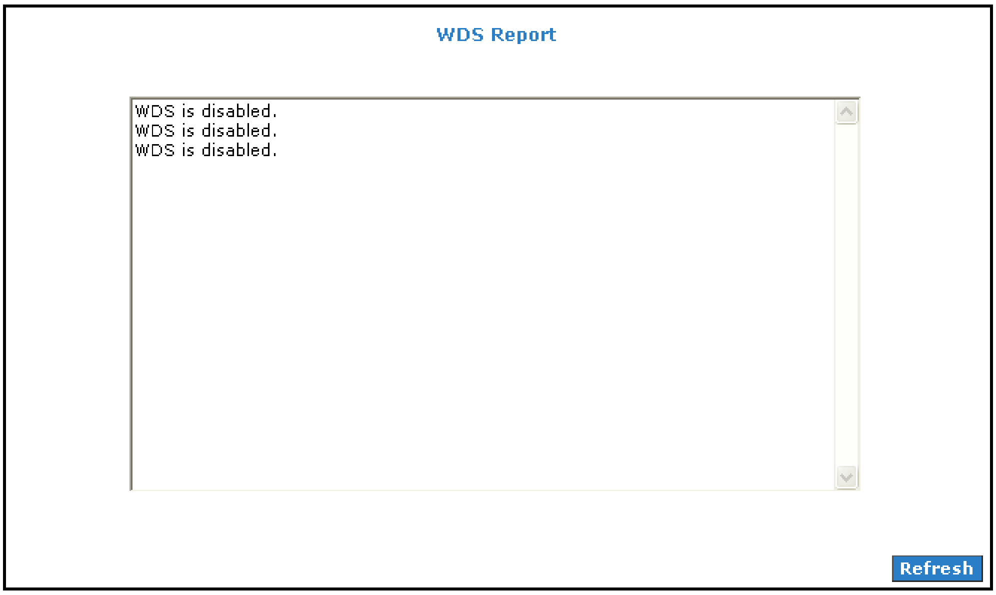
Product Information

WDS Report

This page displays the following WDS-related wireless activities:

- WDS configuration and states
- WDS management statistics
- WDS database

To view the WDS Report, select the **Status Menu** and then click **WDS Report**.

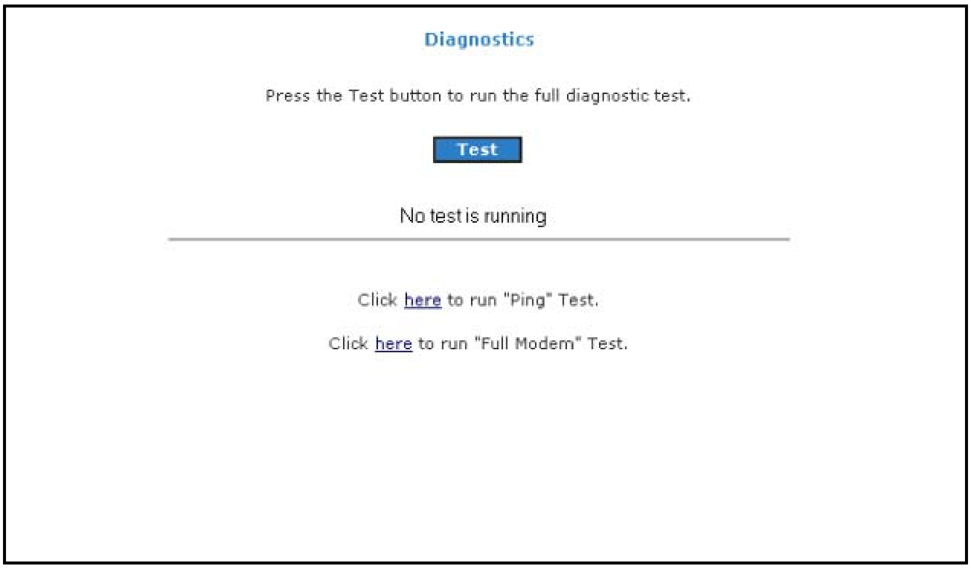


```
WDS is disabled.
WDS is disabled.
WDS is disabled.
```

WDS Report

Performing Diagnostic Tests

Diagnostic Test is used for investigating whether the router is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link.



Diagnostics

Press the Test button to run the full diagnostic test.

No test is running

Click here to run "Ping" Test.

Click here to run "Full Modem" Test.

To run diagnostic test:

1. Select the **Basic Menu** and then click **Diagnostics**. This opens the **Diagnostics** page.
2. Click **Test**. The test status will appear after running the diagnostic test. If a test failed, click **Help** to get the solution.

Ping Test

Once you have your router configured, it is a good idea to make sure you can ping the network. If you can ping an IP on the WAN side successfully, you should be able to surf the Internet.

To perform a ping test:

1. Select the **Basic Menu** and then click **Diagnostics**.
2. Click **Ping Test**. This opens the **Ping Test** page.

3. Change or leave the default settings of the following fields:
   - Enter the IP address to ping
   - Packet size
   - Number of echo request
4. Click **Test**.

   The ping results are displayed in the page. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, you should restart the router.

Full Modem Test

This test is used to check if your modem is properly connected to the network.

To perform a Full Modem test:

1. Select the **Basic Menu** and then click **Diagnostics**.
2. Click **Full Modem Test**. This opens the **Modem Test** page.
3. Select your connection and then click **Test**.

Updating the Firmware

When updating the firmware, make sure you are using the correct file. Once the upgrade is complete the router will reboot. You will need to log back into the router after the firmware upgrade is completed.

To update the firmware:

1. Select the **Advanced Menu** and then click **Firmware Upgrade**. This opens the **Firmware Upgrade** page.
2. Click **Browse** and then locate the firmware file.

3. Click **Update Gateway**. The update may take a few minutes. Make sure that the power is not turned off during the update process.

Restoring the Default Settings

To reset to the default factory settings, press **RESET** for 10 seconds. This can be found at the router's back panel. When you reset, all the software updates will be lost.

To access the web interface again, you need to install the router anew.