User Manual

DSL1000EW(L)

ADSL2/2+ 4-Ports 802.11b/g

LIMITATION OF LIABILITY AND DAMAGES

THE PRODUCT AND THE SOFTWARES WITHIN ARE PROVIDED "AS IS," BASIS. THE MANUFACTURER AND MANUFACTURER'S RESELLERS (COLLECTIVELY REFERRED TO AS "THE SELLERS") DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. IN NO EVENT WILL THE SELLERS BE LIABLE FOR DAMAGES OR LOSS, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL WILLFUL, PUNITIVE, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL, DAMAGES, DAMAGES FOR LOSS OF BUSINESS PROFITS, OR DAMAGES FOR LOSS OF BUSINESS OF ANY CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THE USE OR THE INABILITY TO USE THE PRODUCT OR THE SOFTWARES, INCLUDING BUT NOT LIMITED TO THOSE RESULTING FROM DEFECTS IN THE PRODUCT OR SOFTWARE OR DOCUMENTATION, OR LOSS OR INACCURACY OF DATA OF ANY KIND, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT OR ITS SOFTWARE IS ASSUMED BY CUSTOMER. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABLITY FOR DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO THE PARTIES. IN NO EVENT WILL THE SELLERS' TOTAL CUMULATIVE LIABILITY OF EACH AND EVERY KIND IN RELATION TO THE PRODUCT OR ITS SOFTWARE EXCEED THE AMOUNT PAID BY CUSTOMER FOR THE PRODUCT.

Contents

About the Router

Your router offers an easy way of integrating your computer and other network devices into a single network. Here are some of the benefits you can obtain from using the router in your home or office:

Integrated Modem Feature Your router is an ideal solution for high speed Internet connectivity. It is capable of handling the fastest data transfer speed from your Internet provider and sharing this within your local network devices.

Top Notch Security Your router utilizes built-in firewall security to block service attacks. For added flexibility, it can be modified to allow specific applications to pass through while blocking intrusive threats at the same time.

Intuitive User Interface Applying changes on the router settings can be done easily using a Web browser. The router uses a simplified user interface that allows you to apply the configurations you want for the various features of the router.

Your router will serve as the central figure in establishing your local area network (LAN) by using a combination of hardware and software. The hardware includes the cables, wireless access points, and Ethernet ports that create the path to connect your devices. The software part includes the applications that manage the flow of information in these devices.

You can complete the basic installation and Internet connection within 8 minutes. Some more time is needed if you intend to utilize more advanced functions but it can be worth it. Advanced features like port forwarding will help you create your own web server to store your Web site, Dynamic DNS allows you to access your network from the Internet, and remote access enables you to configure your router settings from different locations.

Once installation is complete, it will be much more easier for you to enjoy voice communication, high speed Internet, and data/audio/video sharing within your network.

Main Features

ADSL Support

- ANSI T1.413 issue 2, ITU-T G.992.1 (G.dmt) and G.992.2 (G.lite) compliant
- G.992.3 (ADSL2), G.992.5 (ADSL2+), RE-ADSL Ready
- ATM Layer with Traffic shaping QoS Support (UBR, CBR, VBR-rt, VBR-nrt)
- AAL ATM Attributes - AAL5
- Multiple PVC up to 8 support
- Spectral compatibility with POTS
- F4 & F5 OAM Loopback/Send and Receive
- Annex A, Annex B, Annex M Support
- TR048 and TR067 compliant
- PVC support VPI=8, VCI=35

Encapsulation Support

- RFC2684 Bridge and Routed LLC and VC Mux support
- RFC2364 PPPoA Client support
- RFC2516 PPPoE Client support
- RFC2225/RFC1577 Classical IP Support
- Transparent Bridge Support
- PAP/CHAP/MS-CHAP for Password Authentication Support

Network Support

- Static IP, Dynamic RIP v1/v2 routing support
- IP/TCP/UDP/ICMP/ARP Application Support
- Network Address Translation (NAT)
- PVC to VLAN Mapping
- Port Forwarding/Triggering
- Easy setup of Port Forwarding rules for popular Games/Application
- NAT Application Level Gateway for popular applications
- DHCP Server/Relay/client
- DNS Relay Agent
- DMZ support
- SIP ALG (Application Layer Gateway) support

- Multiple Sessions IP Sec and PPTP/L2TP VPN pass through support
- PPP Always on
- PPP Dial on Demand with configurable timeout
- Universal Plug and Play Support
- DDNS (Dynamic DNS) Support
- IGMP Proxy Support (IGMP v1 and v2)
- SNTP Support
- QoS Support (DSCP, TOS), including Diffserv, IEEE802.1p - Priority bit, IEEE802.1q - VLAN triggering
- PPP/DHCP Auto Detection (Future release)
- TR-069 Compliant

WLAN Support

- Wireless on Motherboard (WOMBO)
- IEEE 802.11, 802.11b and 802.11g compliant
- Supports 802.11b, 802.11g simultaneously
- Transmit output power up to 20dBm (standard)
- Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi ^{tm}) Standard
- Support seamless WLAN roaming
- Frequency Band:
    - 2412 MHz - 2462 MHz (North America/FCC)
    - 2412 MHz - 2472 MHz (ETSI/Europe)
    - 2412 MHz - 2484 MHz (Japan)
    - 2457 MHz - 2472 MHz (France)
    - 2457 MHz - 2462 MHz (Spain)
- Support Direct Sequence Spread Spectrum (DSSS) technology
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK
- Wireless Media Access Protocol- CSMA/CA with ACK
- 64/128 WEP Encryption
- WPA/WPA2 Support
- MAC filtering Support
- Dynamic Rate Scaling from 54, 48, 36, 24, 12, 11, 9, 6, 5.5, 2, 1 Mb/s
- Operating Range of >300 Meters (Open Air)
- WDS Support (Wireless Distribution System)
- Multiple SSID Support (2)

Management Support

- Web Based HTTP management GUI
- TFTP/FTP Support for Firmware Upgrade
- Web Based Firmware Upgrade (Local)
- Soft Factory Reset Button via Web GUI
- Diagnostic Test (DSL, OAM (ADSL), Network (ADSL), Ping Test)
- TR068 - WAN Access
- Telnet with CLI (Read and Write) configuration
- Syslog Support
- Firmware upgrade-able for future feature enhancement
- Quick firmware upgrade button (depopulation option)
- TR-069 Compliant
- SNMP v1 and v2
- SSH Support

Security Support

- NAT for basic Firewall support
- Packet Filtering Firewall Support
- Stateful Packet Inspection Support
- Protection against Denial of Service attacks
- Password Authentication to Modem
- URL filtering/ Parental Control (Option)
- Real-Time Attack and Alert Logs (Option)

Requirements

Your computer must meet the following minimum requirements.

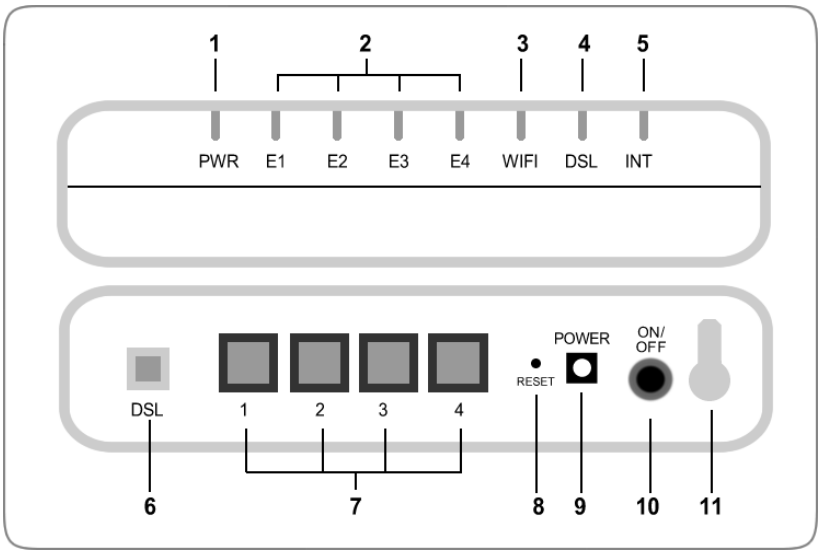
- Any operating system can be used
- Internet Explorer 4.0 or Netscape Navigator 3.02
- 233MHz processor
- CD-ROM Drive
- Ethernet network adapter
- An active DSL Internet account

Package Contents

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

- Router
- Ethernet cable
- Telephone cable
- POTS Splitter (Optional)
- 12V 1A DC Power Adapter
- Easy Start Guide
- Resource CD

Device Design

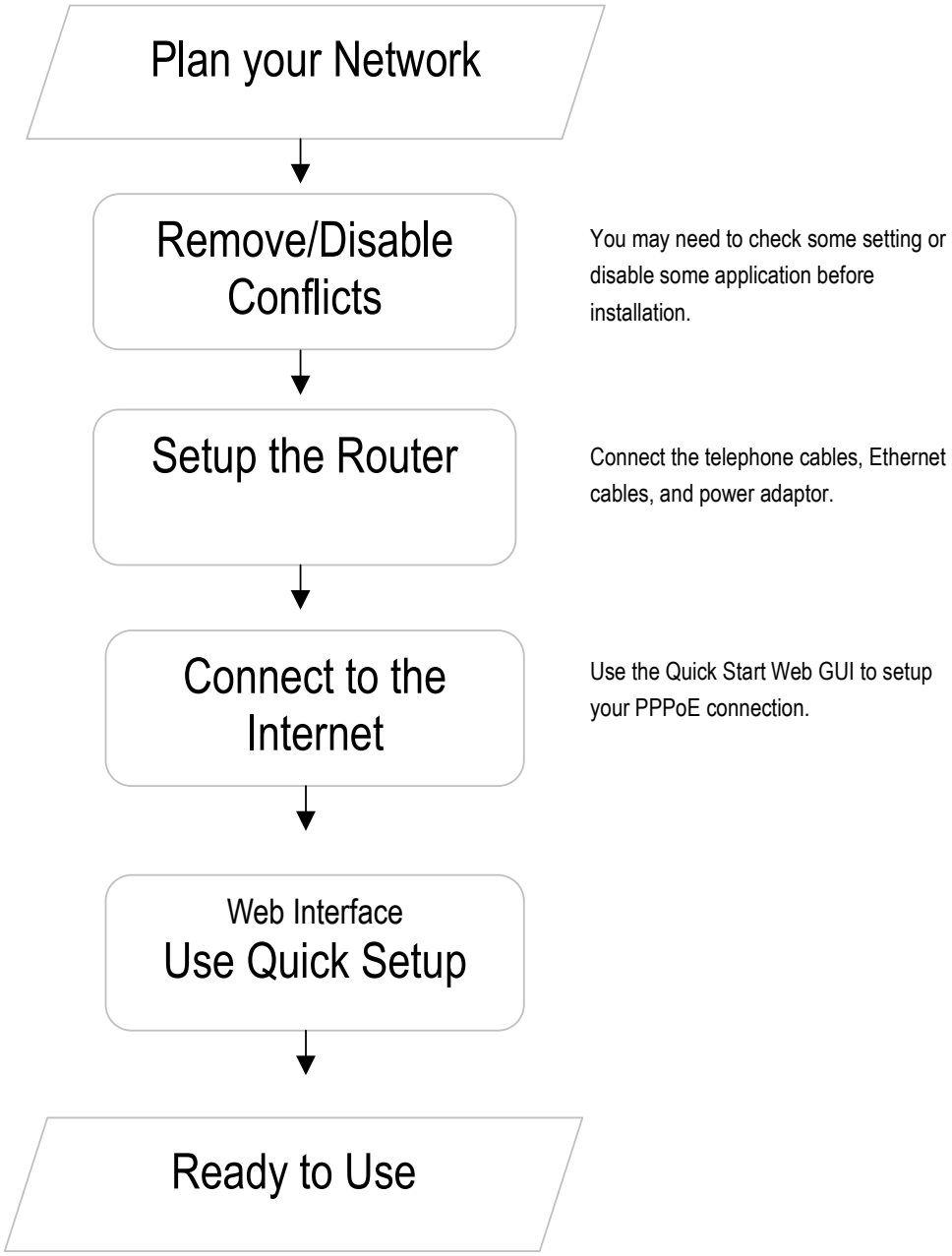


	Label	Action	Description
1	**POWER**	Off	No power is supplied to the device
		Steady green light	Connected to an AC power supply
		Steady red light	Error on the device
2	**ETHERNET 1-4**	Off	No Ethernet connection
		Steady green light	Connected to an Ethernet port
		Blinking green light	Transmitting/Receiving data
3	**WIFI**	Off	Access point is disabled
		Steady green light	Access point is enabled
		Blinking green light	Transmitting/Receiving data
4	**DSL**	Off	No DSL signal
		Blinking green light	Establishing DSL signal
		Steady green light	DSL signal is established
5	**INTERNET**	Off	No Internet connection
		Steady green light	Connected to the Internet
		Blinking green light	Transmitting/Receiving data

		Steady red light	Cannot establish Internet connection
6	**DSL**		Connecting the telephone cable
7	**ETHERNET 1-4**		Connecting with computers/devices through Ethernet cable
8	**RESET**		Resetting the device. Press for 10 seconds to reset.
9	**POWER (12V 1A DC)**		Connecting with the 12V 1A DC power adapter
10	**ON/OFF**		Switching the device on/off
11	**Antenna**		Sending/receiving wireless signals

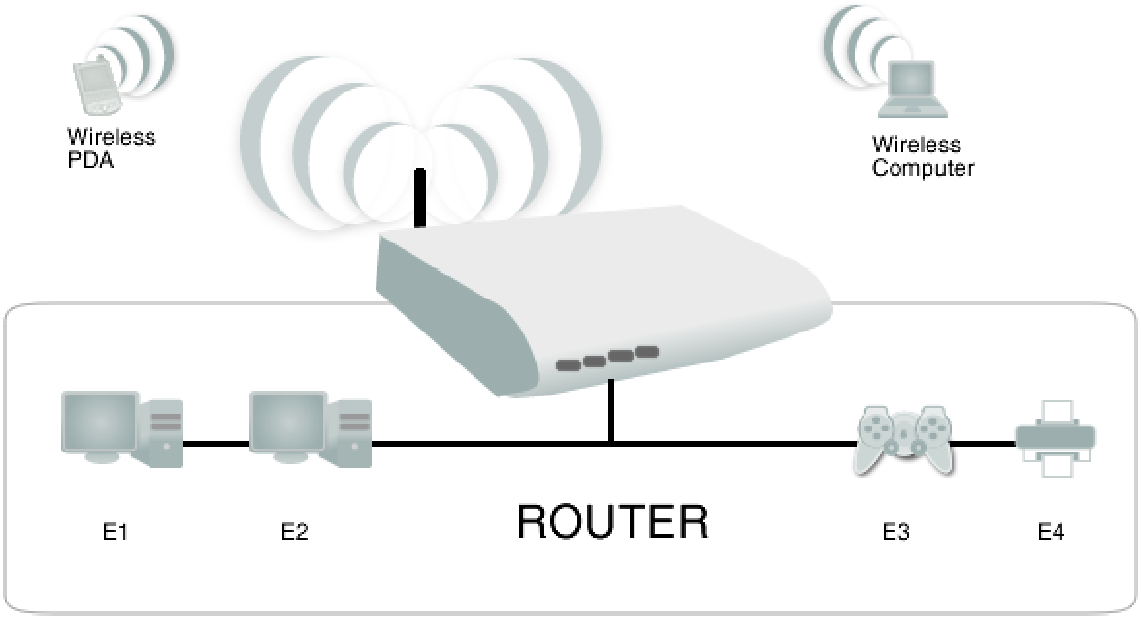
Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps needed to complete the installation. Brief descriptions appear beside each step. Detailed instructions are provided in the subsequent pages.



Planning Your Network

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

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 start the installation.

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

Check if your computer uses the default TCP/IP settings.

To check 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 Internet Properties.
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 Internet Properties.

Removing Temporary Internet Files

Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to clean the cache and remove footprints left by the Web pages you visited.

To remove temporary Internet files:

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

Setup the Device

When installing the router, find an area where there are enough electrical outlets for the router, the main computer, and your other computer devices.

To setup the router:

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. If you have another device you need to connect through wire into the router, use another piece of Ethernet cable. Plug one end of the Ethernet cable from the computer's Ethernet port and then plug the other end into an available Ethernet port in the router.
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.

POTS Splitter

Your phone line carries with it both phone calls and Internet signals. When you are using the Internet, the connection produces high-pitched tones that can affect your voice calls when using the phone. Installing a Plain Old Telephone Service (POTS) splitter separates the two signals and eliminates the noise.

To setup a telephone on the POTS Splitter:

a. Locate the phone jack in your house.

b. Insert the POTS Splitter into the phone jack.

c. Plug one end of the telephone cable from the POTS Splitter's **TEL** port and then plug the other end into the telephone.

4. Connect the power adapter from the router's 12V 1A DC port into the electrical outlet.
5. Press ON.

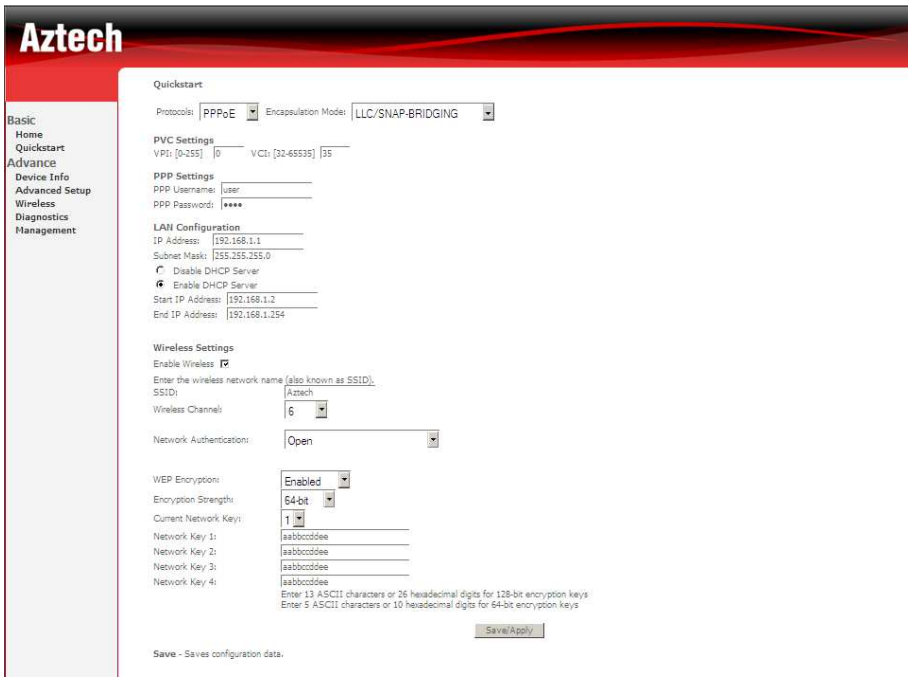
Connecting to the Internet

You can use the Web Interface to setup your Internet connection.

Connecting Via Quick Setup

To connect to the Internet via the Web Interface:

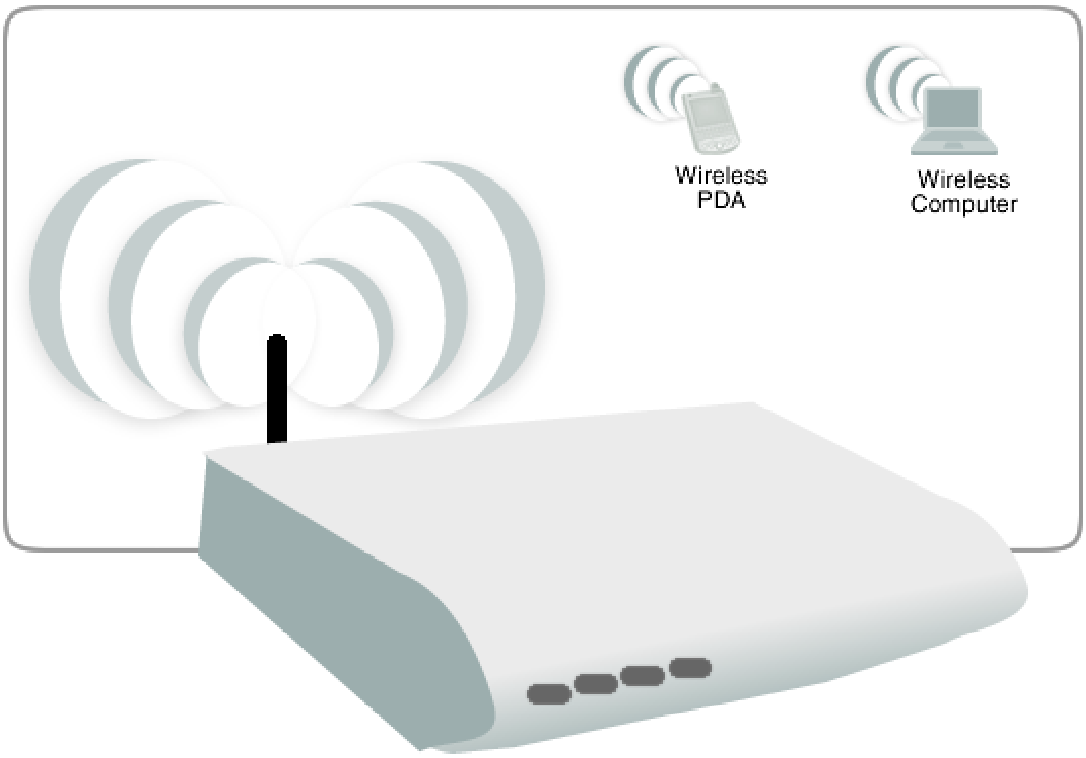
1. Open your browser.
2. Enter 192.168.1.1 and then press Enter.
3. Enter the User name and Password, and then click OK. The default User name and Password is *admin*.
4. Select Quickstart.



5. Enter the connection settings
    a. Select a Protocol and Encapsulation Mode
    b. Enter PVC Settings
    c. Enter the PPP Username and Password
6. Click Save/Apply.

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.



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.

About the Web User Interface

The Web User Interface is used to configure the router settings.

Accessing the Web User Interface

To access the Web User Interface:

1. Open your browser.
2. Enter 192.168.1.1 and then press Enter.
3. Enter the User name and Password, and then click OK.

Default Username and Password is *admin*.

Menus

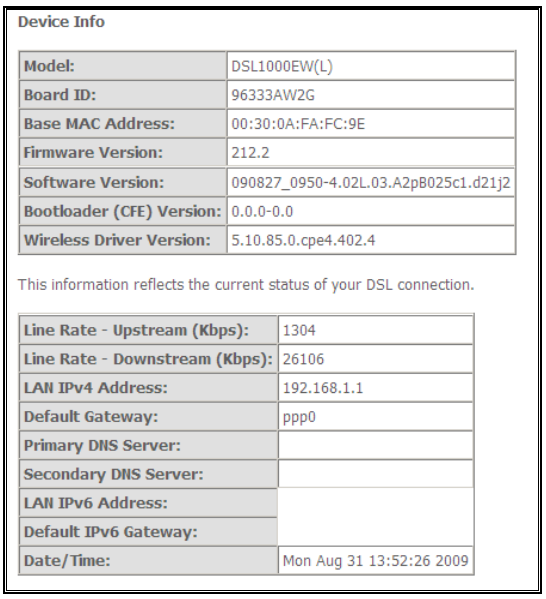
The Web User Interface includes the following menus:

- Home
- Quickstart
- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Management

Device Info

Summary

Summary provides an overview of the operating parameters used in your device.

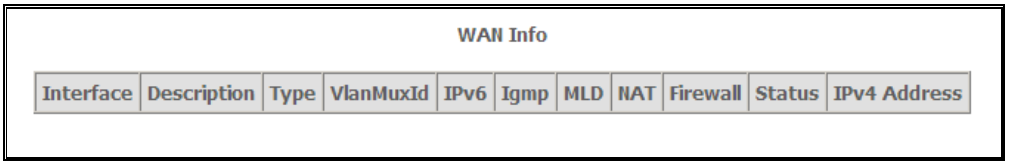


To view Summary:

1. Select Device Info.
2. Click Summary.

WAN

WAN displays a summary of the WAN connection settings.



To view WAN:

1. Select Device Info.
2. Click WAN.

Statistics

Statistical information is provided and displayed by LAN, WAN, ATM, and ADSL.

LAN

LAN displays a statistical summary of the data transaction for each interface.

To view LAN statistics:

1. Select Device Info.
2. Click Statistics > LAN.

WAN

LAN displays a statistical summary of the data transaction for each connection.

To view LAN statistics:

1. Select Device Info.
2. Click Statistics > WAN.

ATM

Asynchronous Transfer Mode (ATM) displays a statistical summary of the data transaction for the ATM interface.

To view ATM statistics:

1. Select Device Info.
2. Click Statistics > ATM.

ADSL

ADSL displays a statistical summary of the ADSL connection.

To view ADSL statistics:

1. Select Device Info.
2. Click Statistics > ADSL.

Route

Route displays the routing rules implemented in the router.

To view Route:

1. Select Device Info.
2. Click Router.

ARP

Address Resolution Protocol (ARP) displays the HW address of each IP device.

To view ARP:

1. Select Device Info.
2. Click ARP.

DHCP

DHSCP displays all the DHCP clients connected to the router.

To view DHCP:

1. Select Device Info.
2. Click DHCP.

Quick Setup

Quick Setup is used to establish an Internet connection.

To use Quick Setup:

1. Open your browser.
2. Enter 192.168.1.1 and then press Enter. This opens Connect to 192.168.1.1.
3. Enter the User name and Password, and then click OK. The default User name and Password is *admin*.
4. Select Quick Setup.

5. Enter the connection settings
    a. Select a Protocol
    b. Select an Encapsulation Mode
    c. Enter the PPP Username and Password
    d. Enter PVC Settings
    e. Check Enable Wireless
    f. Enter an SSID
6. Click Save/Reboot.

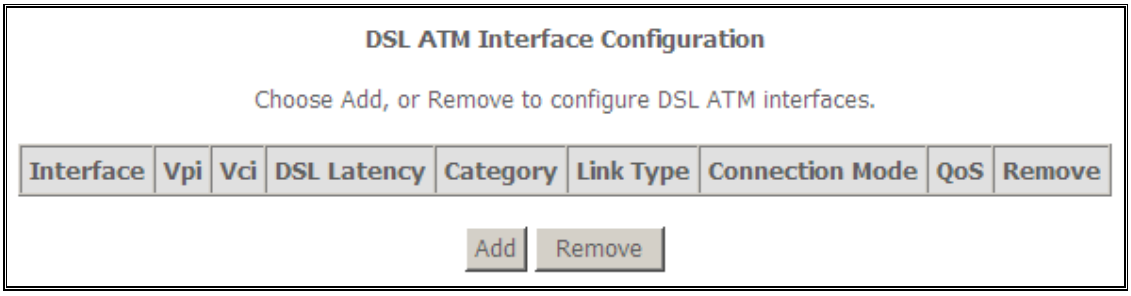
    The router will save your settings and reboot. It will connect to the Internet after the reboot. When the connection is established, the Internet LED on the router lights or blinks green.

Advanced Setup

Advanced Setup provides configuration options for other router functions.

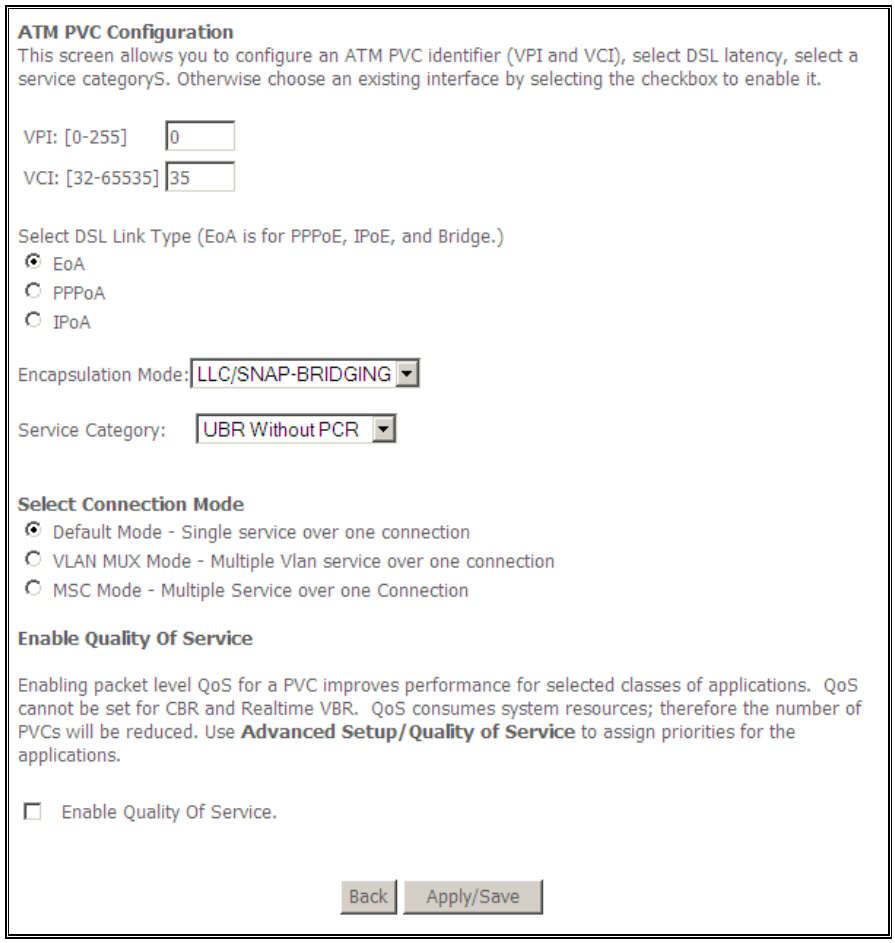
ATM Interface

ATM Interface allows you to add, edit, or remove ATM interface configurations.



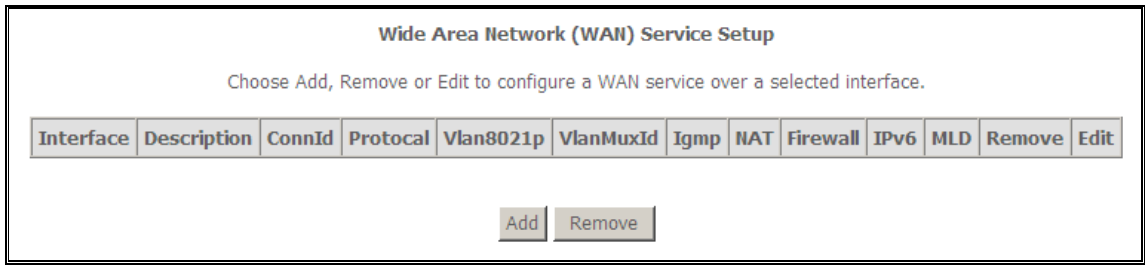
To create a new ATM interface configuration:

1. Select Advanced Setup.
2. Click Layer2 Interface
3. Click ATM Interface.
4. Click Add.
5. Enter the ATM interface settings:
    a. Enter the ATM PVC Configuration, QoS Setting, and then click Apply/Save.



WAN

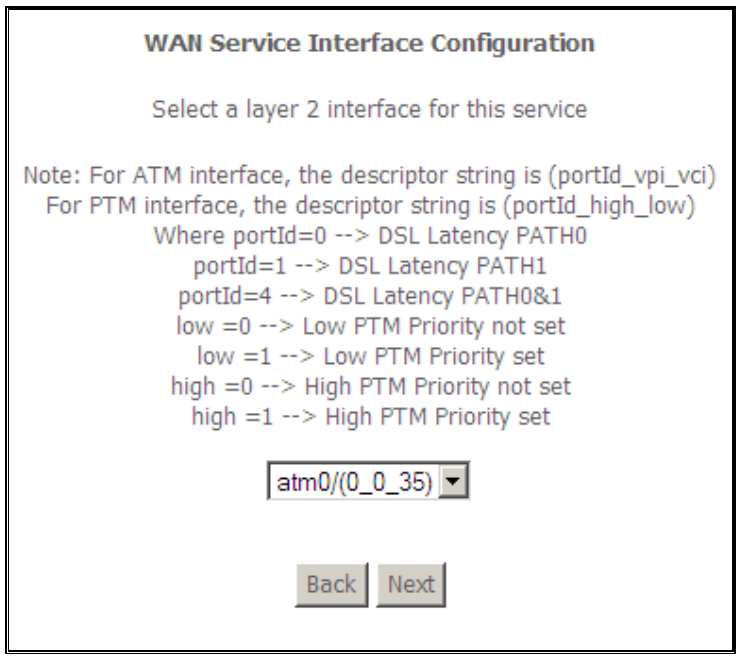
WAN allows you to add, edit, or remove WAN connections.



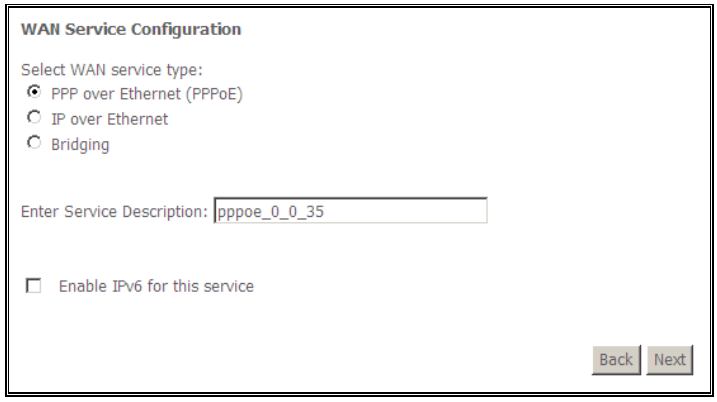
To create a new WAN connection:

1. Select Advanced Setup.
2. Click WAN.

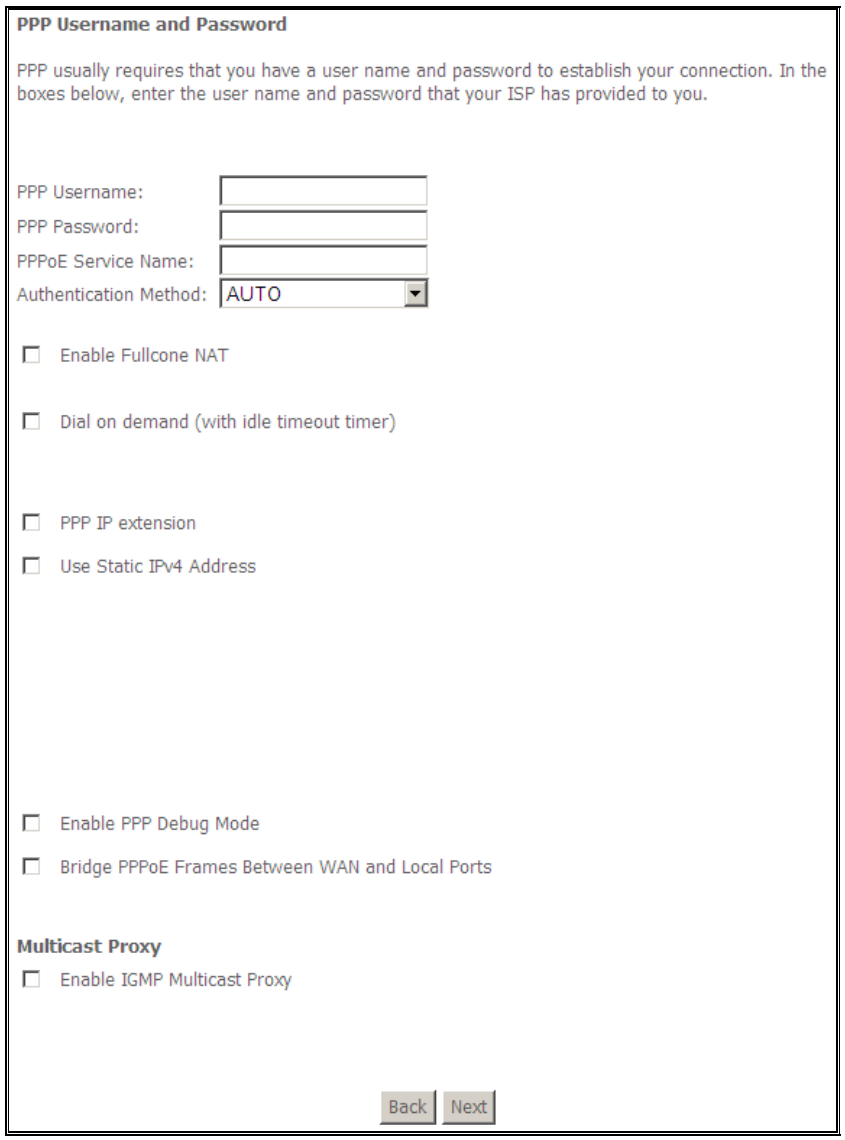
3. Click Add.
4. Enter the connection settings:
    a. Choose a layer 2 interface, and then click Next.



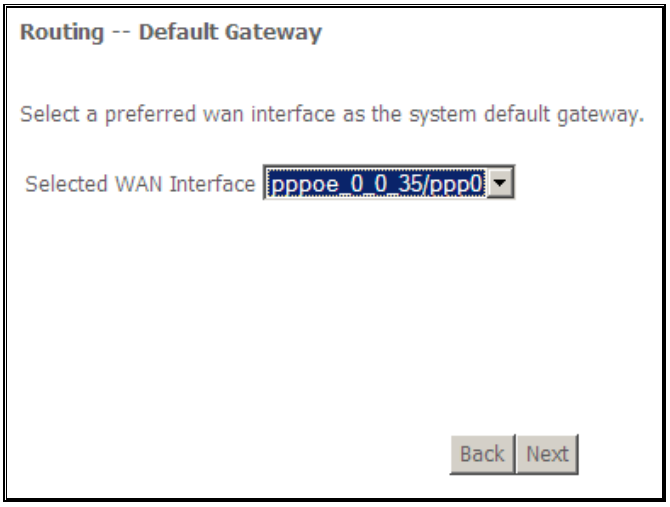
b. Select the WAN service type, and then click Next.



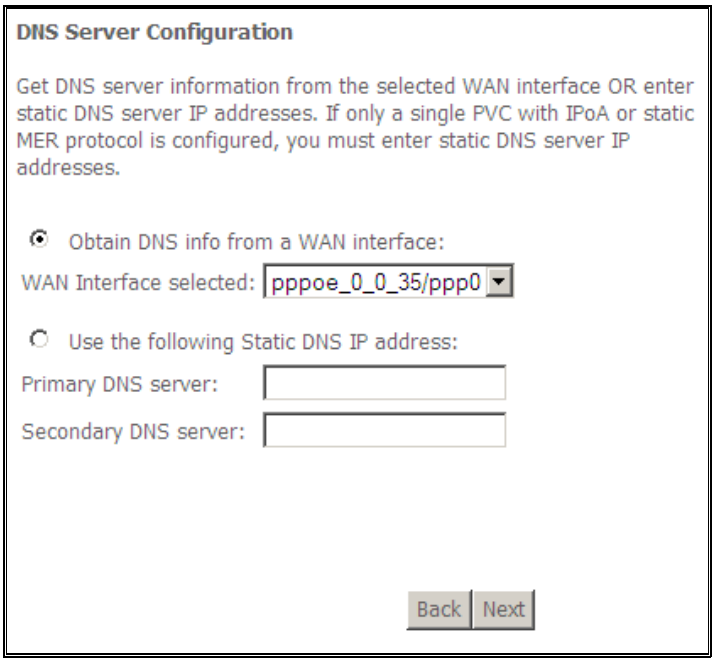
c. Key-in the PPP login information.



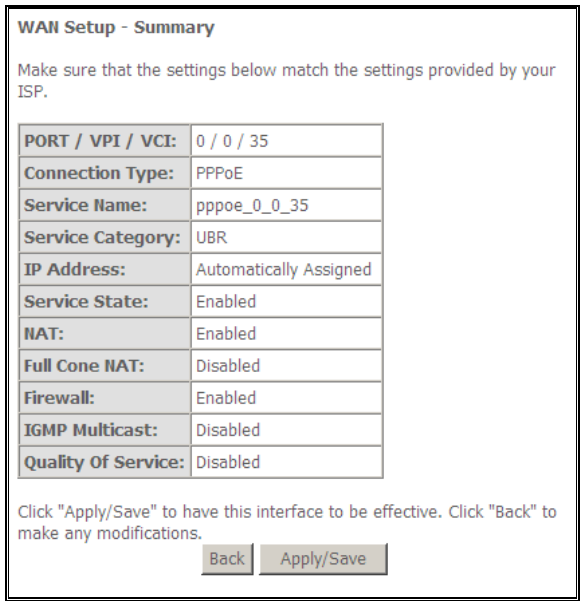
d. Select the wan interface as the system default gateway.



e. Configure the DSN server.



5. Click Apply/Save.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

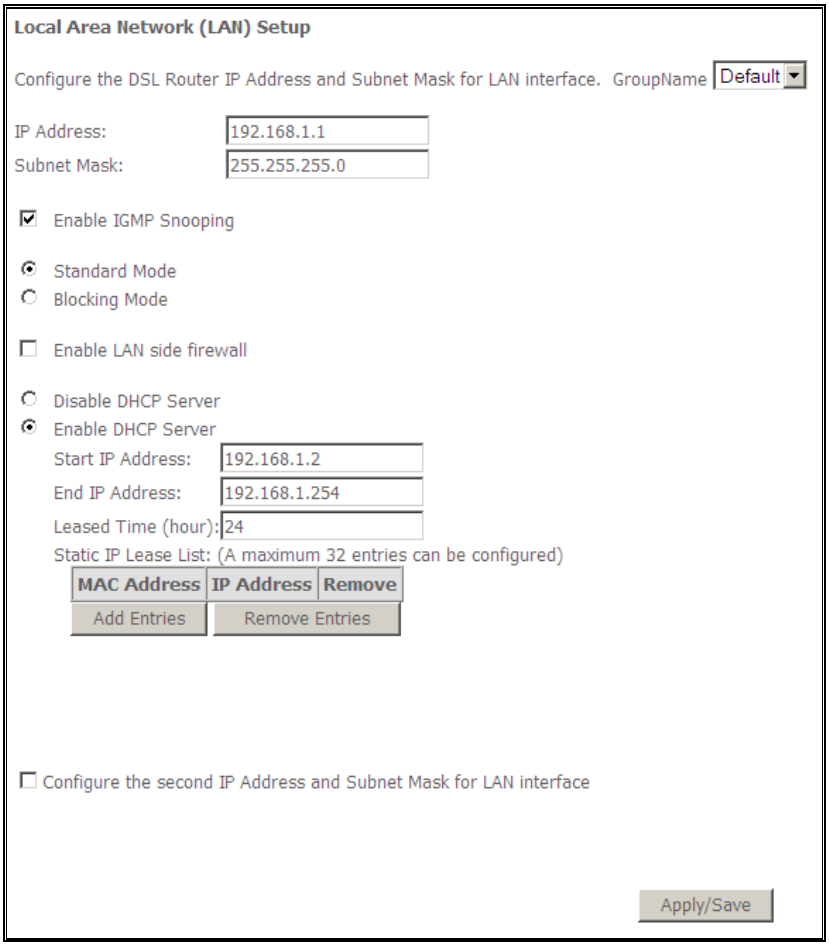
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

LAN

LAN allows you to modify the settings for your local network.

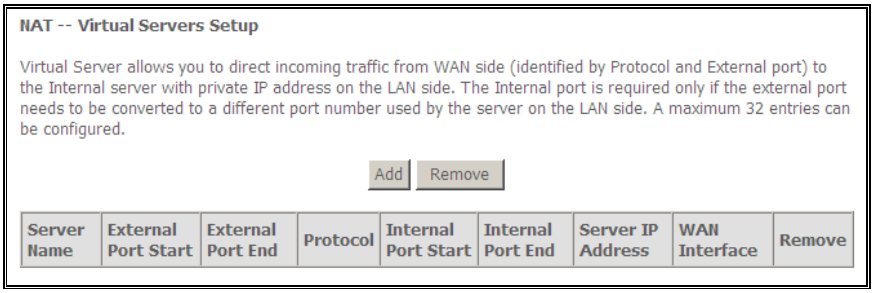


NAT

The routers NAT features include Virtual Servers, Port Triggering, and DMZ Host.

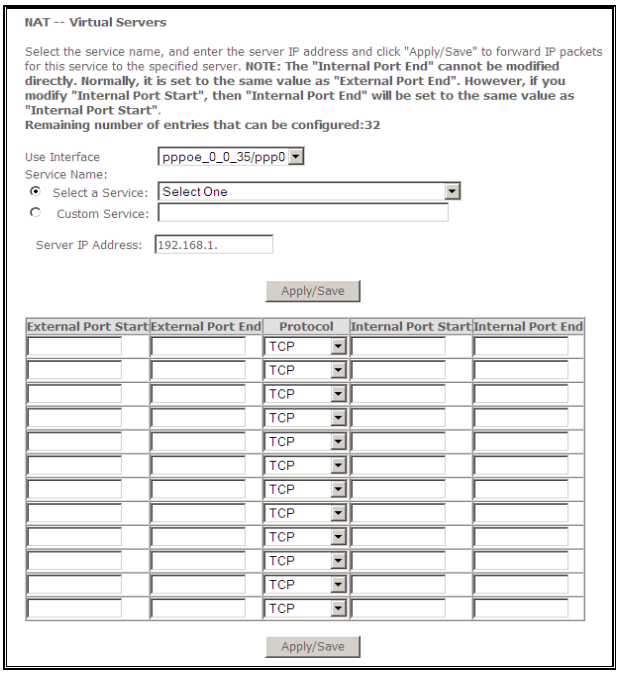
Virtual Servers

Virtual Server allows you to direct incoming traffic from the Internet to a specific computer in your local network. A maximum 32 entries can be configured.



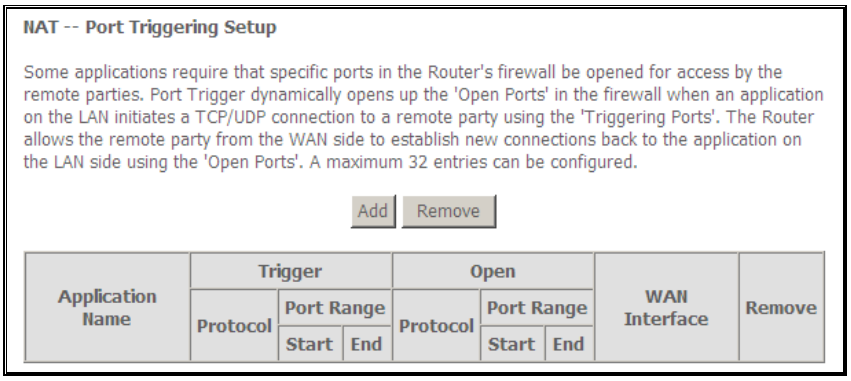
Click Add to create a Virtual Server.

As an example, to setup a web server on a computer using 192.168.1.88 as its IP Address, select HTTP as Service and enter 192.168.1.88 as the Server IP Address. Otherwise if the service you want to setup is not available from the Select a Service drop-down list, you can define your own Virtual Server.

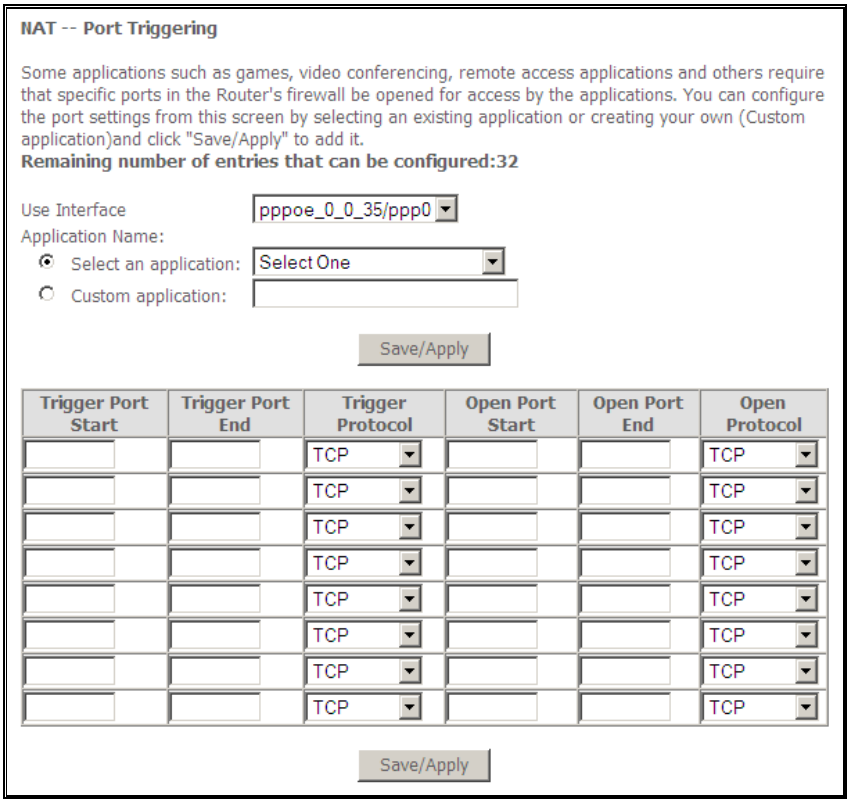


Port Triggering

Some applications require that the specific ports in the router's firewall be opened for access by the remote parties. For instance, an application uses port 25 for requests and port 113 for replies. If a computer on the LAN connects to port 25 on a remote server hosting this application, using Port Triggering on the router, incoming connections to port 113 (from the remote server) could be redirected to the PC which initiated the request. A maximum of 32 entries can be configured.



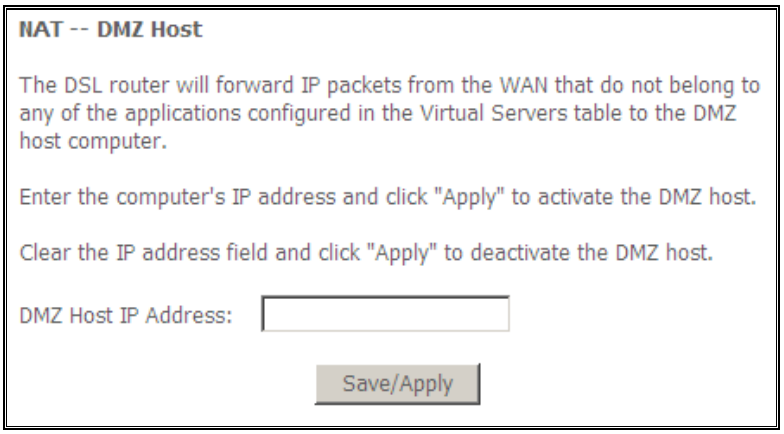
Click Add to setup Port Triggering.



DMZ Host

If a computer is assigned as a DMZ Host, it will receive all the data from the Internet that do not belong to the list of applications configured as a Virtual Server. Enter the LAN IP address of the PC you wish to set as DMZ Host in the DMZ Host IP Address. If you need to disable the DMZ Host, just clear the DMZ Host IP Address field, and then click Save/Apply.

Note: DMZ exposes your computer to the Internet and will be vulnerable to malicious attacks.



Security

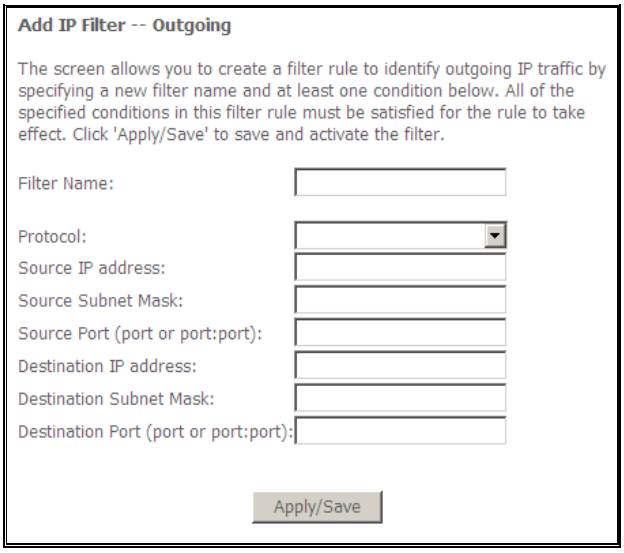
IP Filtering

The router supports IP Filtering, which allows you to easily set up rules to control incoming and outgoing Internet traffic. The router provides two types of IP filtering: Outgoing IP Filtering and Incoming IP Filtering.

Outgoing IP Filtering

By default, the router allows all outgoing Internet traffic from the LAN but by setting up Outgoing IP Filtering rules, you can block some users and/or applications from accessing the Internet.

To create a new outgoing IP filter, click Add. The Add IP Filter-Outgoing page will be displayed.



Key in the following parameters:

Filter Name Key in the name of the filter rule.

Protocol Select the IP protocol to block.

Source IP Address/Subnet Mask Enter the IP address of the PC on the LAN to block.

Source Port Enter the port number used by the application to block.

Destination IP Address/Subnet Mask Enter the IP address of the remote server to which connection should be blocked.

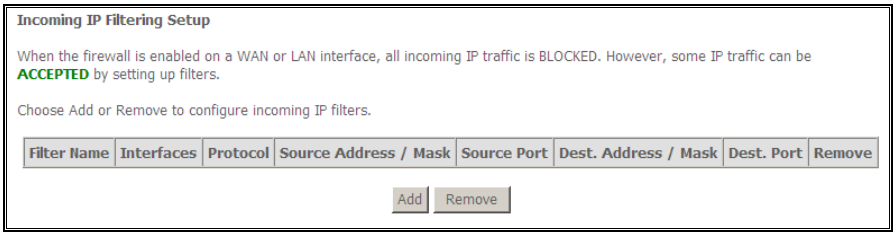
Destination Port Enter the destination port number used by the application to block.

Click Save/Apply to take effect the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

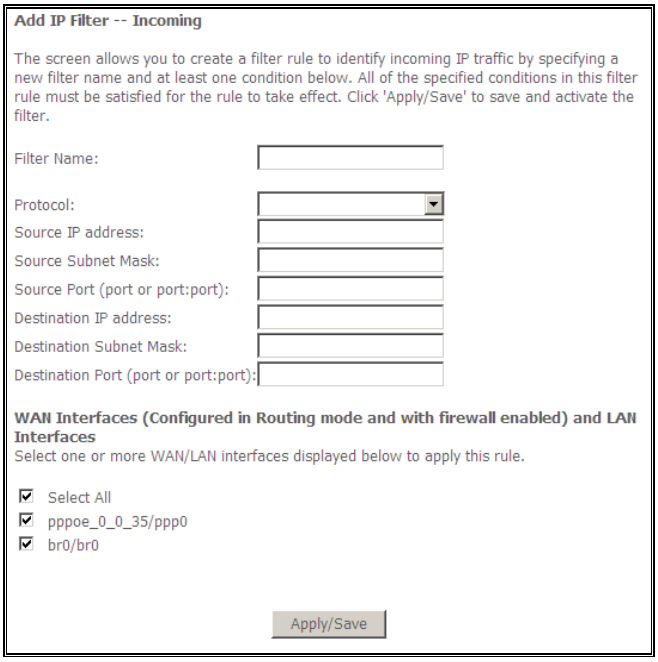
To delete the rule, click Remove checkbox next to the selected rule, and click Remove.

Incoming IP Filtering

By default, when NAT is enabled, all incoming IP traffic from WAN is blocked except for responses to requests from the LAN. However, some incoming traffic from the Internet can be accepted by setting up Incoming IP Filtering rules.



To create a new incoming IP filter, click Add. The Add IP Filter-Incoming page will be displayed.



Key in the following parameters:

Filter Name Key in the name of the filter rule.

Protocol Select the IP protocol to allow.

Source IP Address/Subnet Mask Enter the IP address of the remote server from which to allow connection.

Source Port Enter the port number used by the application to allow.

Destination IP Address/Subnet Mask Enter the IP address of the PC on the LAN to which connection is allowed.

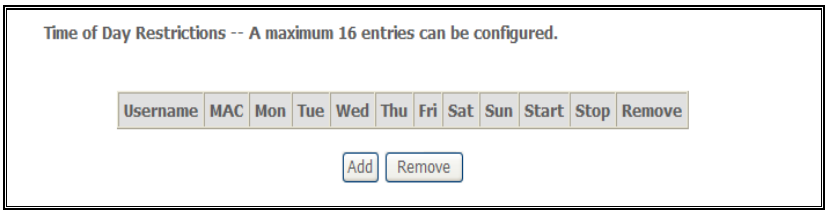
Destination Port Enter the destination port number used by the application to allow.

Click Save/Apply to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.

To delete the rule, click Remove checkbox next to the selected rule, and click Remove.

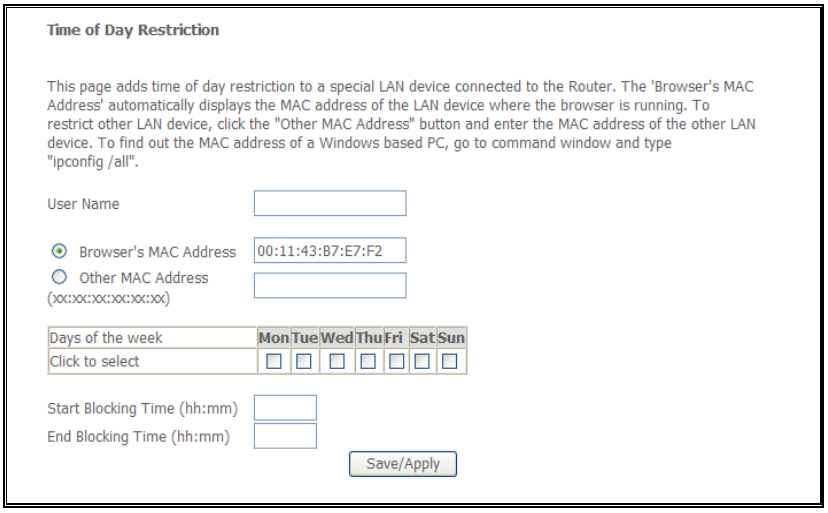
Parental Control

Parental Control allows you to apply router access restrictions among LAN devices within specific times in a day. A maximum of 16 restriction rules can be created.



To add restrictions, click Add. This opens the Time of Day Restriction page. Click Start to enable a restriction or click Stop to disable the rule.

To delete a restriction, click Remove checkbox next to the selected restriction, and click Remove.



Key in the following parameters:

User Name Enter a descriptive name for the restriction.

Browser's MAC Address or Other MAC Address Enter the device MAC Address.

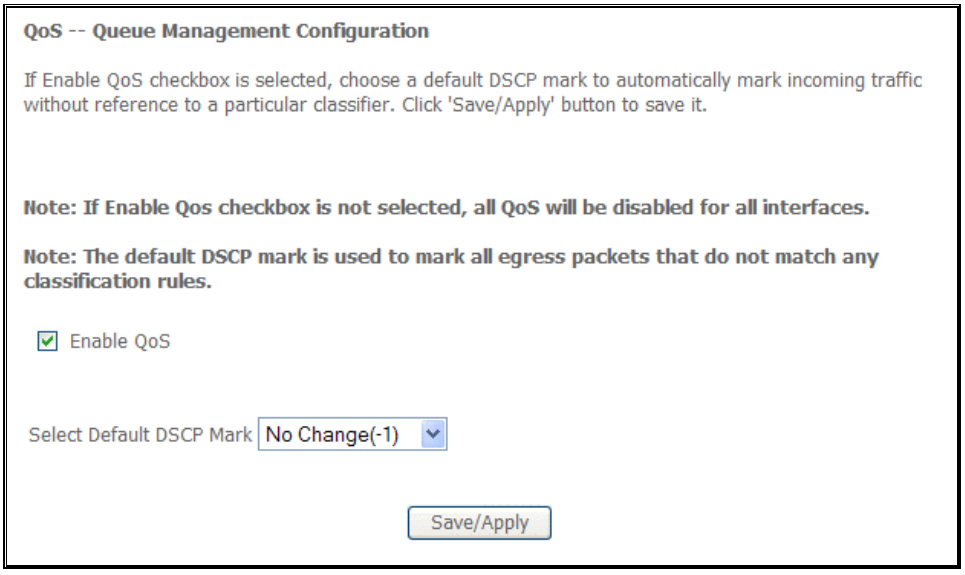
Days of the week Click to select the days on which to apply the restriction.

Start Blocking Time (hh:mm) Enter the time when the restriction will be enabled (00:00 to 23:59).

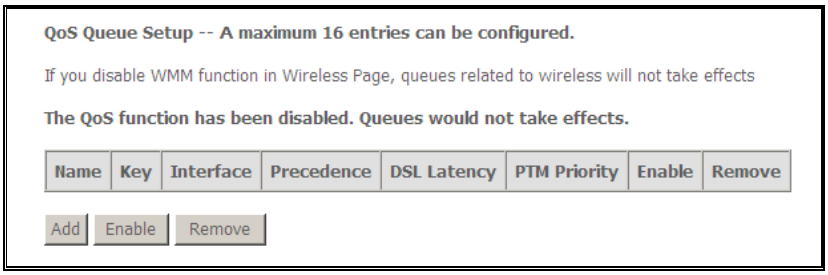
End Blocking Time (hh:mm) Enter the time when the restriction will be disabled (00:00 to 23:59).

Quality of Service

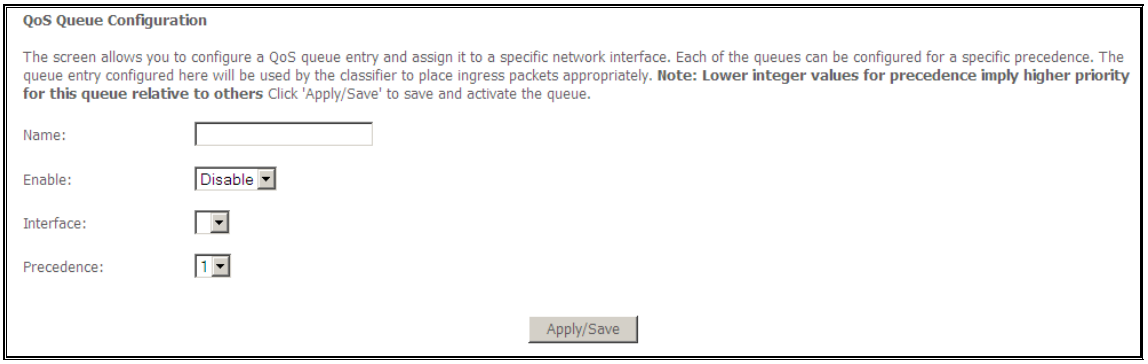
QoS gives you the capability to specify the level of quality to be provided for specific applications. By default, QoS is not enabled.



Queue Config

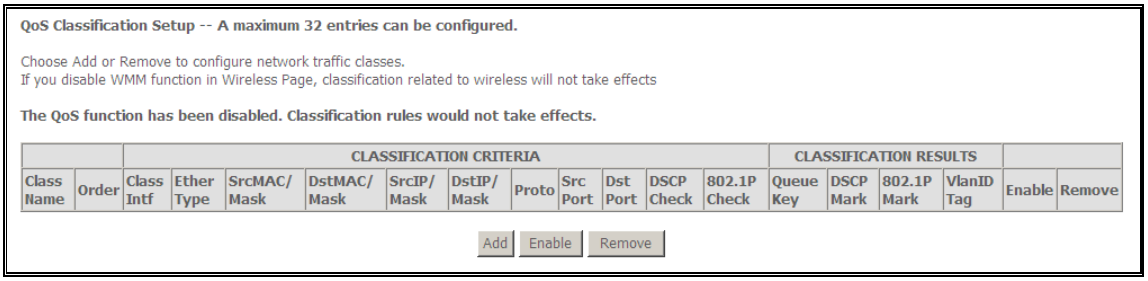


Click Add to create a QoS Queue Configuration.



QoS Classification

You can add or remove QoS Classification rules.



QoS Classification Setup -- A maximum 32 entries can be configured.

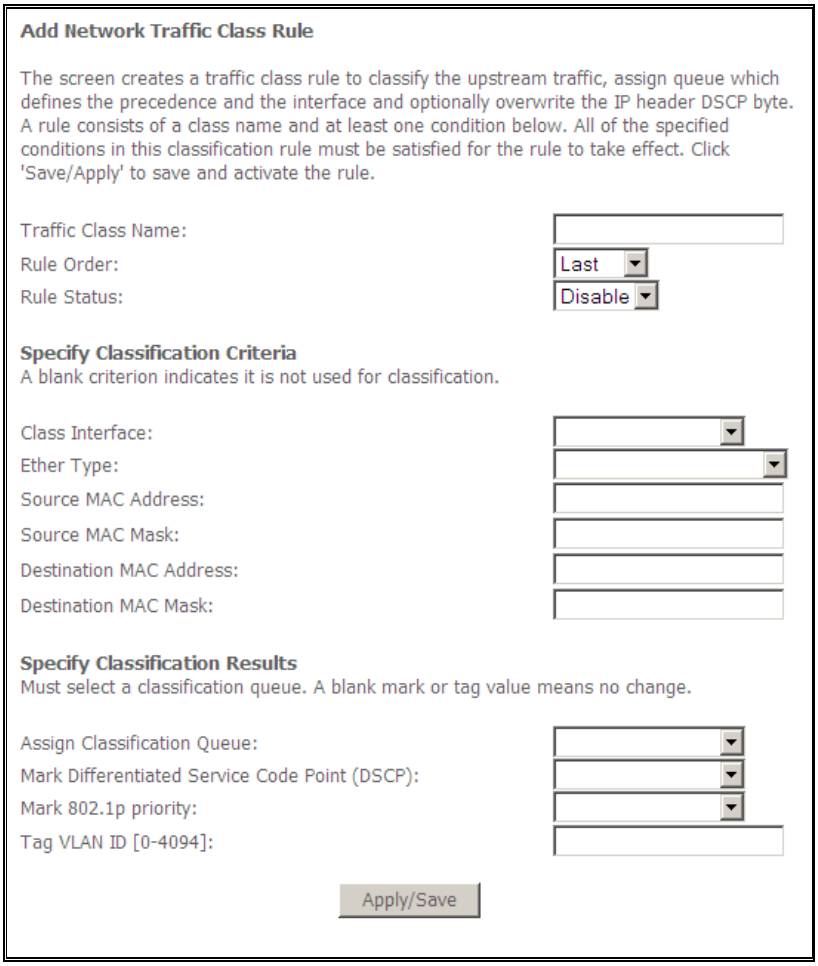
Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove

Add Enable Remove

Click Add to create a Network Traffic Class Rule.



Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:
Rule Order: Last
Rule Status: Disable

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface:
Ether Type:
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

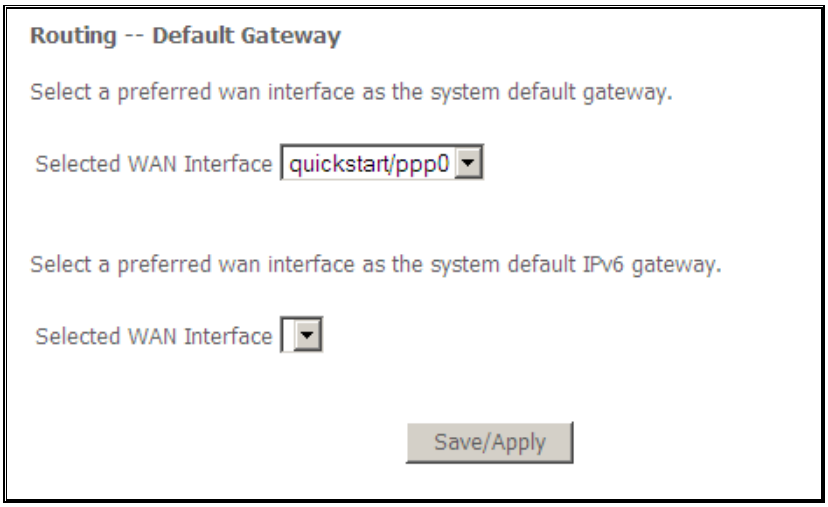
Assign Classification Queue:
Mark Differentiated Service Code Point (DSCP):
Mark 802.1p priority:
Tag VLAN ID [0-4094]:

Apply/Save

Routing

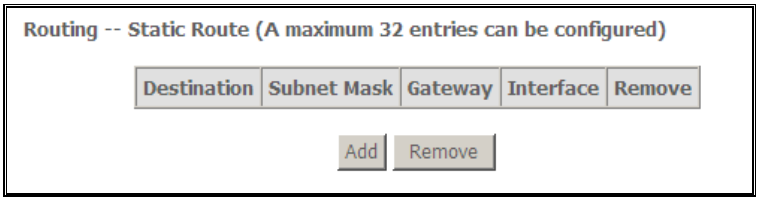
Default Gateway

The Enable Automatic Assigned Default Gateway checkbox is ticked by default. The router will accept the first received Default Gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s).

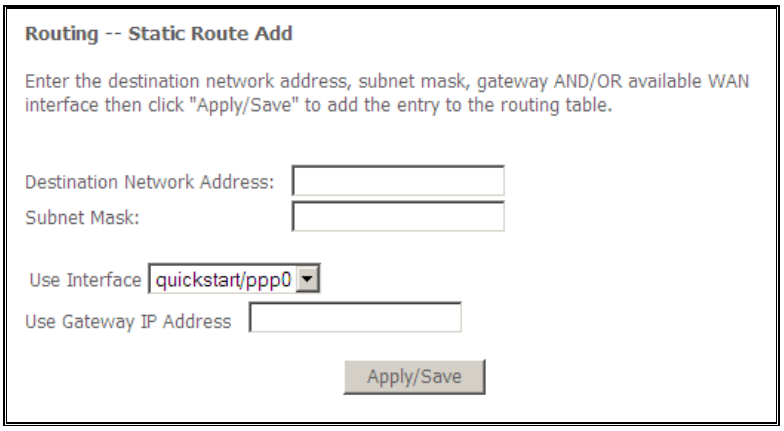


Static Route

If your LAN consists of multiple subnets and you want to manually define the data transmitting paths, Static Route is to be used.



To create a new Static Route, click Add. The Routing-Static Route Add page will shows up.



The key settings for adding a new Static Route are explained:

Destination Network Address Enter the network address to which the data packets are to be sent.

Subnet Mask Enter the subnet mask for this destination.

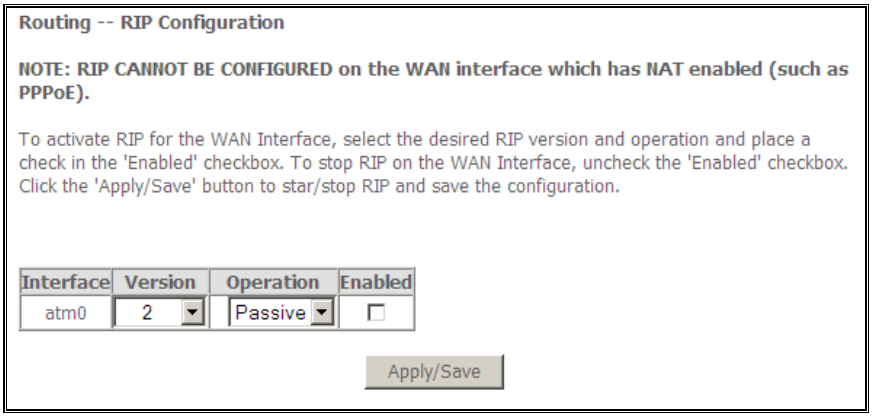
Use Gateway IP Address If you wish to use a specific gateway to reach the destination network, select this checkbox and then enter the IP address of the gateway.

Use Interface If you wish to use a particular WAN interface, select the checkbox and select the interface.

Click Save/Apply to take effect the settings.

To delete the entry from the routing table list, click its corresponding Remove button.

RIP



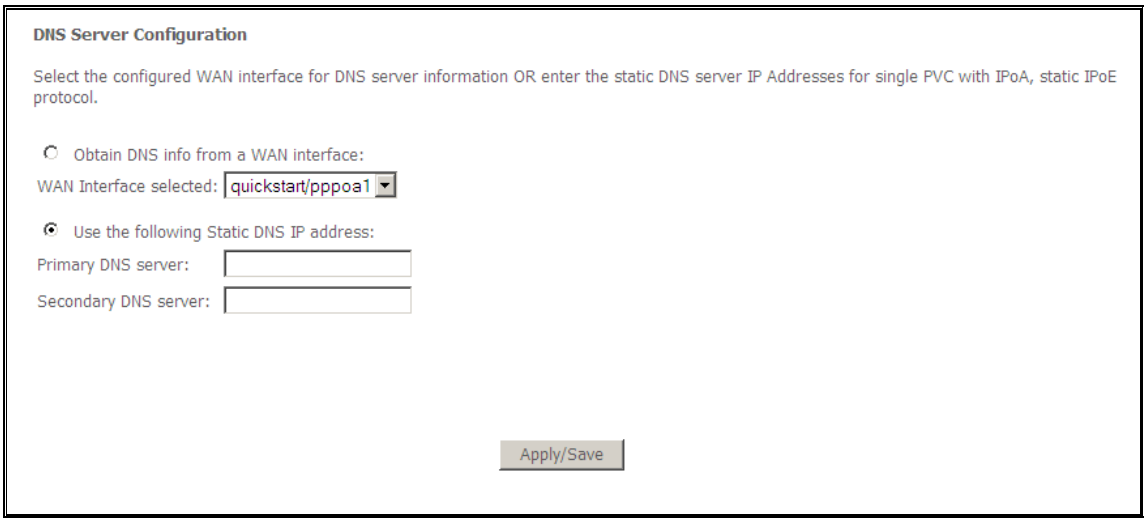
DNS

DNS Server

DNS (Domain Name System) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Therefore, each time you type a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system consists of a network of DNS servers. If one DNS server does not know how to translate a particular domain name, it asks another one and so on until the correct IP address is returned.

If you select the Enable Automatic Assigned DNS checkbox, the router will receive and use the DNS Server assigned by your ISP.

To use your preferred DNS servers, disable the Enable Automatic Assigned DNS checkbox and key in the IP address of your Primary DSN server. Adding a Secondary DNS server is optional.



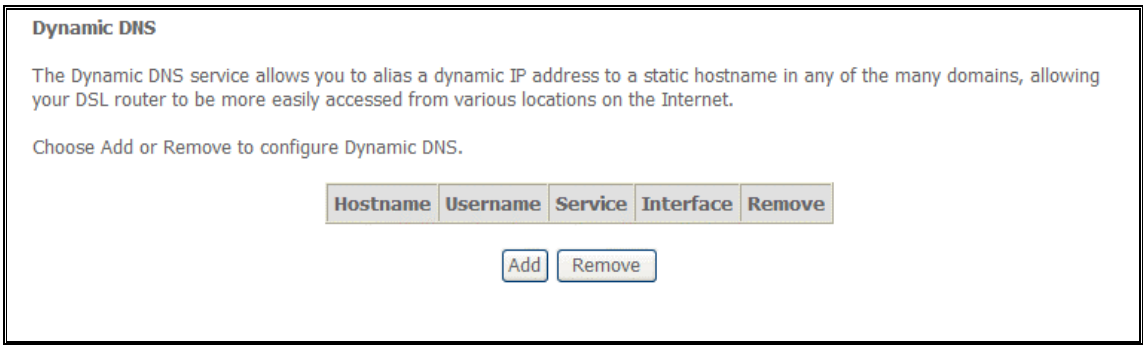
Dynamic DNS

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router.

Before using this feature, you need to sign up for DDNS service providers. The router supports these popular Dynamic DNS service providers:

- www.dyndns.org
- www.tzo.com

Click Add to create a Dynamic DNS setting.



Using DynDNS.org

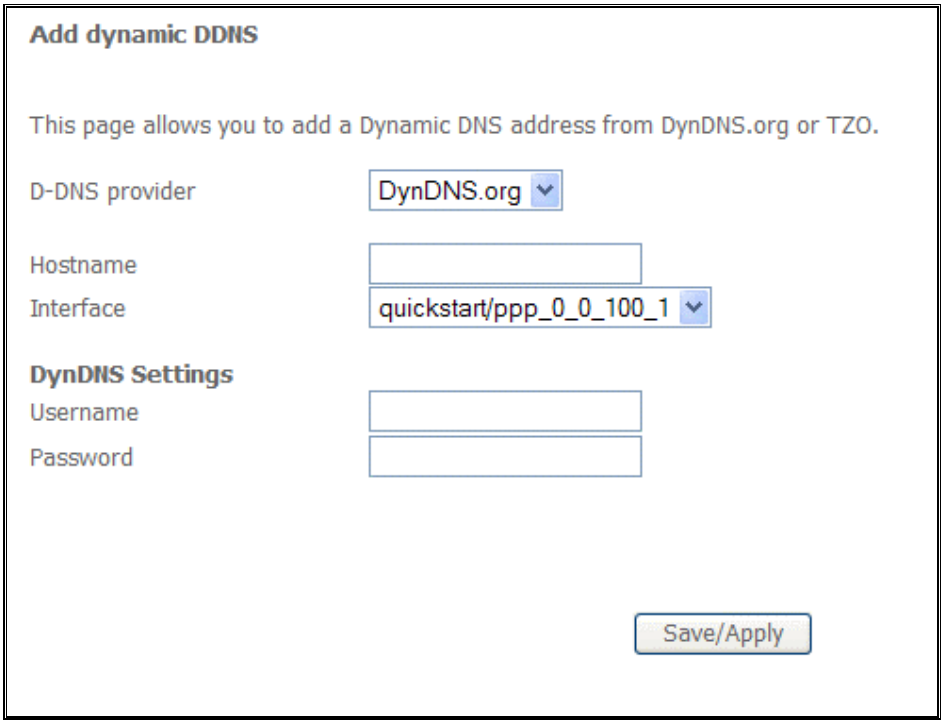
Key in the following parameters:

D-DNS provider Select DynDNS.org.

Hostname Enter the hostname.

Interface Select an interface.

DynDNS Settings Enter your dyndns.org Username and password.



Using TZO

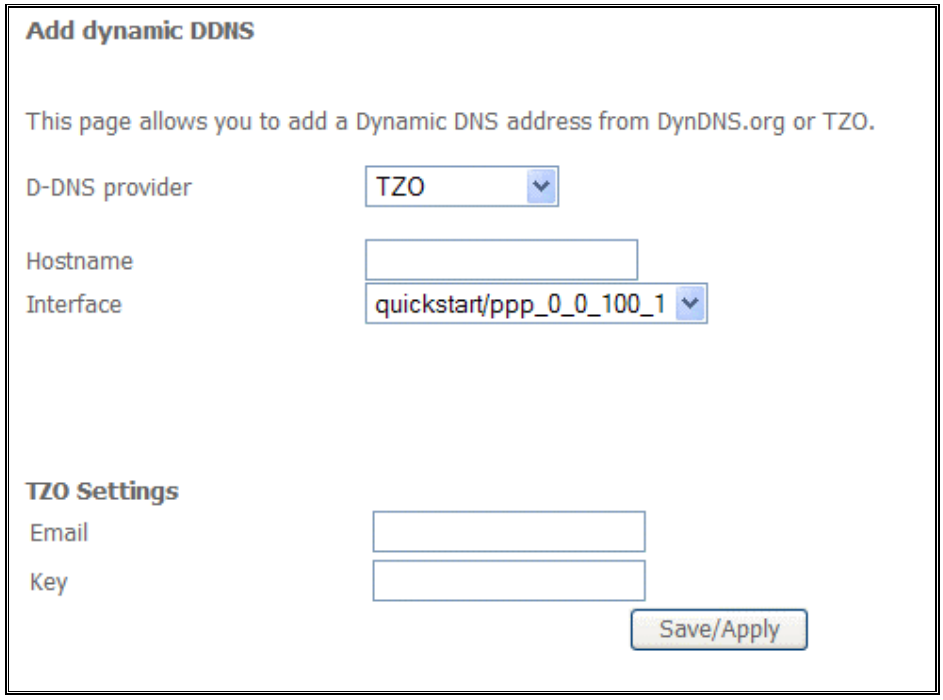
Key in the following parameters:

D-DNS provider Select TZO.

Hostname Enter the hostname.

Interface Select an interface.

TZO Settings Enter your TZO e-mail and key.

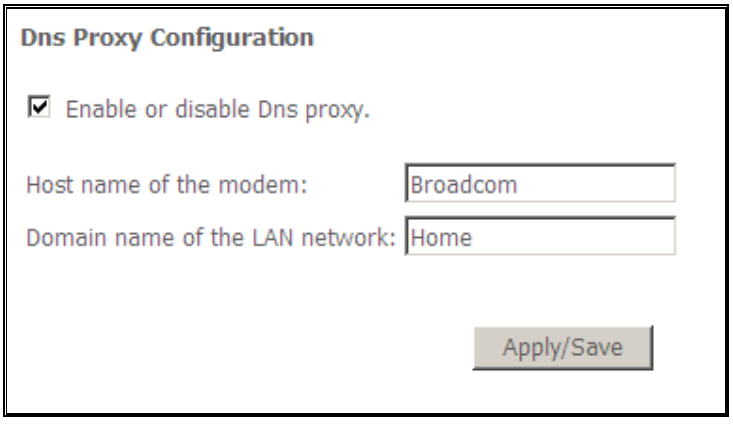


DSL

The DSL page allows you to select the modulation, the phone line pair and the capability.

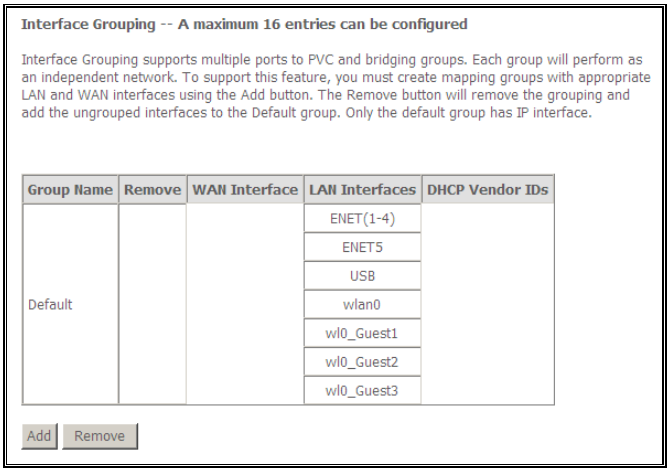
DNS Proxy Configuration

The DNS Proxy Configuration page allows you to enable and specify a DNS proxy name.

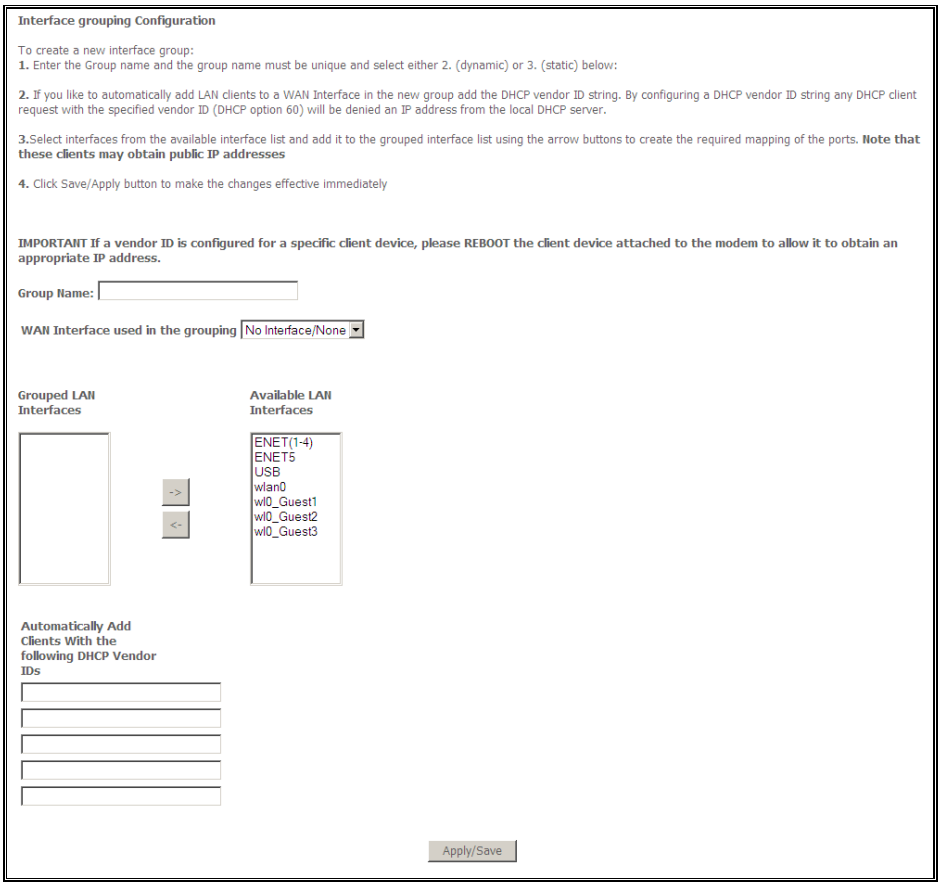


Interface Grouping

Interface Grouping allows you to create groups composed of the various interfaces available in your router.

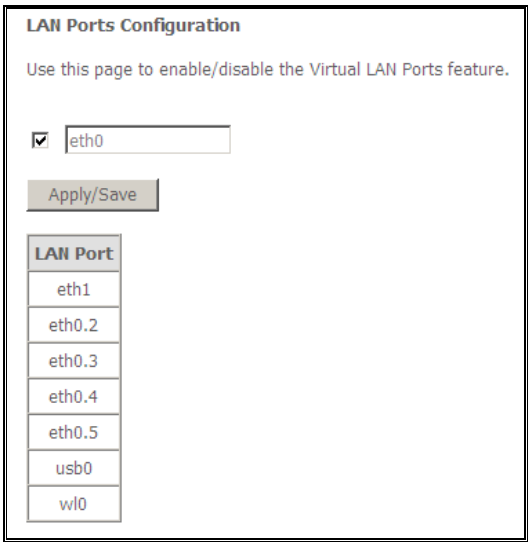


Click Add to create an Interface grouping.



LAN Ports

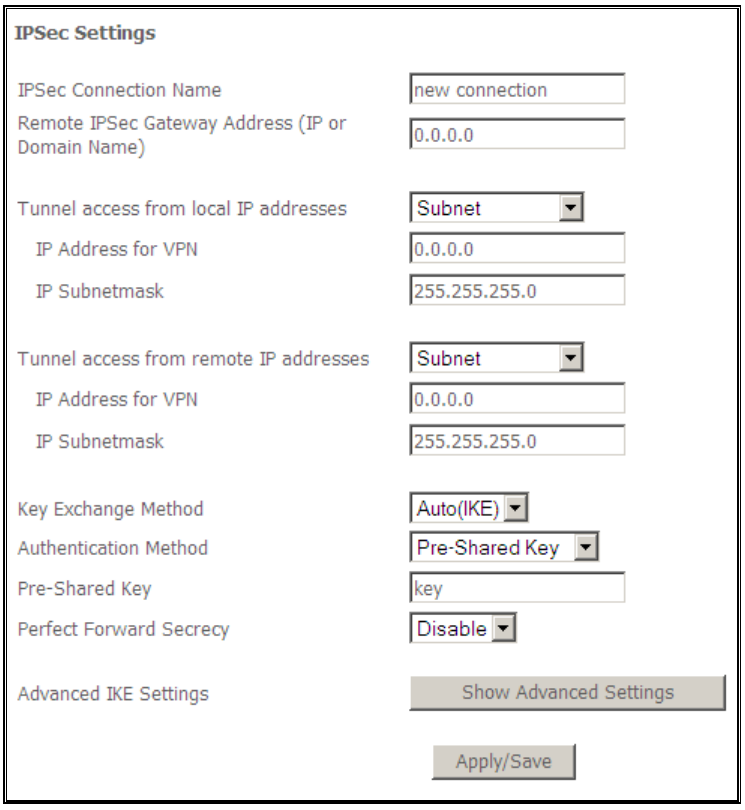
LAN Ports allow you to enable/disable the virtual LAN ports feature on your router.



IPSec

Your router supports the authentication and encryption of data packets.

Click Add New Connection to create an IPSec Setting.

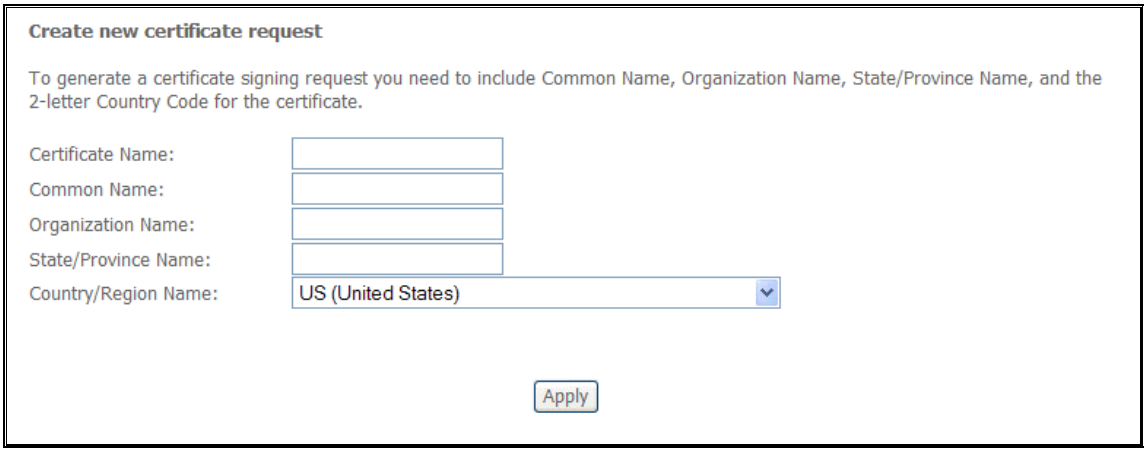

IPSec Settings
IPSec Connection Name
new connection
Remote IPSec Gateway Address (IP or Domain Name)
0.0.0.0
Tunnel access from local IP addresses
Subnet
IP Address for VPN
0.0.0.0
IP Subnetmask
255.255.255.0
Tunnel access from remote IP addresses
Subnet
IP Address for VPN
0.0.0.0
IP Subnetmask
255.255.255.0
Key Exchange Method
Auto(IKE)
Authentication Method
Pre-Shared Key
Pre-Shared Key
key
Perfect Forward Secrecy
Disable
Advanced IKE Settings
Show Advanced Settings
Apply/Save

Certificate

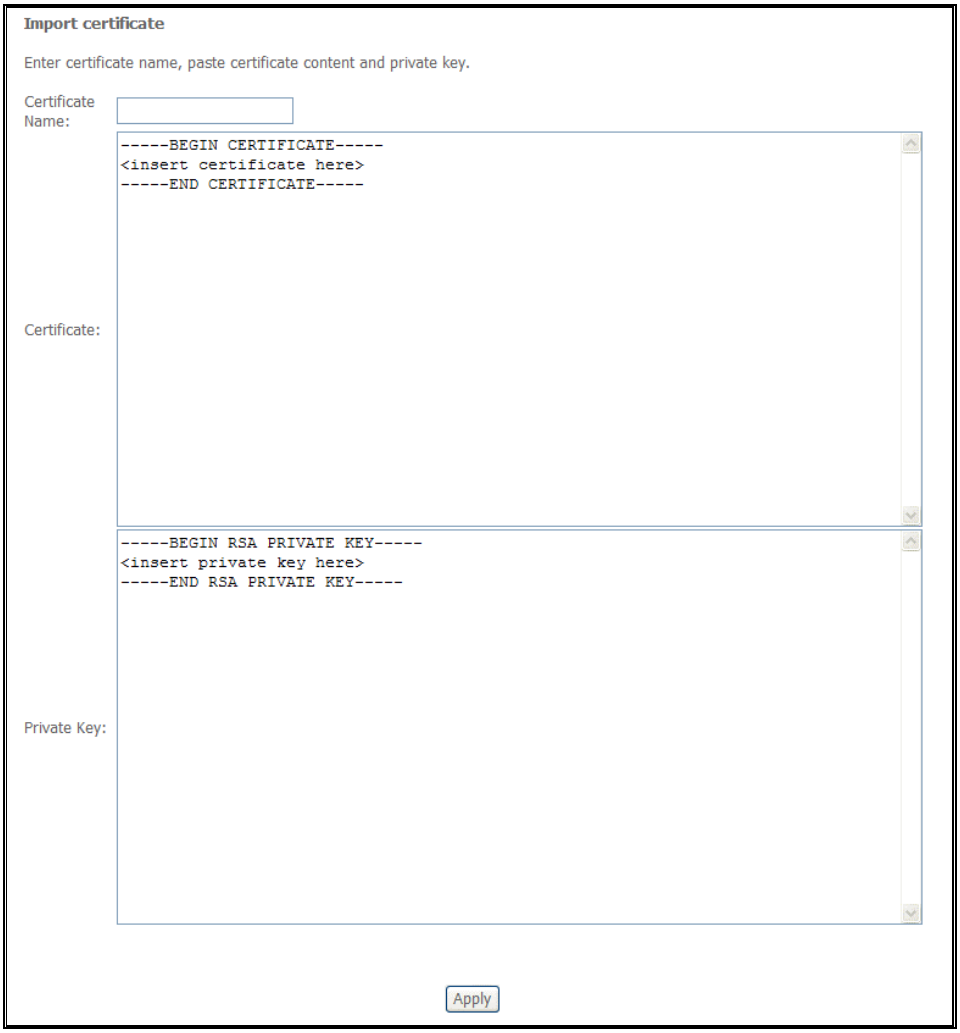
Certificates are used to verify the identity of you and your peers. You can either create or import a Certificate Request.

Local

Create Certificate Request

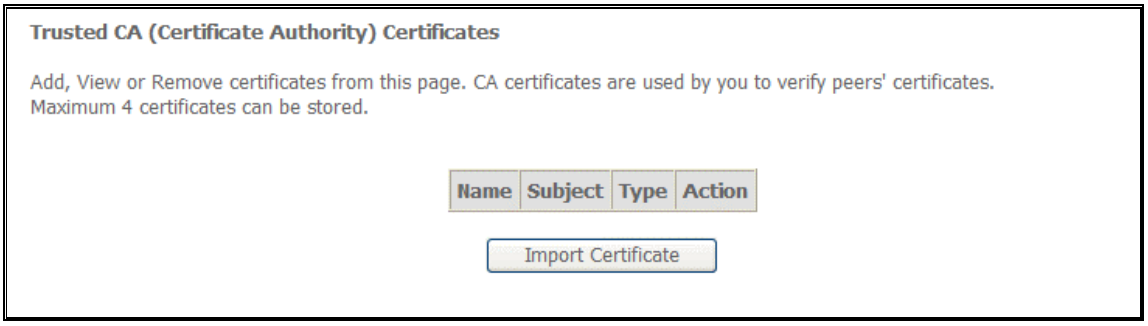


Import Certificate

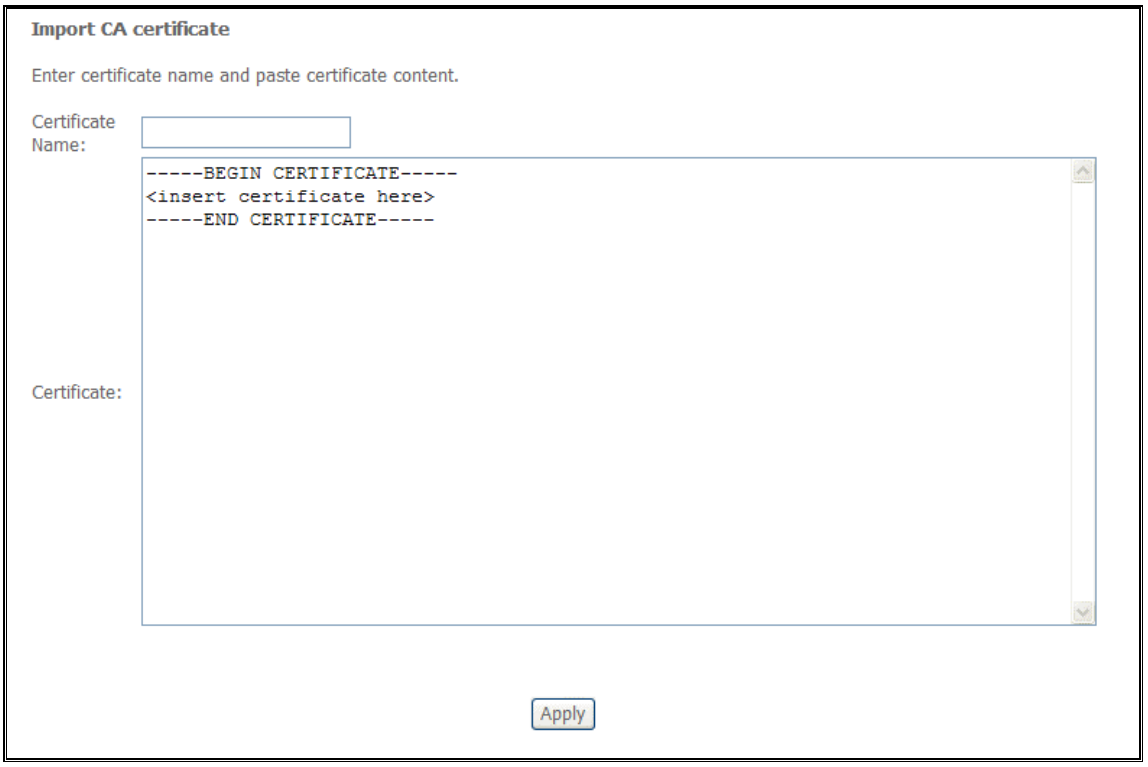


Trusted CA

Trusted CA is used to verify the certificate of your peers.



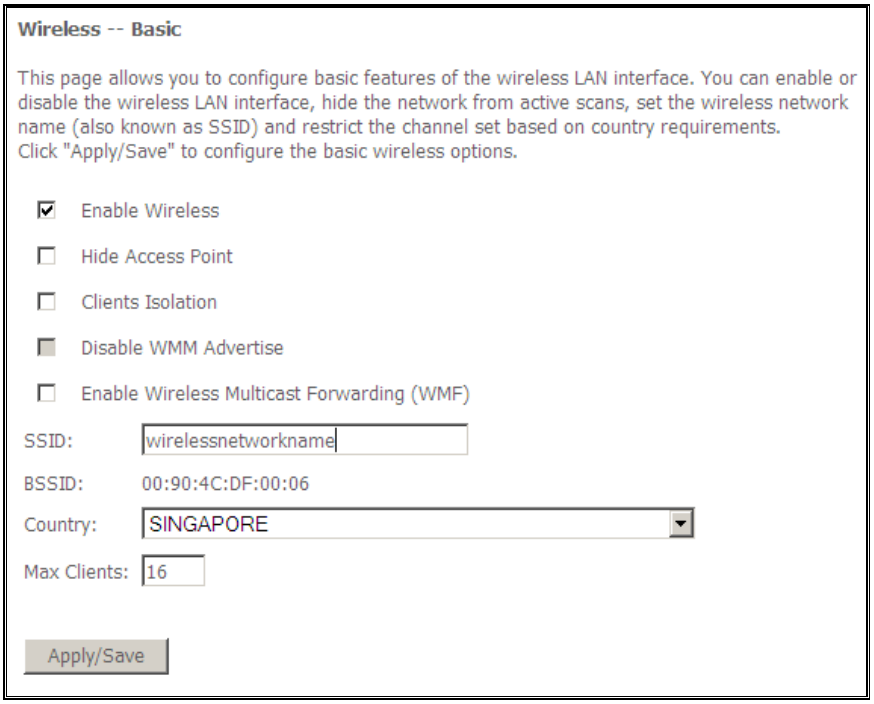
Click Import Certificate.



Wireless

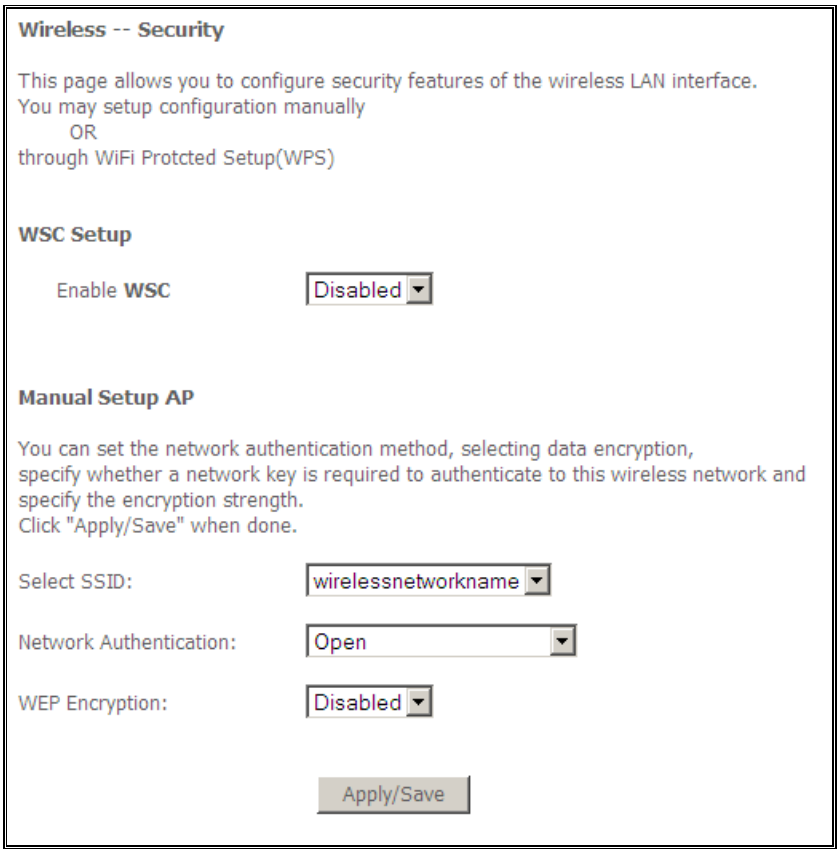
Basic

The Wireless Basic page allows you to enable the wireless network and configure its basic settings.



Security

The router supports all the popular wireless security protocols.



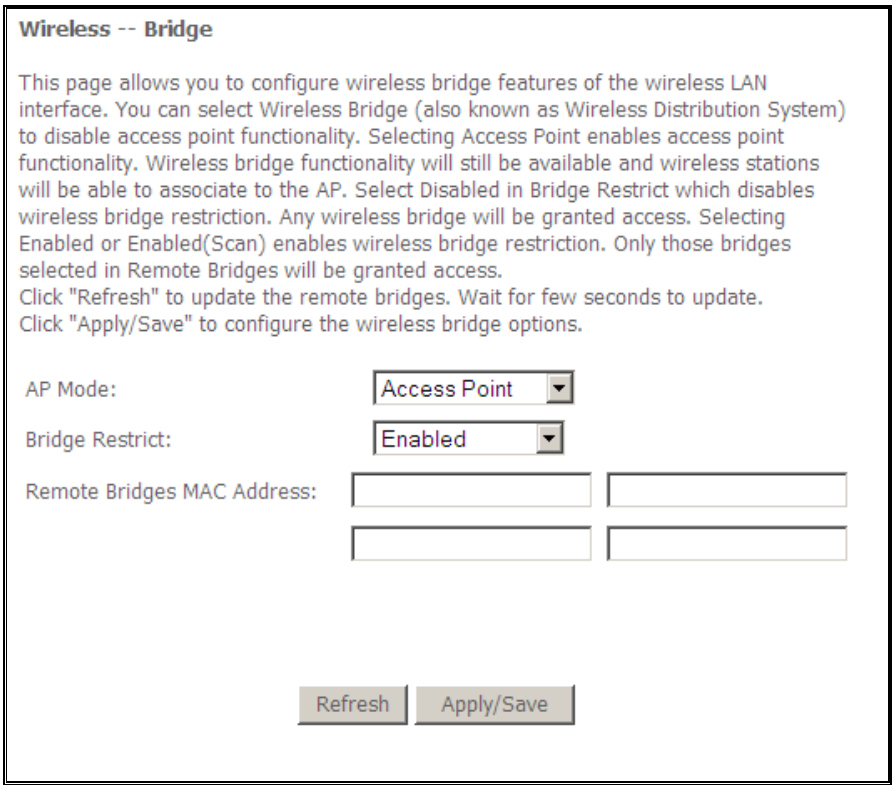
MAC Filter

MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network.

Click Add to add a MAC Address.

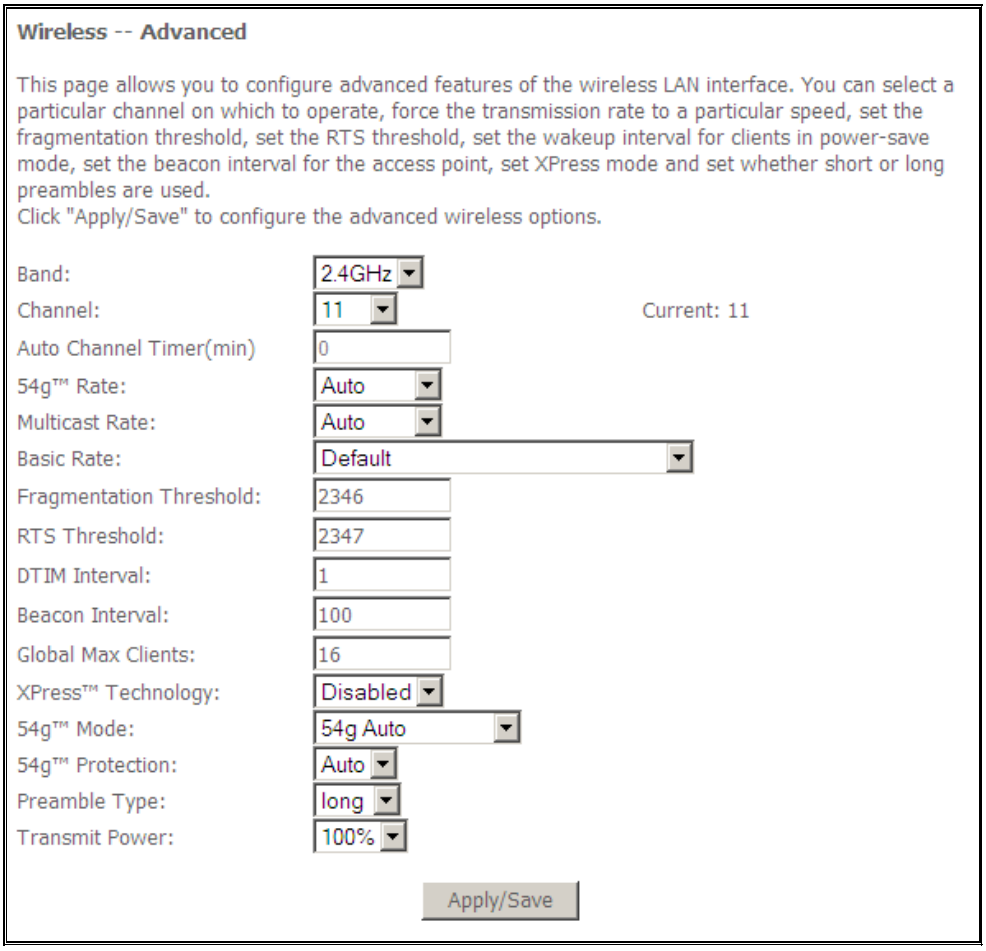
Wireless Bridge

Wireless Bridge allows you to configure the router's access point as a bridge.



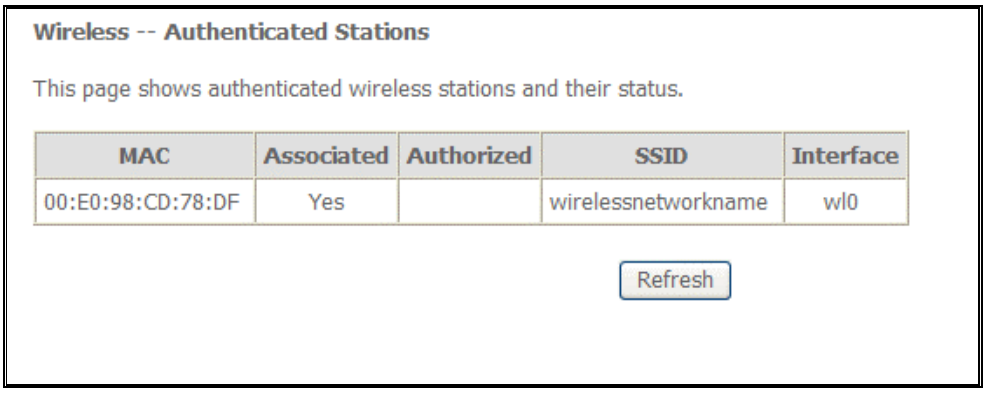
Advanced

Advanced Wireless allows you to configure detailed wireless settings.



Station Info

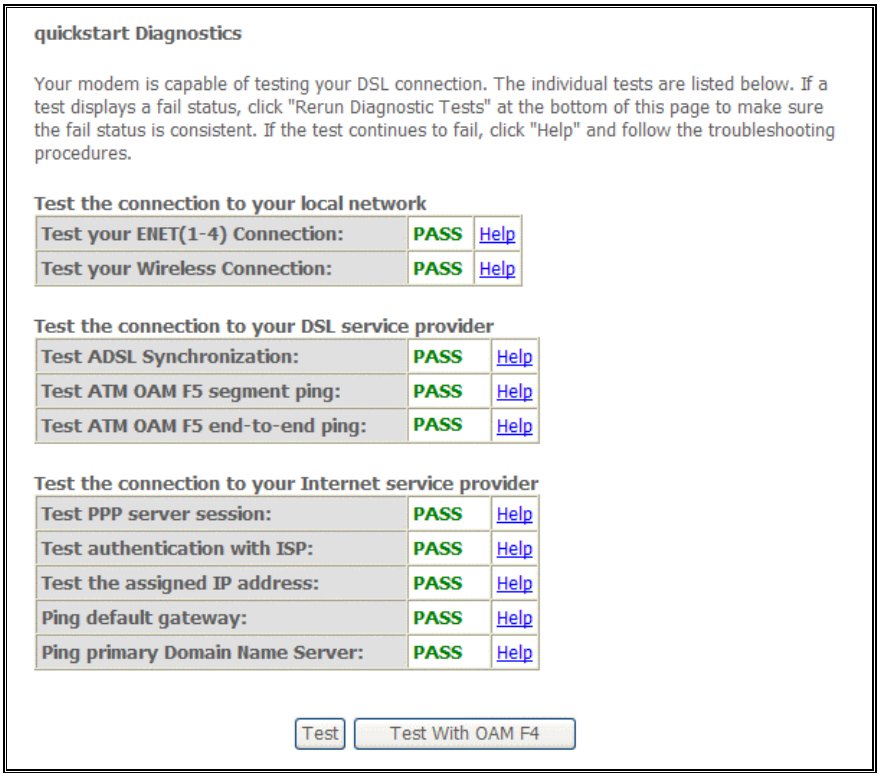
Station Info scans wireless stations and displays their status.



Diagnostics

The router has a diagnostic feature to test your DSL connection. You can use the diagnostic menu to perform the following test functions from the router.

- Testing the connection to your local network
- Testing the connection to your DSL service provider.
- Testing the connection to your Internet service provider.



Management

Settings

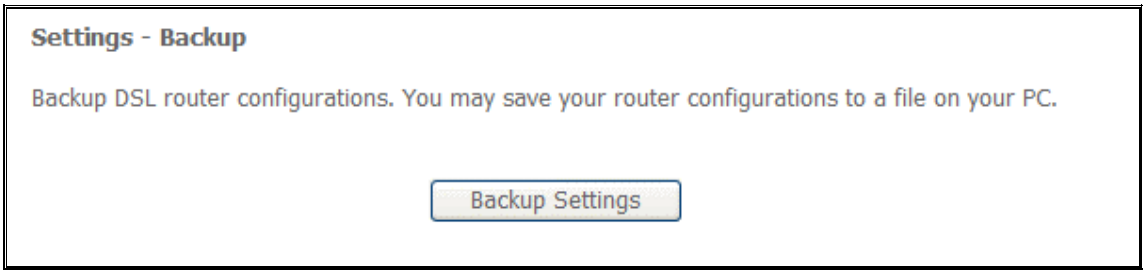
When it comes to managing the settings that you have executed to the router, you can choose to:

- Backup the settings as a configuration file stored onto your PC
- Update the current settings from a previously saved configuration file
- Erase the current settings and restore the default factory values

Backup

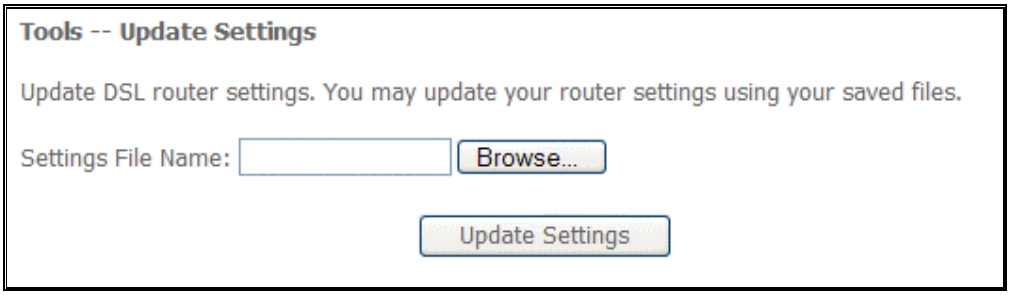
To backup the settings as a configuration file saved on your PC, click Backup Settings.

Select the folder where you want to save the file and key in the file name under which you want to save the settings.



Update

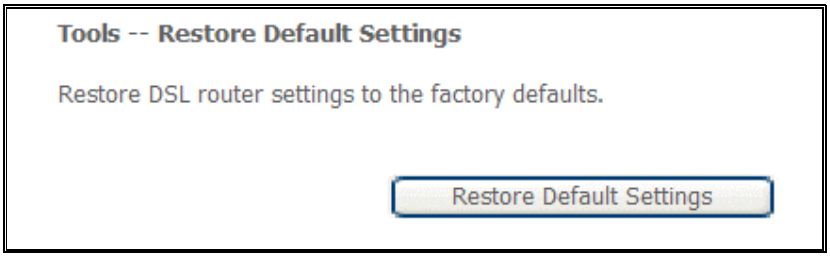
To import a previously saved configuration file from your PC and update the settings of your router, click Browse to locate the binary (.BIN or .IMG) upgrade file. Then click Update Settings.



Restore Default

To restore your router to its factory default settings, click Restore Default Settings. When prompted, click OK.

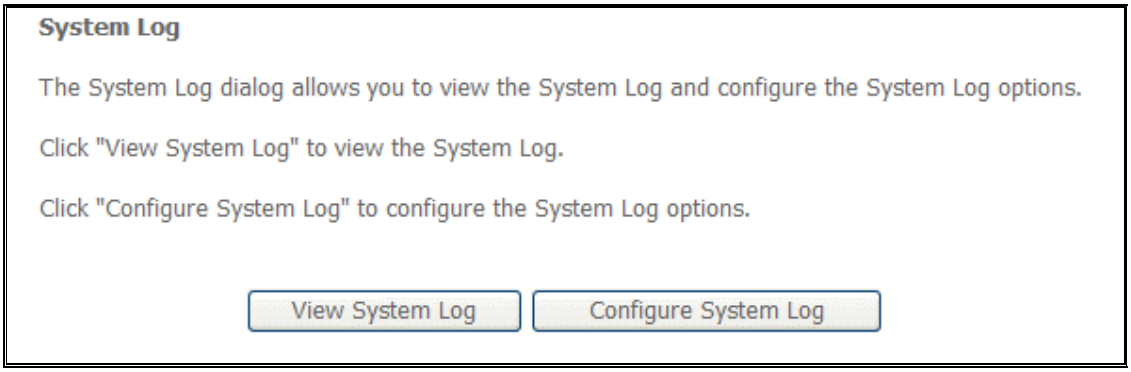
Upon clicking OK, you will be prompted to follow the instruction as shown below.



System Log

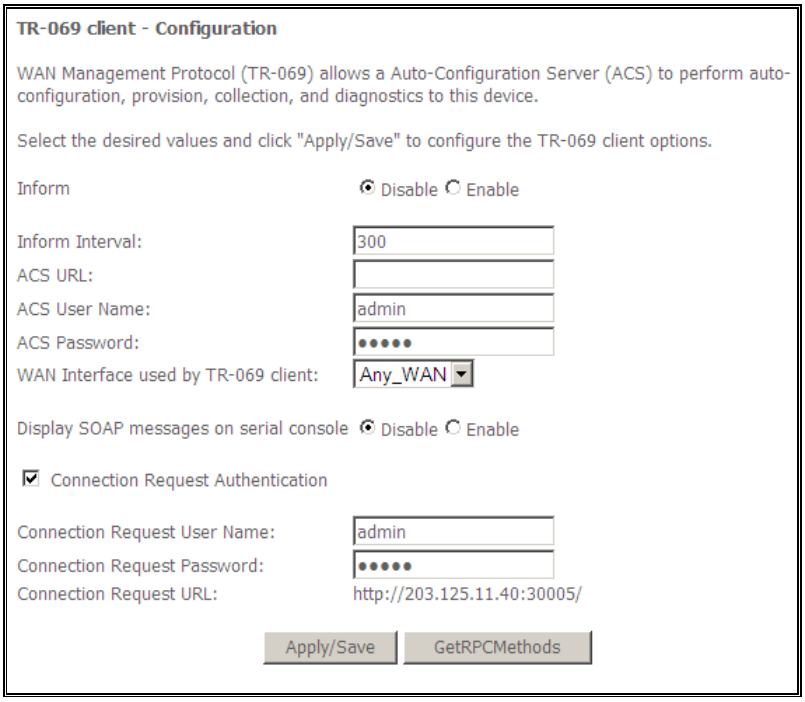
This feature provides you a comprehensive list of log entries reporting events which you have configured for viewing.

To view the log, click View System Log.



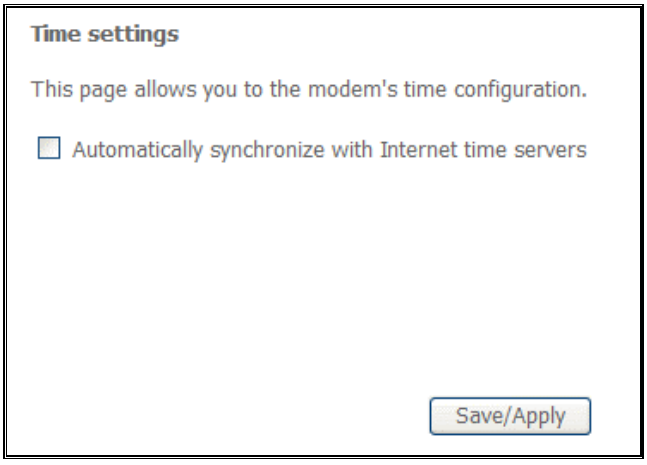
TR-069 Client

As a TR-069 capable router, the Internet service provider can remotely update the settings of the device.



Internet Time

Enable Internet Time to automatically synchronize your time with a time server.

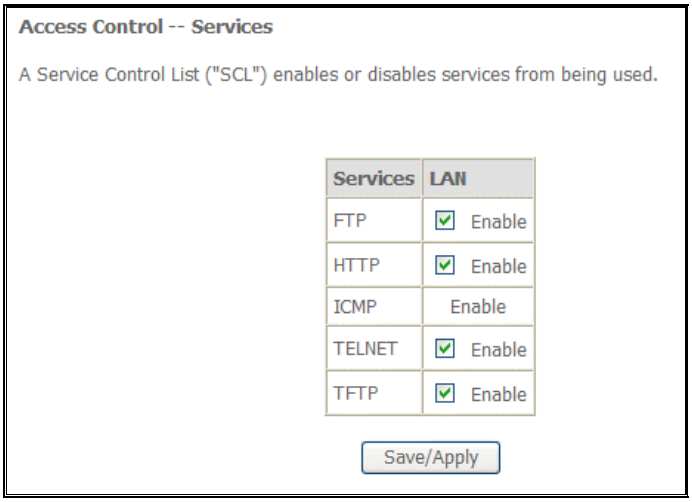


Access Control

This feature enables you manage the user access rights for remote access management based on the Services being used, IP addresses and Passwords.

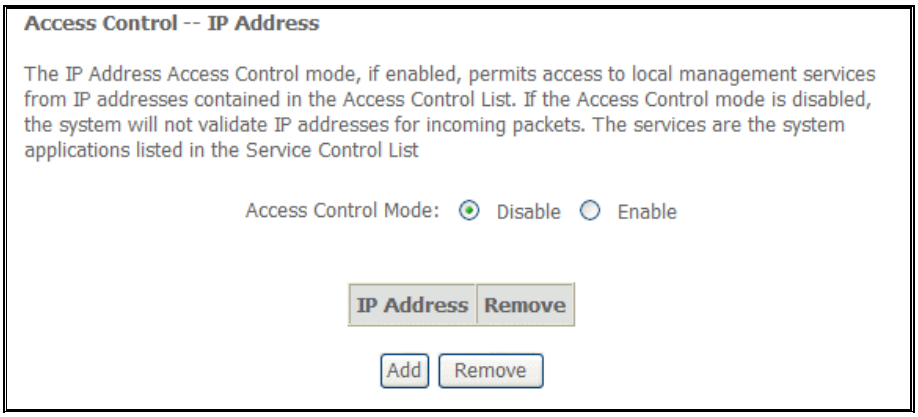
Services

Select which Services to allow and whether to allow from the LAN or the WAN.



IP Addresses

The Access Control Mode is disabled by default.

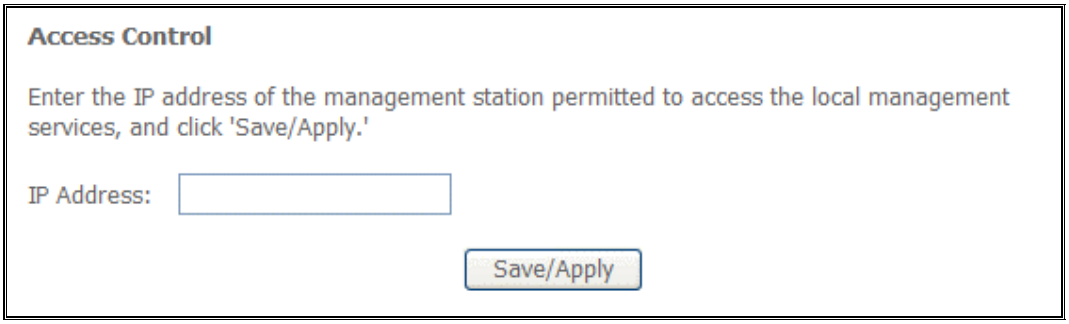


To allow remote management based on an authorized IP address, select Enable and click Add.

Key in the IP address of the PC from which a user will be allowed to access the web configuration menu.

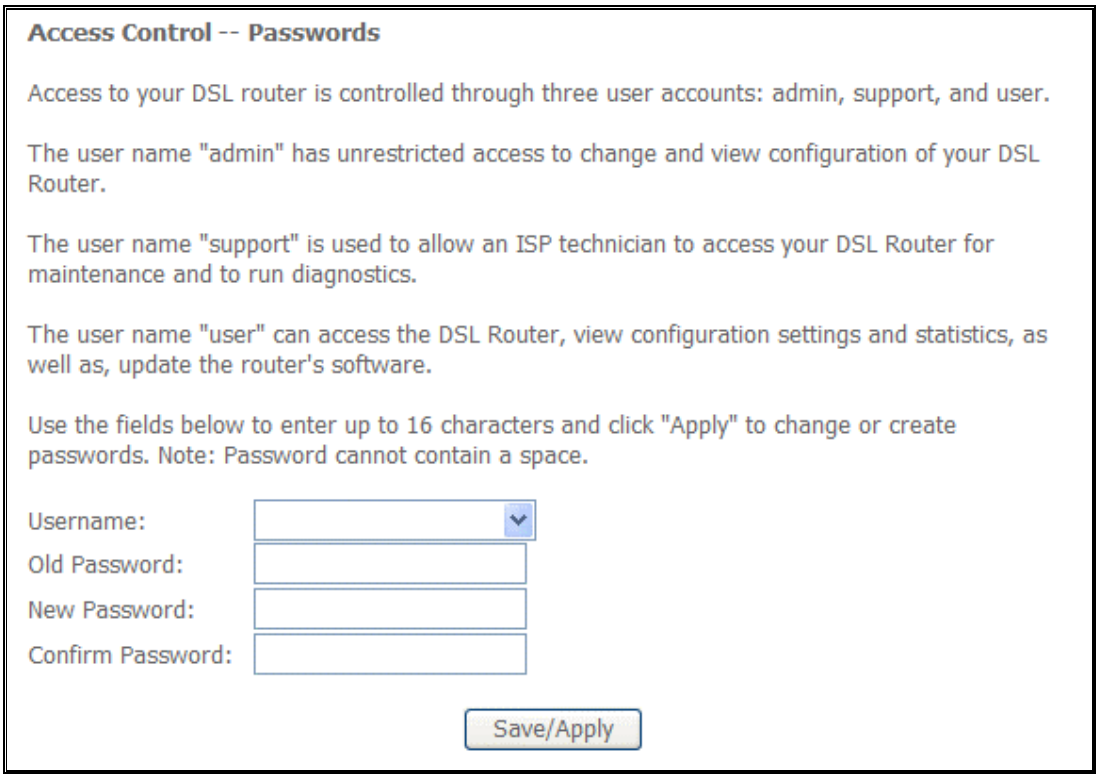
Click Save/Apply to take effect the settings. Then the IP Address will be added into the table list.

To delete the existing IP address, tick the Remove checkbox next to the selected IP address in the table list and click then Remove.



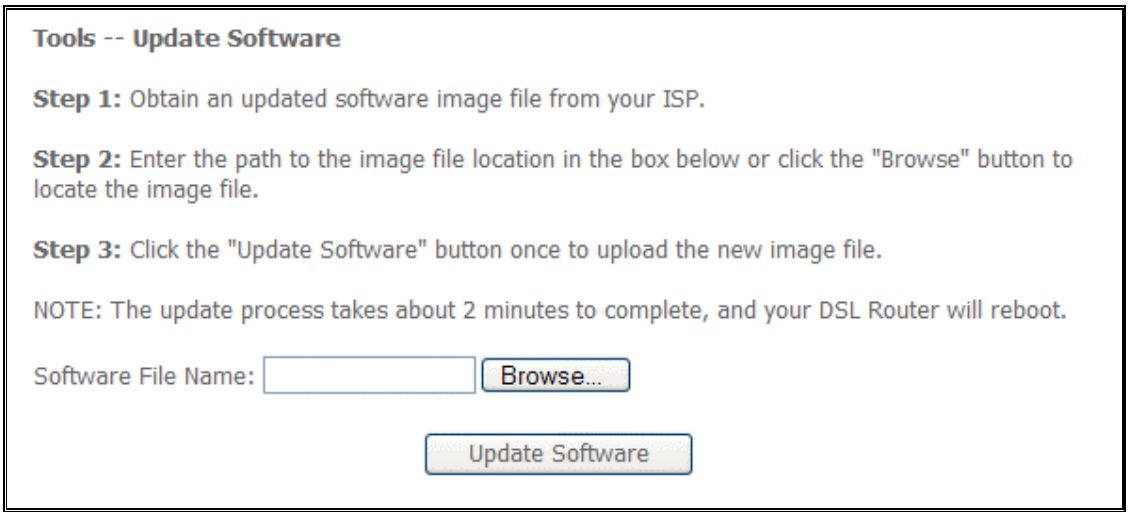
Passwords

When you configure the router through an Internet browser, the system requires you to enter your user name and password to validate your access permission. By default, the Username is set to “admin” and the Password to “admin”.



Update Software

The router's software is stored in the FLASH memory and can be upgraded as new software is released. Click Browse to locate the software file and then click Update Software.



Reboot

This feature allows the router to enable new network configuration to take effect or to clear problems with the modem router's network connection.

⚠ 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.

FCC Notice

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Aztech could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Exposure Information to Radio Frequency Energy

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