

# **User Manual**

Ethernet Wireless Router

© Copyright 2007 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. We reserve the right to revise this document at any time without the obligation to notify any person and/or entity. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

#### 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 LIABILITY 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

<b>About the Router</b> .....	<b>6</b>
<b>Requirements</b> .....	<b>7</b>
<b>Package Contents</b> .....	<b>7</b>
<b>Device Design</b> .....	<b>8</b>
<b>Getting Started</b> .....	<b>10</b>
<b>Planning Your Network</b> .....	<b>11</b>
<b>Remove or Disable Conflicts</b> .....	<b>12</b>
Internet Sharing, Proxy, and Security Applications.....	12
Configuring TCP/IP Settings.....	13
Configuring Internet Properties.....	13
Removing Temporary Internet Files.....	14
<b>Setup the Device</b> .....	<b>15</b>
<b>Connecting to the Internet</b> .....	<b>16</b>
Connecting Via Quick Setup.....	16
Connecting Via the Setup Utility Wizard.....	18
<b>Connecting Wireless Devices</b> .....	<b>19</b>
<b>About the Web User Interface</b> .....	<b>20</b>
<b>Accessing the Web User Interface</b> .....	<b>20</b>
<b>Menus</b> .....	<b>20</b>
Device Info.....	21
Quick Setup.....	21
Advanced Setup.....	22
Wireless.....	22
Diagnostics.....	23
Management.....	23
<b>Device Info</b> .....	<b>24</b>
<b>Summary</b> .....	<b>24</b>
<b>WAN</b> .....	<b>24</b>
<b>Statistics</b> .....	<b>25</b>
LAN.....	25

WAN.....	25
ATM.....	26
ADSL.....	27
<b>Route</b> .....	<b>28</b>
<b>ARP</b> .....	<b>28</b>
<b>DHCP</b> .....	<b>29</b>
<b>Quick Setup</b> .....	<b>30</b>
<b>Advanced Setup</b> .....	<b>32</b>
<b>WAN</b> .....	<b>32</b>
<b>LAN</b> .....	<b>34</b>
<b>NAT</b> .....	<b>35</b>
Virtual Servers.....	35
Port Triggering.....	36
DMZ Host.....	37
<b>Security</b> .....	<b>39</b>
IP Filtering.....	39
Parental Control.....	42
<b>Quality of Service</b> .....	<b>43</b>
Queue Config.....	44
QoS Classification.....	45
<b>Routing</b> .....	<b>46</b>
Default Gateway.....	46
Static Route.....	46
RIP.....	47
<b>DNS</b> .....	<b>48</b>
DNS Server.....	48
Dynamic DNS.....	49
<b>DSL</b> .....	<b>52</b>
<b>Print Server</b> .....	<b>52</b>
<b>Port Mapping</b> .....	<b>53</b>
<b>IPSec</b> .....	<b>54</b>
<b>Certificate</b> .....	<b>55</b>
Local.....	55
Trusted CA.....	57

---

<b>Wireless</b> .....	<b>58</b>
<b>Basic</b> .....	<b>58</b>
<b>Security</b> .....	<b>59</b>
<b>MAC Filter</b> .....	<b>59</b>
<b>Wireless Bridge</b> .....	<b>61</b>
<b>Advanced</b> .....	<b>62</b>
<b>Station Info</b> .....	<b>63</b>
<b>Diagnostics</b> .....	<b>64</b>
<b>Management</b> .....	<b>65</b>
<b>Settings</b> .....	<b>65</b>
Backup.....	65
Update .....	65
Restore Default .....	66
<b>System Log</b> .....	<b>66</b>
<b>TR-069 Client</b> .....	<b>67</b>
<b>Internet Time</b> .....	<b>67</b>
<b>Access Control</b> .....	<b>68</b>
Services .....	68
IP Addresses.....	69
Passwords .....	70
<b>Update Software</b> .....	<b>71</b>
<b>Save/Reboot</b> .....	<b>71</b>

# 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.

## Requirements

Your computer must meet the following minimum requirements.

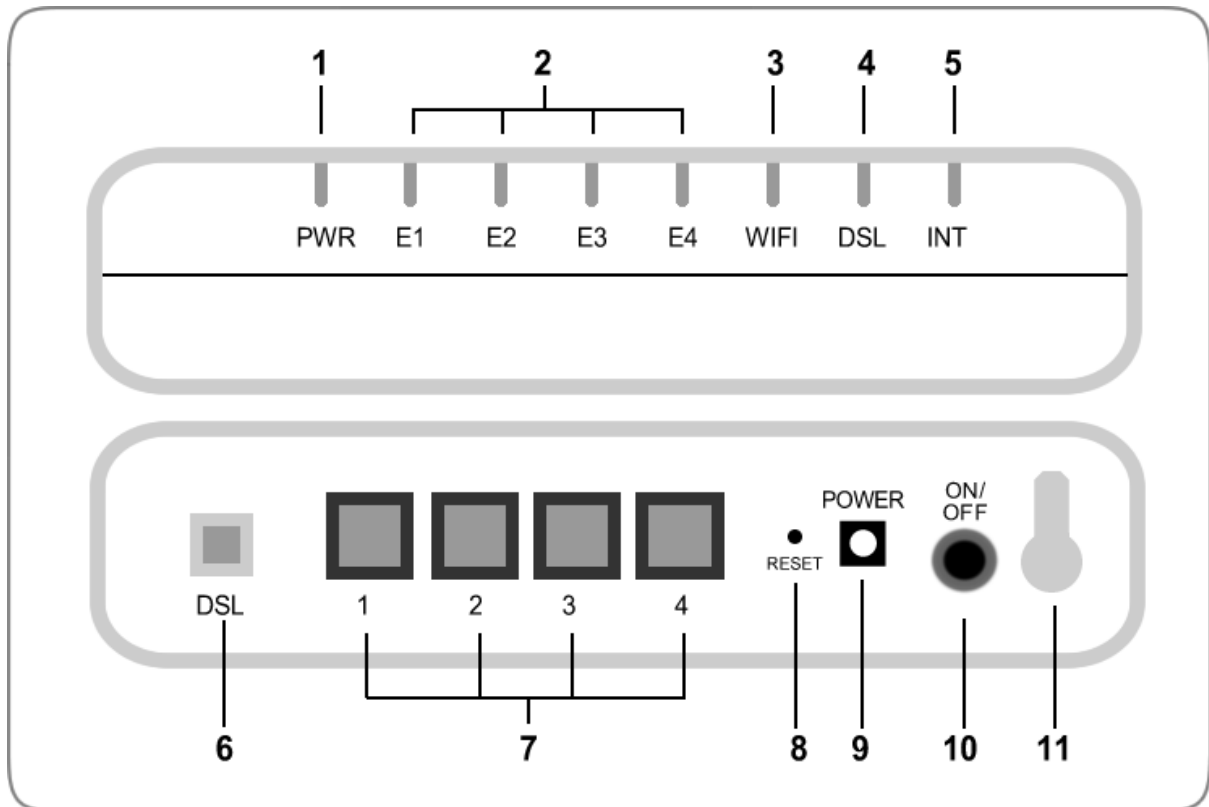
- Any operating system can be used
- Internet Explorer 4.0 or Netscape Navigator 3.02
- 233MHz processor
- CD-ROM Drive
- Ethernet network adapter
- An active DSL Internet account

## 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
- 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 light	Connected to an AC power supply
2	ETHERNET 1-4	Off	No Ethernet connection
		Steady light	Connected to an Ethernet port
		Blinking light	Transmitting/Receiving data
3	WiFi	Off	Access point is disabled
		Steady light	Access point is enabled
		Blinking light	Transmitting/Receiving data
4	DSL	Off	No DSL signal
		Blinking light	Establishing DSL signal
		Steady light	DSL signal is established

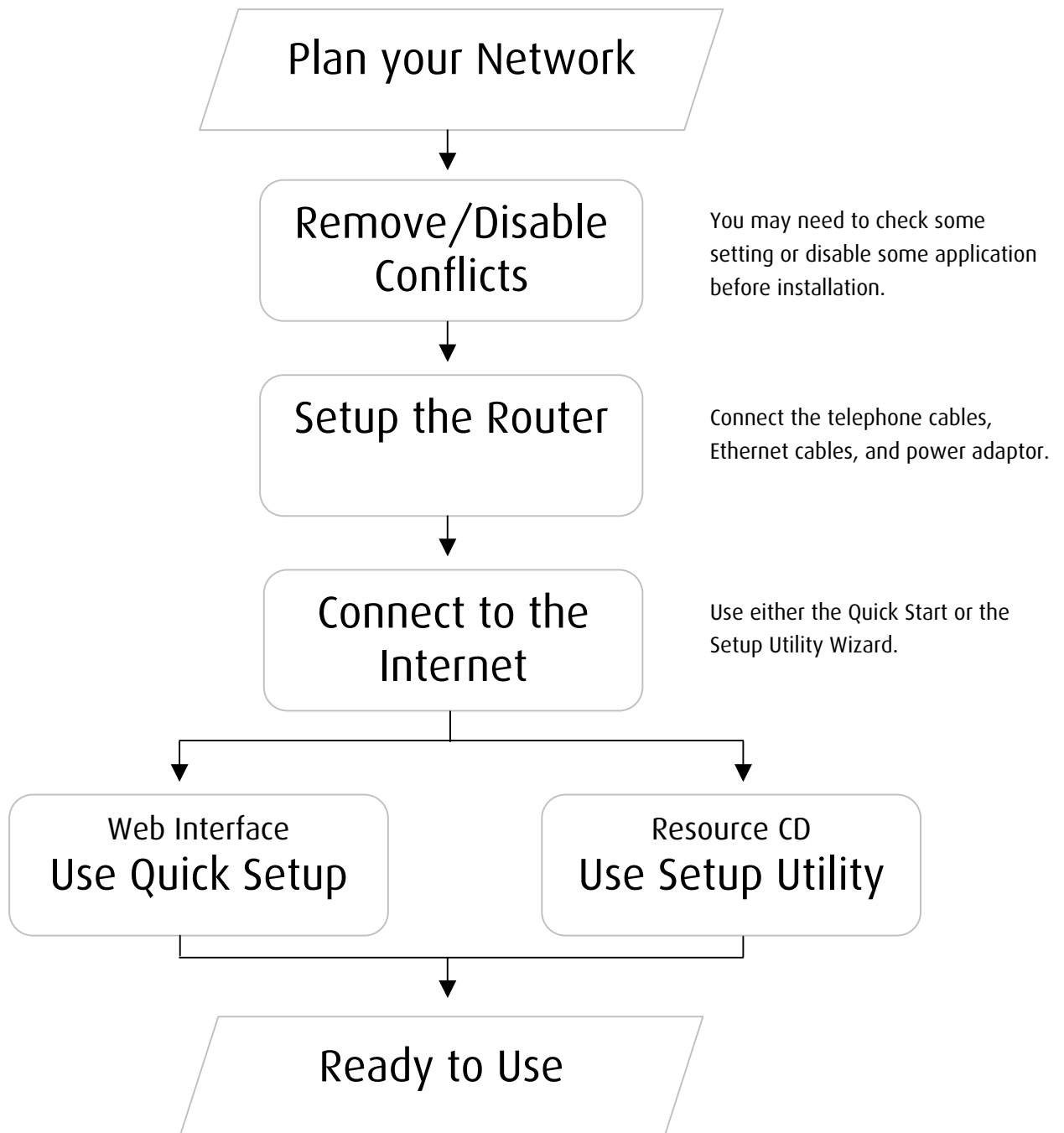


---

5	INTERNET	Off	No Internet connection
		Green light	Connected to the Internet
		Green Blinking light	Transmitting/Receiving data
		Red Blinking 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

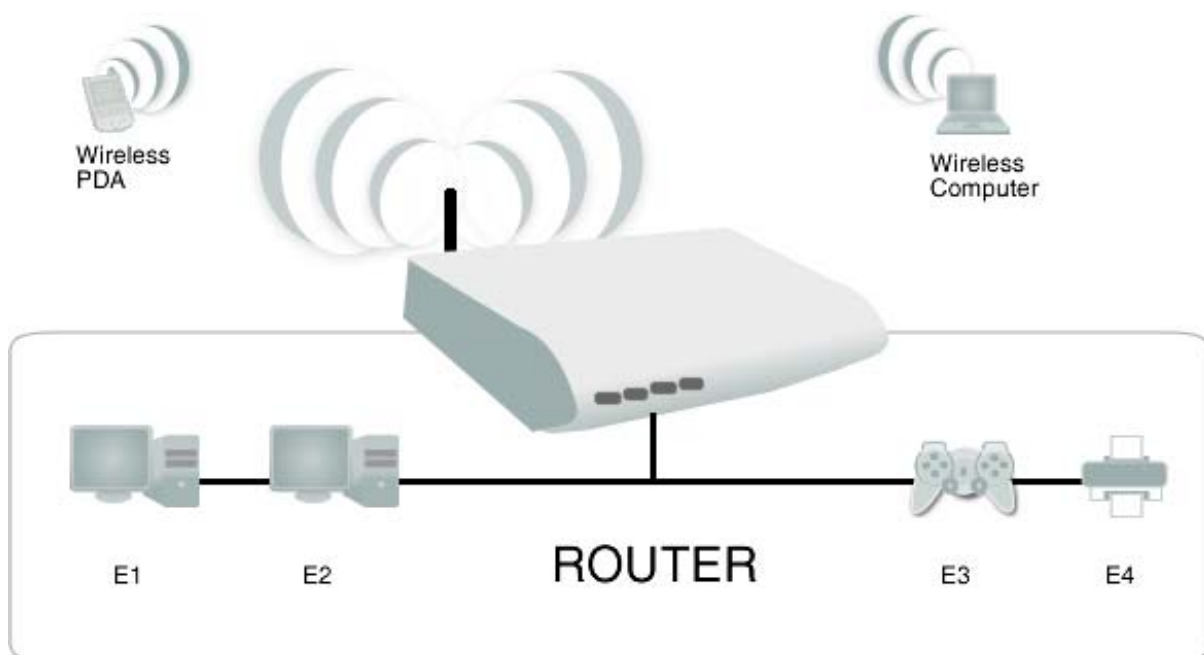
# Getting Started

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.

---

<b>Internet Sharing Applications</b>	<b>Proxy Software</b>	<b>Security Software</b>
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 the telephone 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

There are two ways to connect to the Internet. You can either use the Web Interface or the Utility Wizard.

## Connecting Via Quick Setup

### To connect to the Inter via the Web Interface:

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.

**Quick Setup**

Service Name: Quickstart

Protocols:  Encapsulation Mode:

**PPP Settings**

PPP Username:

PPP Password:

**PVC Settings**

VPI: [0-255]  VCI: [32-65535]

**LAN Configuration**

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

**Wireless Settings**

Enable Wireless

Enter the wireless network name (also known as SSID).

SSID:

Save - Only saves configuration data.  
Save/Reboot - Saves configuration data and reboots the router to make the new configuration effective.

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.

## Connecting Via the Setup Utility Wizard

The Setup Utility Wizard can be used to configure your router. However, this only runs on Windows operating systems with a CD-ROM drive.



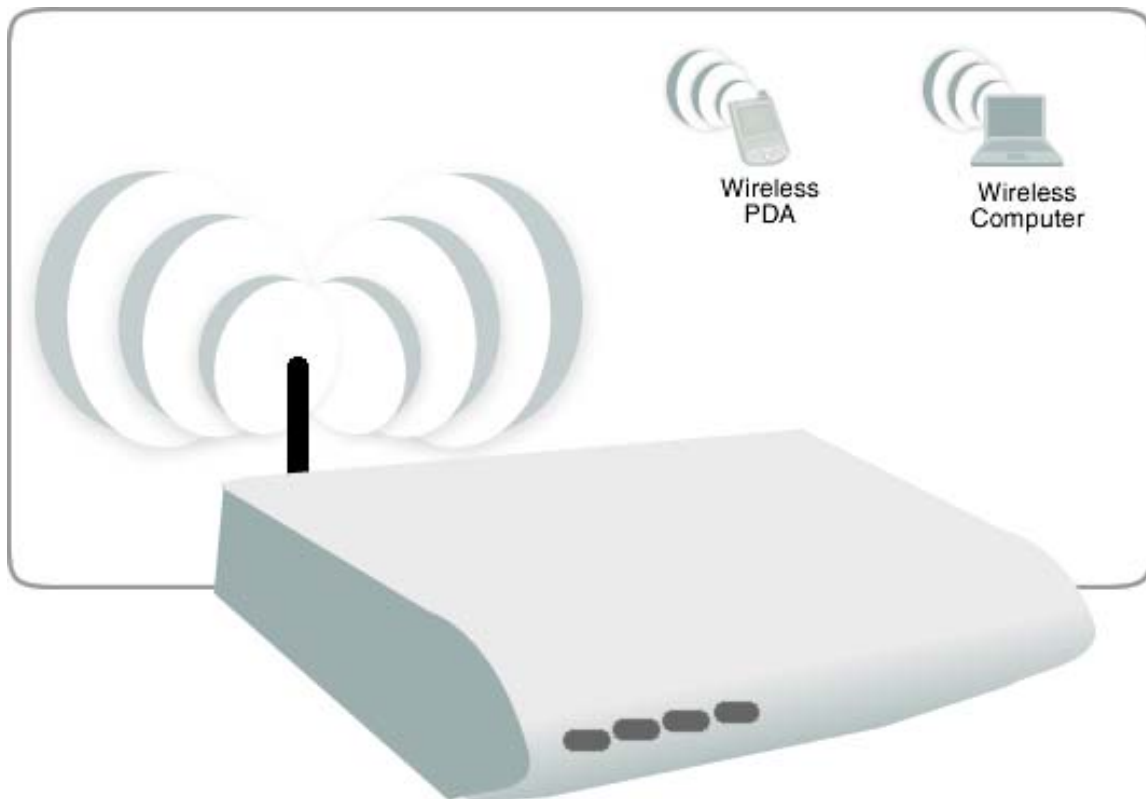
### **To connect to the Internet thru Setup Utility Wizard:**

1. Insert the Resource 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.

---

## 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 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. 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*.




## Menus


The Web User Interface includes the following menus:

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management

## Device Info

 <b>Device Info</b> Summary WAN Statistics Route ARP DHCP Quick Setup Advanced Setup Wireless Diagnostics Management	<b>Device Info</b>	
	<b>Model:</b>	Lynx L526
	<b>Board ID:</b>	96358M
	<b>Base MAC Address:</b>	00:30:0A:9E:5D:4E
	<b>Firmware Version:</b>	157.48.1
	<b>Software Version:</b>	3.10L.02.A2pB023c.d20h
	<b>Bootloader (CFE) Version:</b>	1.0.37-10.1
	<b>Wireless Driver Version:</b>	4.120.24.0.cpe2.1
	This information reflects the current status of your DSL connection.	
	<b>Line Rate - Upstream (Kbps):</b>	
	<b>Line Rate - Downstream (Kbps):</b>	
	<b>LAN IP Address:</b>	192.168.1.1
	<b>Default Gateway:</b>	
	<b>Primary DNS Server:</b>	192.168.1.1
<b>Secondary DNS Server:</b>	192.168.1.1	
<b>Date/Time:</b>	Sat Jan 1 00:30:11 2000	

## Quick Setup

 Device Info <b>Quick Setup</b> Advanced Setup Wireless Diagnostics Management	<b>Quick Setup</b>	
	Service Name: Quickstart	
	Protocols: <input type="text" value="PPPoE"/>	Encapsulation Mode: <input type="text" value="LLC/SNAP-BRIDGING"/>
	<b>PPP Settings</b>	
	PPP Username: <input type="text" value="user"/>	PPP Password: <input type="password" value="••••"/>
	<b>PVC Settings</b>	
	VPI: [0-255] <input type="text" value="0"/>	VCI: [32-65535] <input type="text" value="35"/>
	<b>LAN Configuration</b>	
	IP Address: <input type="text" value="192.168.1.1"/>	Subnet Mask: <input type="text" value="255.255.255.0"/>
	<input type="radio"/> Disable DHCP Server <input checked="" type="radio"/> Enable DHCP Server	
	Start IP Address: <input type="text" value="192.168.1.2"/>	End IP Address: <input type="text" value="192.168.1.254"/>
	<b>Wireless Settings</b>	
	Enable Wireless <input checked="" type="checkbox"/> Enter the wireless network name (also known as SSID). SSID: <input type="text" value="starbridge"/>	
	<input type="button" value="Save"/> <input type="button" value="Save/Reboot"/>	
<b>Save</b> - Only saves configuration data. <b>Save/Reboot</b> - Saves configuration data and reboots the router to make the new configuration effective.		

# Advanced Setup

**ST** **BRIDGE**

- Device Info
- Quick Setup
- Advanced Setup
- WAN
- LAN
- NAT
- Security
- Quality of Service
- Routing
- DNS
- DSL
- Port Mapping
- Certificate
- Wireless
- Diagnostics
- Management

### Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
Choose Save/Reboot to apply the changes and reboot the system.

Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	quickstart	ppp_0_0_35_1	PPPoE	Disabled	Enabled	Enabled	<input type="checkbox"/>	<input type="button" value="Edit"/>

# Wireless

**ST** **BRIDGE**

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Basic
- Security
- MAC Filter
- Wireless Bridge
- Advanced
- Station Info
- Diagnostics
- Management

### Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.  
Click "Apply" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise

SSID:

BSSID:


Country:

Max Clients:

#### Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Max Clients	BSSID
<input type="checkbox"/>	<input style="width: 150px;" type="text" value="Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="128"/>	N/A
<input type="checkbox"/>	<input style="width: 150px;" type="text" value="Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="128"/>	N/A
<input type="checkbox"/>	<input style="width: 150px;" type="text" value="Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 50px;" type="text" value="128"/>	N/A

# Diagnostics



quickstart Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your ENET1 Connection:	PASS	<a href="#">Help</a>
Test your ENET2 Connection:	PASS	<a href="#">Help</a>
Test your ENET3 Connection:	PASS	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>


**Test the connection to your DSL service provider**

Test ADSL Synchronization:	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	PASS	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	PASS	<a href="#">Help</a>

**Test the connection to your Internet service provider**

Test PPP server connection:	PASS	<a href="#">Help</a>
Test authentication with ISP:	PASS	<a href="#">Help</a>
Test the assigned IP address:	PASS	<a href="#">Help</a>
Ping default gateway:	PASS	<a href="#">Help</a>
Ping primary Domain Name Server:	PASS	<a href="#">Help</a>

# Management



Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

- Device Info
- Quick Setup
- Advanced Setup
- Wireless
- Diagnostics
- Management**
- Settings
- System Log
- TR-069 Client
- Internet Time
- Access Control
- Update Software
- Save/Reboot

# Device Info

## Summary

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

Device Info	
Model:	Lynx L526
Board ID:	96358M
Base MAC Address:	00:30:0A:9E:5D:4E
Firmware Version:	157.48.1
Software Version:	3.10L.02.A2pB023c.d20h
Bootloader (CFE) Version:	1.0.37-10.1
Wireless Driver Version:	4.120.24.0.cpe2.1

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	
Secondary DNS Server:	
Date/Time:	

### To view Summary:

1. Select Device Info.
2. Click Summary.

## WAN

WAN displays a summary of the WAN connection settings.

WAN Info										
Port/VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address

### 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.

**Statistics -- LAN**

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet eth0	312312	2445	0	0	1171946	2721	0	0
Wireless	0	0	0	0	0	0	0	0

[Reset Statistics](#)

### 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.

**Statistics -- WAN**

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
quickstart	0/0/35	PPPoE	ppp_0_0_35_1	0	0	0	0	0	0	0	0

[Reset Statistics](#)

### 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.

ATM Interface Statistics											
In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
0	0	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics							
In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics					
VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0

### To view ATM statistics:

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

## ADSL

ADSL displays a statistical summary of the ADSL connection.

Statistics -- ADSL		
Mode:		
Type:		
Line Coding:		
Status:	Link Down	
Link Power State:	L0	
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		
<input type="button" value="ADSL BER Test"/> <input type="button" value="Reset Statistics"/>		

### To view ADSL statistics:

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

# Route

Route displays the routing rules implemented in the router.

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

## To view Route:

1. Select Device Info.
2. Click Router.

# ARP

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

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:11:43:B7:E7:F2	br0

## To view ARP:

1. Select Device Info.
2. Click ARP.

---

# DHCP

DHSCP displays all the DHCP clients connected to the router.

Device Info -- DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
mycomputer	00:11:43:B7:E7:F2	192.168.1.2	23 hours, 56 minutes, 58 seconds

### 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.

**Quick Setup**

Service Name: Quickstart

Protocols:  Encapsulation Mode:

**PPP Settings**

PPP Username:

PPP Password:

**PVC Settings**

VPI: [0-255]  VCI: [32-65535]

**LAN Configuration**

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

**Wireless Settings**

Enable Wireless

Enter the wireless network name (also known as SSID).

SSID:

Save - Only saves configuration data.  
Save/Reboot - Saves configuration data and reboots the router to make the new configuration effective.

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.

## WAN

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

### Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.  
Choose Save/Reboot to apply the changes and reboot the system.

Port/VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
--------------	---------	----------	---------	-----------	----------	------	-----	-------	--------	------

### To create a new WAN connection:

1. Select Advanced Setup.
2. Click WAN.
3. Click Add.
4. Enter the connection settings:
  - a. Enter the ATM PVC Configuration, QoS Setting, and then click Next.

#### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

VLAN Mux - Enable Multiple Protocols Over a Single PVC

Service Category:

#### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service



- b. Select the Connection Type, Encapsulation, and then click Next.

**Connection Type**

Select the type of network protocol for IP over Ethernet as WAN interface

PPP over ATM (PPPoA)  
 PPP over Ethernet (PPPoE)  
 MAC Encapsulation Routing (MER)  
 IP over ATM (IPoA)  
 Bridge

**Encapsulation Mode**

VC/MUX ▼

- c. Enable/Disable Bridge Service

**Unselect the check box below to disable this WAN service**

Enable Bridge Service:

Service Name:

- d. Check the settings. Click Back to apply modifications.

**WAN Setup - Summary**

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

<b>VPI / VCI:</b>	
<b>Connection Type:</b>	Bridge
<b>Service Name:</b>	test
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Not Applicable
<b>Service State:</b>	Disabled
<b>NAT:</b>	Disabled
<b>Firewall:</b>	Disabled
<b>IGMP Multicast:</b>	Not Applicable
<b>Quality Of Service:</b>	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.  
 NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

5. Click Save.

# LAN

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

**Local Area Network (LAN) Setup**

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:

Subnet Mask:

Enable IGMP Snooping

Standard Mode

Blocking Mode

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Enable DHCP Server Relay

DHCP Server IP Address:

Configure the second IP Address and Subnet Mask for LAN interface

# 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.

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	-------------	--------

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.

**NAT -- Virtual Servers**

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**  
 Remaining number of entries that can be configured:32

Server Name:  
 Select a Service:  ▼  
 Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP <span style="float: right;">▼</span>	<input type="text"/>	<input type="text"/>	<input type="text"/>

## 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.

**NAT -- Port Triggering Setup**

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application	Trigger		Open		Remove		
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	

Click Add to setup Port Triggering.

**NAT -- Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

**Remaining number of entries that can be configured:32**

Application Name:

- Select an application:
- Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	TCP <input type="button" value="v"/>

## 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.

**NAT -- DMZ Host**

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

# 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.

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

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

**Add IP Filter -- Outgoing**

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

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.

Incoming IP Filtering Setup							
By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be <b>ACCEPTED</b> by setting up filters.							
Choose Add or Remove to configure incoming IP filters.							
Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>							

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

Add IP Filter -- Incoming	
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.	
Filter Name:	<input type="text"/>
Protocol:	<input type="text" value="↓"/>
Source IP address:	<input type="text"/>
Source Subnet Mask:	<input type="text"/>
Source Port (port or port:port):	<input type="text"/>
Destination IP address:	<input type="text"/>
Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>
<b>WAN Interfaces (Configured in Routing mode and with firewall enabled only)</b>	
Select at least one or multiple WAN interfaces displayed below to apply this rule.	
<input checked="" type="checkbox"/>	Select All
<input checked="" type="checkbox"/>	pppoe_0_35_1/ppp_0_35_1
<input type="button" value="Save/Apply"/>	



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.

Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

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.

**Time of Day Restriction**

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address 
  
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

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.

## QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS

Select Default DSCP Mark

Save/Apply

## Queue Config

**QoS Queue Configuration -- A maximum 16 entries can be configured.**

Interfacename	Description	Precedence	Queue Key	Enable	Remove
---------------	-------------	------------	-----------	--------	--------

Click Add to create a QoS Queue Configuration.

**QoS Queue Configuration**

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

Queue:

Queue Precedence:

# QoS Classification

You can add or remove QoS Classification rules.

**Quality of Service Setup**  
 Choose Add or Remove to configure network traffic classes.

MARK				TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit

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:  ▼

Rule Status:  ▼

**Assign ATM Priority and/or DSCP Mark for the class**  
 If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:  ▼

Assign Differentiated Services Code Point (DSCP) Mark:  ▼

Mark 802.1p if 802.1q is enabled:  ▼

**Specify Traffic Classification Rules**  
 Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

**SET-1**

Physical LAN Port:  ▼

Protocol:  ▼

Differentiated Services Code Point (DSCP) Check:  ▼

▼

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

**SET-2**

802.1p Priority:  ▼

# 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).

**Routing -- Default Gateway**

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

Enable Automatic Assigned Default Gateway

## 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.

**Routing -- Static Route (A maximum 32 entries can be configured)**

Destination	Subnet Mask	Gateway	Interface	Remove
-------------	-------------	---------	-----------	--------

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

**Routing -- Static Route Add**

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface

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

**Routing -- RIP Configuration**

To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Global RIP Mode  Disabled  Enabled

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ppp_0_0_100_1	0/0/100	2	Passive	<input type="checkbox"/>

# 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 DNS server. Adding a Secondary DNS server is optional.

### DNS Server Configuration

If 'Enable Automatic Assigned DNS' checkbox is selected, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click 'Save' button to save the new configuration. You must reboot the router to make the new configuration effective.

Enable Automatic Assigned DNS

Save



## 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](http://www.dyndns.org)
- [www.tzo.com](http://www.tzo.com)

Click Add to create a Dynamic DNS setting.

**Dynamic DNS**

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

## 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.

**Add dynamic DDNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

**DynDNS Settings**

Username

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.

**Add dynamic DDNS**

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

**TZO Settings**

Email

Key

## DSL

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

**DSL Settings**

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

## Print Server

Your router supports the creation of a Print Server.

**Print Server settings**

This page allows you to enable / disable printer support.

- Enable on-board print server.

# Port Mapping

Port Mapping allows you to create groups composed of the various interfaces available in your router.

**Port Mapping -- A maximum 16 entries can be configured**

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				USB	<input checked="" type="checkbox"/>
				ENET	<input checked="" type="checkbox"/>

Click Add to create a port mapping group.

**Port Mapping Configuration**

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.  
**Note that these clients may obtain public IP addresses**
3. Click Save/Apply button to make the changes effective immediately

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

**IMPORTANT** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces:

Available Interfaces: ENET  
USB

Automatically Add Clients With the following DHCP Vendor IDs

# IPSec

Your router supports the authentication and encryption of data packets.

**IPSec Tunnel Mode Connections**

Add, edit or remove IPSec tunnel mode connections from this page.

Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses
--------	-----------------	----------------	-----------------	------------------

[Add New Connection](#)

Click Add New Connection to create an IPSec Setting.

**IPSec Settings**

IPSec Connection Name

Remote IPSec Gateway Address

Tunnel access from local IP addresses

IP Address for VPN

IP Subnetmask

Tunnel access from remote IP addresses

IP Address for VPN

IP Subnetmask

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings [Show Advanced Settings](#)

[Save / Apply](#)

# Certificate

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

## Local

**Local Certificates**

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
------	--------	---------	------	--------

## Create Certificate Request

**Create new certificate request**

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

## Import Certificate

**Import certificate**

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```



## Trusted CA

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

**Trusted CA (Certificate Authority) Certificates**

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.  
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
------	---------	------	--------

Click Import Certificate.

**Import CA certificate**

Enter certificate name and paste certificate content.

Certificate Name:

Certificate: 

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

# Wireless

## Basic

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

**Wireless -- Basic**

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

SSID:

BSSID:

Country:

Max Clients:

**Wireless - Guest/Virtual Access Points:**

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="Guest"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	N/A
<input type="checkbox"/>	<input type="text" value="Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	N/A
<input type="checkbox"/>	<input type="text" value="Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="128"/>	N/A

# Security

The router supports all the popular wireless security protocols.

**Wireless -- Security**

This page allows you to configure security features of the wireless LAN interface.

**Manual Setup AP**

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.  
Click "Save/Apply" when done.

Select SSID:

Network Authentication:

WEP Encryption:

# 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.

**Wireless -- MAC Filter**

MAC Restrict Mode:  Disabled  Allow  Deny

Click Add to add a MAC Address.

**Wireless -- MAC Filter**

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:



# Wireless Bridge

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

## Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.

Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

# Advanced

Advanced Wireless allows you to configure detailed wireless settings.

**Wireless -- Advanced**

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.  
Click "Apply" to configure the advanced wireless options.

Band:	2.4GHz	Current: 11
Channel:	11	
Auto Channel Timer(min)	0	
54g™ Rate:	Auto	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
XPress™ Technology:	Disabled	
54g™ Mode:	54g Auto	
54g™ Protection:	Auto	
Preamble Type:	long	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Disabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Save/Apply

# Station Info

Station Info scans wireless stations and displays their status.

**Wireless -- Authenticated Stations**

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
00:E0:98:CD:78:DF	Yes		starbridge	wl0

[Refresh](#)

# 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.

quickstart Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

**Test the connection to your local network**

Test your ENET1 Connection:	PASS	<a href="#">Help</a>
Test your ENET2 Connection:	PASS	<a href="#">Help</a>
Test your ENET3 Connection:	PASS	<a href="#">Help</a>
Test your ENET4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>

**Test the connection to your DSL service provider**

Test ADSL Synchronization:	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping:	PASS	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	PASS	<a href="#">Help</a>

**Test the connection to your Internet service provider**

Test PPP server connection:	PASS	<a href="#">Help</a>
Test authentication with ISP:	PASS	<a href="#">Help</a>
Test the assigned IP address:	PASS	<a href="#">Help</a>
Ping default gateway:	PASS	<a href="#">Help</a>
Ping primary Domain Name Server:	PASS	<a href="#">Help</a>



---

# Management

## Settings

When it comes to managing the settings which 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.

**Settings - Backup**

Backup DSL router configurations. You may save your router configurations to a file on your PC.

## 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.

**Tools -- Update Settings**

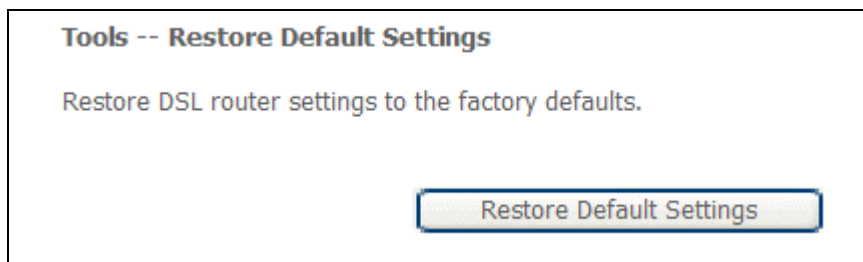
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

## Restore Default

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

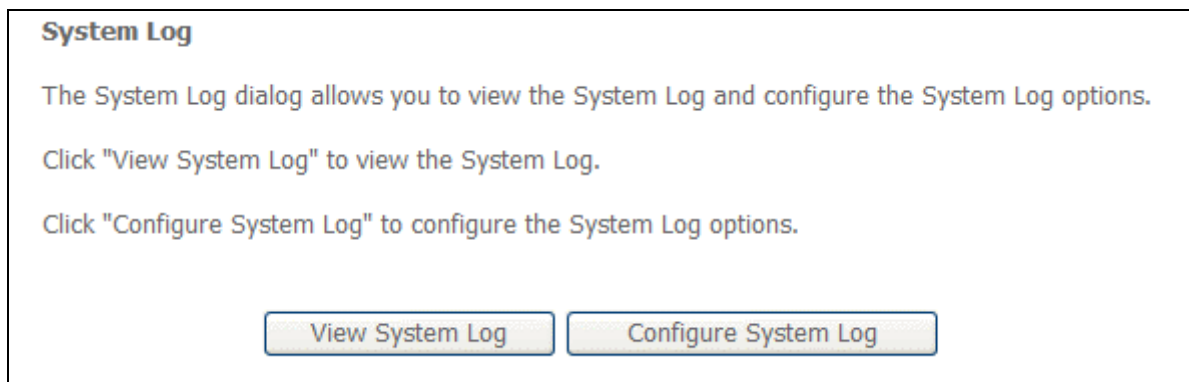
Upon clicking OK, you will be prompted to follow the instruction as shown below.



## 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.

**TR-069 client - Configuration**

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

Inform  Disable  Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Display SOAP messages on serial console  Disable  Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

## Internet Time

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

**Time settings**

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Time zone offset:

# 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.

**Access Control -- Services**

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	Enable	<input type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

## IP Addresses

The Access Control Mode is disabled by default.

**Access Control -- IP Address**

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode:  Disable  Enable

IP Address	Remove
	<input type="checkbox"/>

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.

**Access Control**

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

## 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".

**Access Control -- Passwords**

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

---

## 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.

### Tools -- Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

## Save/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.

Click the button below to save and reboot the router.

## 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.