

User Manual

DSL1000EW(L)

ADSL2/2+ 4-Ports 802.11b/g

© Copyright 2009 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

About the Router	6
Main Features	7
Requirements	10
Package Contents	10
Device Design	11
Getting Started	13
Planning Your Network	14
Remove or Disable Conflicts	15
Internet Sharing, Proxy, and Security Applications	15
Configuring TCP/IP Settings	16
Configuring Internet Properties	16
Removing Temporary Internet Files	17
Setup the Device	18
Connecting to the Internet	19
Connecting Via Quick Setup	19
Connecting Wireless Devices	20
About the Web User Interface	21
Accessing the Web User Interface	21
Menus	21
Device Info	21
Quick Setup	21
Advanced Setup	21
Wireless	21
Diagnostics	21
Management	21
Device Info	22
Summary	22
WAN	22
Statistics	23
LAN	23

WAN.....	23
ATM	23
ADSL.....	24
Route.....	25
ARP	25
DHCP	26
Quick Setup.....	27
Advanced Setup.....	28
ATM Interface.....	28
WAN.....	29
LAN	34
NAT.....	35
Virtual Servers.....	35
Port Triggering.....	36
DMZ Host.....	37
Security.....	38
IP Filtering	38
Parental Control.....	41
Quality of Service	42
Queue Config	43
QoS Classification.....	44
Routing.....	45
Default Gateway.....	45
Static Route	45
RIP	46
DNS.....	47
DNS Server	47
Dynamic DNS	48
DSL.....	51
DNS Proxy Configuration.....	51
Interface Grouping.....	52
LAN Ports.....	53
IPSec.....	53
Certificate.....	55

Local	55
Trusted CA	57
Wireless.....	58
Basic	58
Security.....	59
MAC Filter	60
Wireless Bridge	61
Advanced.....	62
Station Info.....	63
Diagnostics.....	64
Management.....	65
Settings.....	65
Backup.....	65
Update	65
Restore Default	66
System Log	66
TR-069 Client	67
Internet Time	67
Access Control.....	68
Services	68
IP Addresses	69
Passwords	70
Update Software.....	71
Reboot.....	71
FCG Notice.....	73

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™) 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

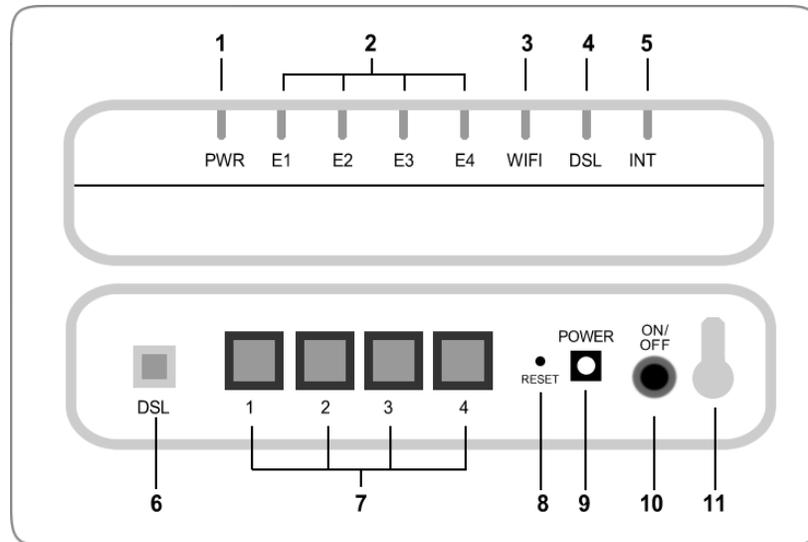
Package Contents

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

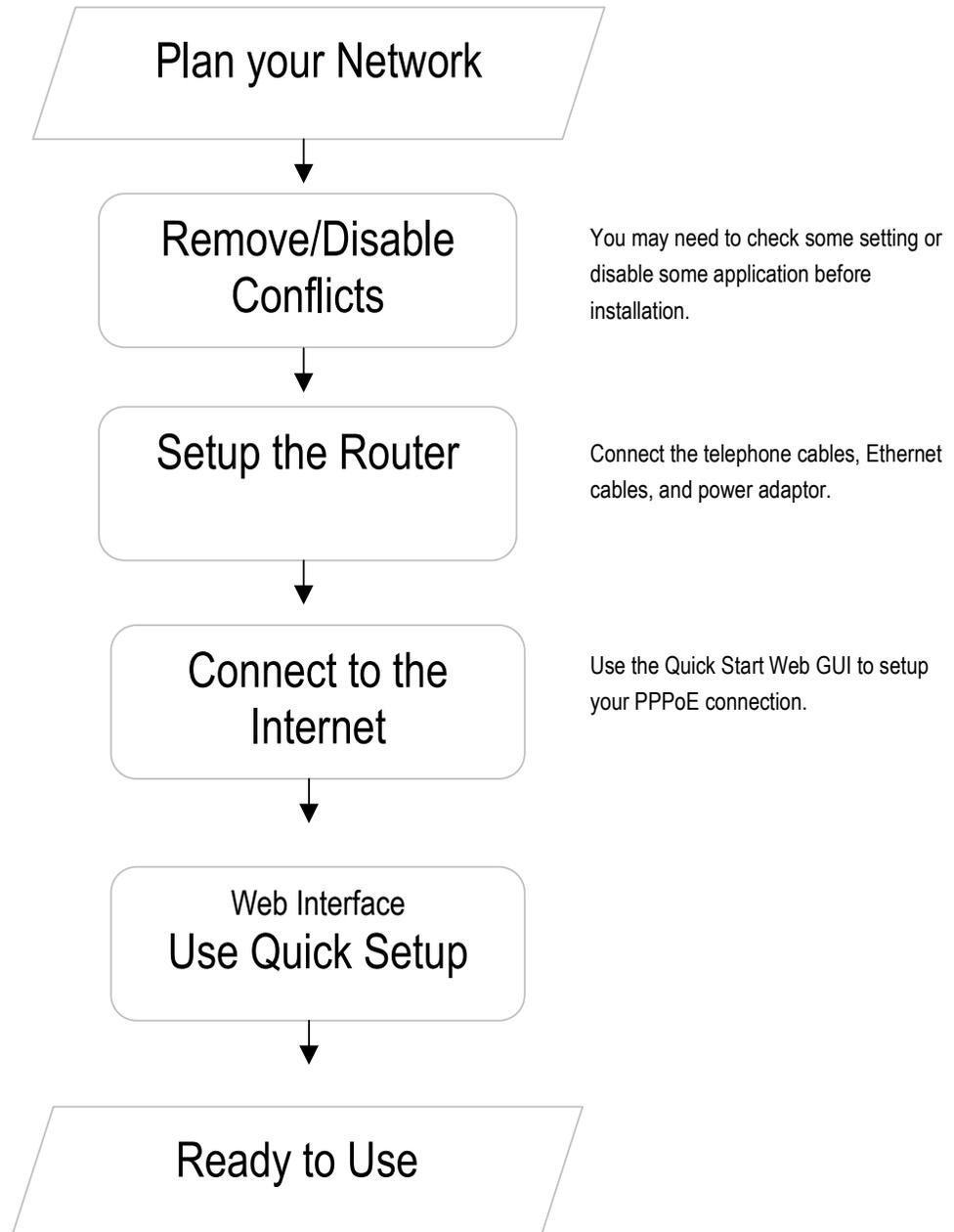


	Label	Action	Description
1	POWER	Off	No power is supplied to the device
		Steady green light	Connected to an AC power supply
		Steady red light	Error on the device
2	ETHERNET 1-4	Off	No Ethernet connection
		Steady green light	Connected to an Ethernet port
		Blinking green light	Transmitting/Receiving 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

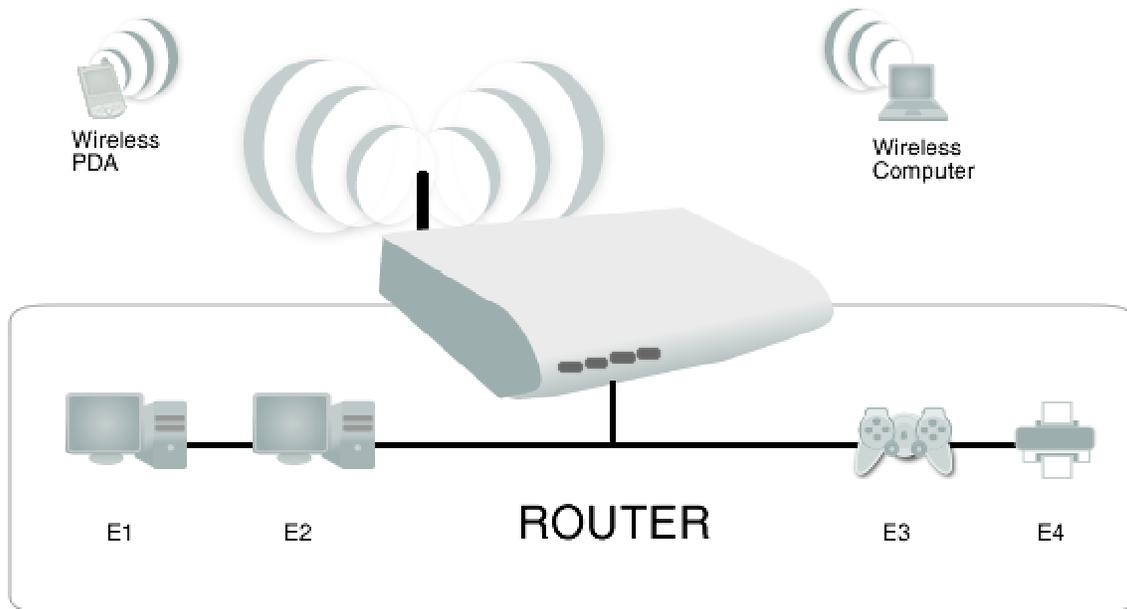
Getting Started

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 inetctl.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.

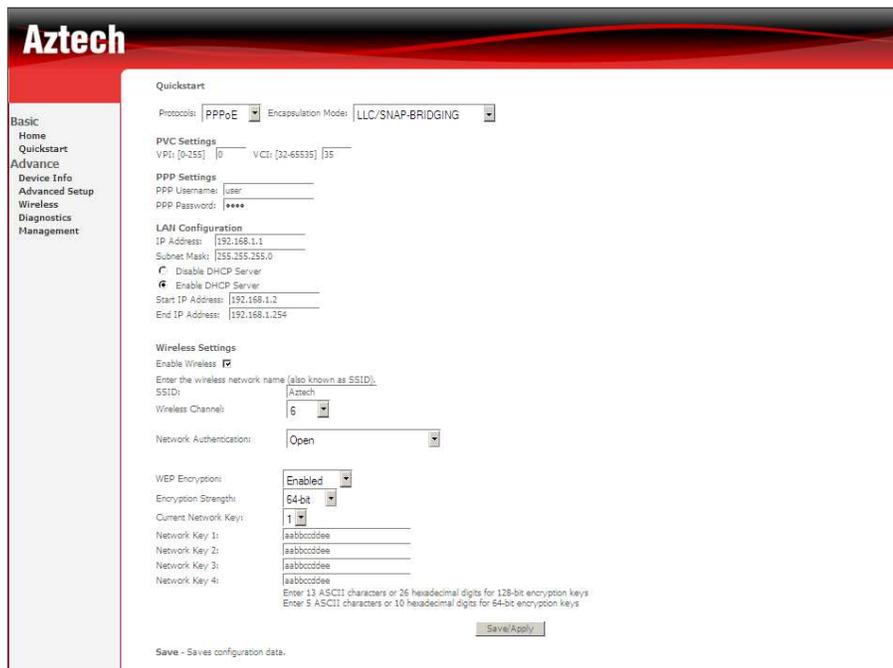
Connecting to the Internet

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

Connecting Via Quick Setup

To connect to the Internet via the Web Interface:

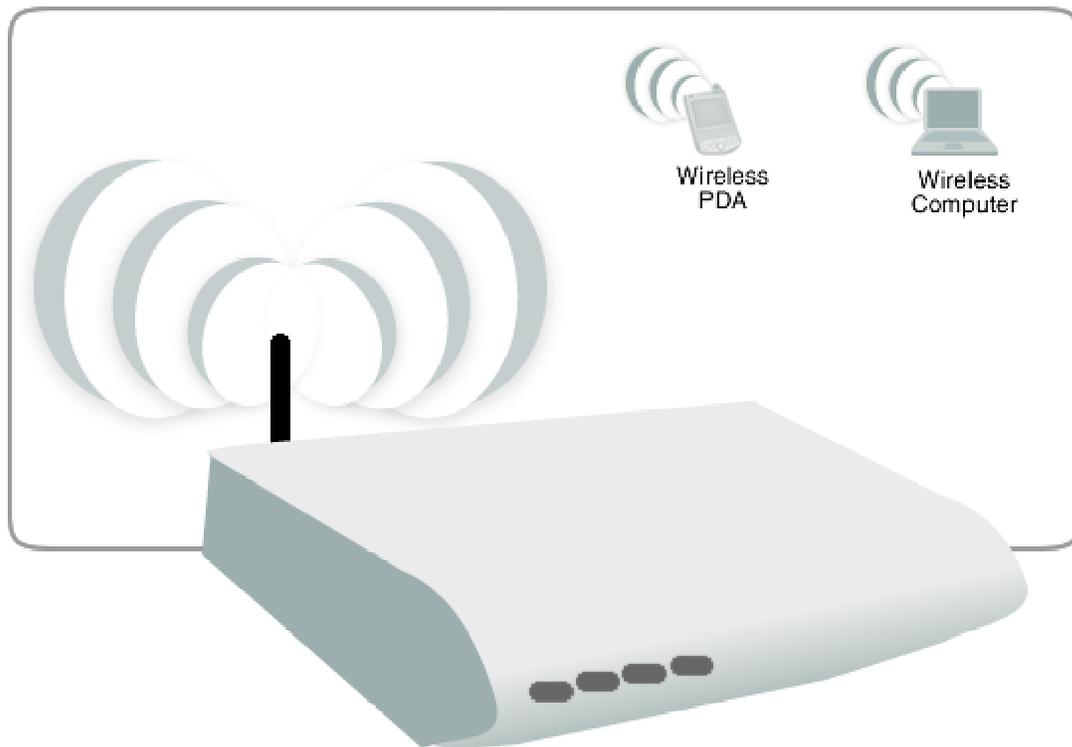
1. Open your browser.
2. Enter 192.168.1.1 and then press Enter.
3. Enter the User name and Password, and then click OK. The default User name and Password is *admin*.
4. Select Quickstart.



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.

Device Info	
Model:	DSL1000EW(L)
Board ID:	96333AW2G
Base MAC Address:	00:30:0A:FA:FC:9E
Firmware Version:	212.2
Software Version:	090827_0950-4.02L.03.A2pB025c1.d21j2
Bootloader (CFE) Version:	0.0.0-0.0
Wireless Driver Version:	5.10.85.0.cpe4.402.4

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	1304
Line Rate - Downstream (Kbps):	26106
LAN IPv4 Address:	192.168.1.1
Default Gateway:	ppp0
Primary DNS Server:	
Secondary DNS Server:	
LAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Mon Aug 31 13:52:26 2009

To view Summary:

1. Select Device Info.
2. Click Summary.

WAN

WAN displays a summary of the WAN connection settings.

WAN Info										
Interface	Description	Type	VlanMuxId	IPv6	Igmp	MLD	NAT	Firewall	Status	IPv4 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.

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.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
-----------	-----	-----	-------------	----------	-----------	-----------------	-----	--------

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.

ATM PVC Configuration

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

VPI: [0-255]

VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Select Connection Mode

- Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection
 MSC Mode - Multiple Service over one Connection

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.

WAN

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

Wide Area Network (WAN) Service Setup												
Choose Add, Remove or Edit to configure a WAN service over a selected interface.												
Interface	Description	ConnId	Protocol	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	MLD	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Remove"/>												

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.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

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

WAN Service Configuration

Select WAN service type:

PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

Enable IPv6 for this service

- c. Key-in the PPP login information.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

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

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

- e. Configure the DSN server.

DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:
WAN Interface selected:

Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS 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.

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. GroupName Default ▾

IP Address:
Subnet Mask:

Enable IGMP Snooping

Standard Mode
 Blocking Mode

Enable LAN side firewall

Disable DHCP Server
 Enable DHCP Server

Start IP Address:
End IP Address:
Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

Configure the second IP Address and Subnet Mask for LAN interface

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 Name	Trigger		Open			WAN Interface	Remove	
	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

Use Interface:

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="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

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:

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 'Apply/Save' 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

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
<div style="display: flex; justify-content: center; gap: 10px;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>							

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 'Apply/Save' 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):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All

pppoe_0_0_35/ppp0

br0/br0

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
<div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div>											

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"/>						

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 

Queue Config

QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
<input type="button" value="Add"/>	<input type="button" value="Enable"/>	<input type="button" value="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 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 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Precedence:

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
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="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:

Rule Status:

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]:

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

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface

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 shows up.

Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

Use Interface:

Use Gateway IP Address:

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

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm0	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

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

Obtain DNS info from a WAN interface:
WAN Interface selected:

Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:

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.

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
----------	----------	---------	-----------	--------

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

DNS Proxy Configuration

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

Dns Proxy Configuration

Enable or disable Dns proxy.

Host name of the modem:

Domain name of the LAN network:

Interface Grouping

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

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping 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	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			ENET(1-4)	
			ENET5	
			USB	
			wlan0	
			wl0_Guest1	
			wl0_Guest2	
			wl0_Guest3	

Add Remove

Click Add to create an Interface grouping.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface 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.
3. 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. **Note that these clients may obtain public IP addresses**
4. Click Save/Apply button to make the changes effective immediately

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:

WAN Interface used in the grouping

Grouped LAN Interfaces

->

<-

Available LAN Interfaces

ENET(1-4)

ENET5

USB

wlan0

wl0_Guest1

wl0_Guest2

wl0_Guest3

Automatically Add Clients With the following DHCP Vendor IDs

Apply/Save

LAN Ports

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

LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

LAN Port
eth1
eth0.2
eth0.3
eth0.4
eth0.5
usb0
wl0

IPSec

Your router supports the authentication and encryption of data packets.

IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove
-----------------	----------------	-----------------	------------------	--------

Click Add New Connection to create an IPSec Setting.

IPSec Settings

IPSec Connection Name	<input type="text" value="new connection"/>
Remote IPSec Gateway Address (IP or Domain Name)	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="Auto(IKE)"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="text" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Show Advanced Settings"/>
	<input type="button" value="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

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/Save" to configure the basic wireless options.

Enable Wireless

Hide Access Point

Clients Isolation

Disable WMM Advertise

Enable Wireless Multicast Forwarding (WMM)

SSID:

BSSID: 00:90:4C:DF:00:06

Country:

Max Clients:

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.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)

WPS Setup

Enable WPS:

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 "Apply/Save" 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

MAC Address **Remove**

Add **Remove**

Click Add to add a MAC Address.

Wireless -- MAC Filter

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

MAC Address:

Apply/Save

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

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

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/Save" to configure the advanced wireless options.

Band:	<input type="text" value="2.4GHz"/>	
Channel:	<input type="text" value="11"/>	Current: 11
Auto Channel Timer(min)	<input type="text" value="0"/>	
54g™ Rate:	<input type="text" value="Auto"/>	
Multicast Rate:	<input type="text" value="Auto"/>	
Basic Rate:	<input type="text" value="Default"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
DTIM Interval:	<input type="text" value="1"/>	
Beacon Interval:	<input type="text" value="100"/>	
Global Max Clients:	<input type="text" value="16"/>	
XPress™ Technology:	<input type="text" value="Disabled"/>	
54g™ Mode:	<input type="text" value="54g Auto"/>	
54g™ Protection:	<input type="text" value="Auto"/>	
Preamble Type:	<input type="text" value="long"/>	
Transmit Power:	<input type="text" value="100%"/>	

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		wirelessnetworkname	wl0

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 ENET(1-4) Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	PASS	Help
Test ATM OAM F5 segment ping:	PASS	Help
Test ATM OAM F5 end-to-end ping:	PASS	Help

Test the connection to your Internet service provider

Test PPP server session:	PASS	Help
Test authentication with ISP:	PASS	Help
Test the assigned IP address:	PASS	Help
Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

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.

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

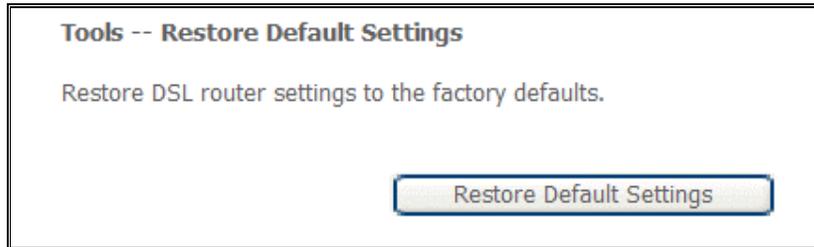
Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Restore Default

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

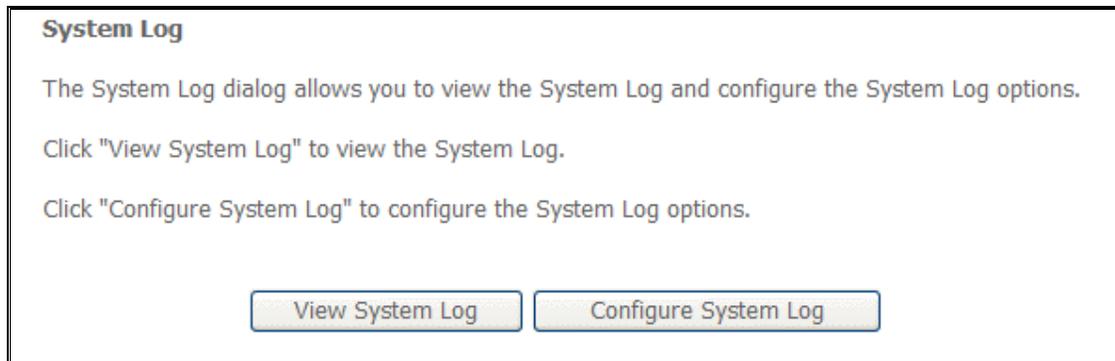
Upon clicking OK, you will be prompted to follow the instruction as shown below.



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/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

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

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
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" 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="text"/>	<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:

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 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.

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.