



# **USER MANUAL** v1.0

## **DSL1015EN(L)**

4 Port ADSL 2/2+ Wireless N Modem Router



© Copyright 2010 All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form 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.

# Table of Contents

<b>About the Router</b>	<b>1</b>
Minimum System Requirements	2
Package Contents	2
Device Overview	3
Front Panel	3
Back Panel	4
<b>Getting Started</b>	<b>5</b>
Planning Your Network	6
Remove or Disable Conflicts	7
Internet Sharing, Proxy, and Security Applications	7
Configuring TCP/IP Settings	8
Configuring Internet Properties	8
Removing Temporary Internet Files	9
Hardware Setup	10
Connecting to the Internet	10
Connecting via Quick Setup	10
<b>About the Web User Interface</b>	<b>12</b>
Accessing the Web User Interface	12
Menus	12
Quick Setup	13
Home Network Configuration	14
Local Area Network (LAN) Setup	14
DCHP Lease Information	15
Device Status	15
Statistics	16
Firewall Configuration	17
Firewall	17
Port Forwarding	18
DMZ	19
Device Administration	20
System – Backup	20
Restore to Default	20
Update Settings	21
Reboot	21
User Password	22

<b>Admin Mode</b>	<b>23</b>
Accessing the Admin Mode Web User Interface	23
<b>Menus</b>	<b>24</b>
Device Info	24
Device Status	25
Device Statistics	26
Home Network	26
Local Area Network (LAN) Setup	26
Advanced Setup	28
WAN	28
DDNS	28
Quality of Service	31
Routing – Default Gateway	31
Static Route	32
DSL Settings	34
Port Mapping	35
Firewall	36
IP Filtering	36
Parental Control	37
TCP/IP Sessions	38
Port Forwarding	39
Port Triggering	40
DMZ Host	41
Management	42
Firmware Upgrade	42
Settings Update	43
Settings Backup	44
Restore Default	45
Save/Reboot	46
Internet Time	47
Troubleshooting	48
System Log	48
Diagnostics	49
Network Tools	50
Access Control	51
Services	51
Password Settings	51
<b>Safety Precautions</b>	<b>53</b>



# About the Router

The Aztech DSL1015EN(L) ADSL2+ Wireless LAN 802.11b/g/n Advanced 4 Port Managed Switch Gateway using a solution that fully complies with ADSL, ADSL2, and ADSL2+ ITU standards. Aztech DSL1015EN(L) also supports the latest WiFi Alliance standard 802.11n Spec. This next generation ADSL advanced gateway will support Multiple Inputs and Multiple Outputs (MIMO) transmission at a speed of up to 300Mbps wireless speed.

Targeted at the residential and SOHO users that desires high quality triple play services, it is the ideal solution to provide a 6 in 1 device for both Wired and Wireless connectivity via a ADSL2/2+ Modem support, Routing functionality for multi-user sharing, 4 port 10/100 AutoMDI/MDix Managed Switch for IPTV deployment with QoS support, high speed 300 Mbps IEEE802.11n Wireless LAN access point with backward compatibility to 802.11b/g clients, USB 2.0 host for network storage attachment or printers.

Security is provided via double Stateful Packet Inspection and NAT based firewall. Hardware accelerated AES/WEP/WPA/WPA2 based encryption/MAC Address Filtering for Wireless links. Multiple session VPN Pass-through and DMZ support provide additional security support for telecommuters as well as allow flexibility while maintaining security against malicious hackers. Choices of Dynamic DNS server give users the flexibility of hosting a web or an FTP server with various domain names.

With Universal Plug and Play support, home networking becomes a breeze for everyone in the family. Multi Port Range/Popular Application Forwarding makes it even easier to select which application you want your network to allow while ensuring your security at the same time.

# Minimum System Requirements

Your computer must meet the following minimum requirements.

- Any operating system can be used
- Web Browser
- CDROM drive
- 233MHz processor
- 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

- Modem Router Aztech DSL1015EN(L)
- Power Adapter
- DSL Microfilter (Optional)
- Resource CD
- Ethernet cable (RJ45)
- Telephone cable (RJ11)
- Easy Start Guide

# Device Overview

## Front Panel



	Indicator Label	Action	Description
1	Power	Off	No power is supplied to the device
		On - Steady Green	Connected to an AC power supply
		On - Steady Red	Error on the device
2	Ethernet 1-4	Off	No Ethernet connection
		On - Steady Green	Connected to an Ethernet Device
		On - Blinking Green	Transmitting/Receiving data
3	USB Host	Off	No USB device connected
		On - Steady Green	USB device connected
4	Wireless	Off	Wireless interface disabled
		On - Steady Green	Wireless Interface enabled
		On - Blinking Green	Transmitting/Receiving data
5	DSL	Off	No DSL signal
		On - Blinking	Establishing DSL connection
		On - Steady Green	DSL connection established
6	Internet	Off	No Internet Connection
		On - Steady Green	Internet connection established
		On - Blinking Green	Transmitting/Receiving data
		On - Steady Red	PPP authentication failure

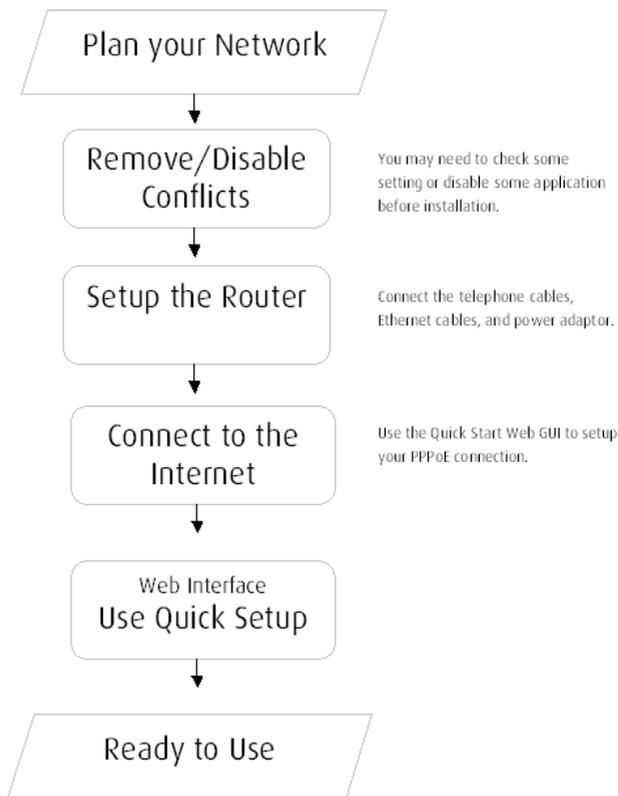
# Back Panel



Component	Description
1 Antenna	Sending/receiving wireless signals
2 Switch	Switching the device on/off
3 Power Adapter Jack	Connecting the power adapter
4 Reset Button	Resetting the device, press for 2 seconds to reset
5 USB Port	Connecting the USB Storage or Printer device
6 Ethernet Ports 1 - 4	Connecting with computers/devices through Ethernet cable
7 DSL	Connecting the telephone cable

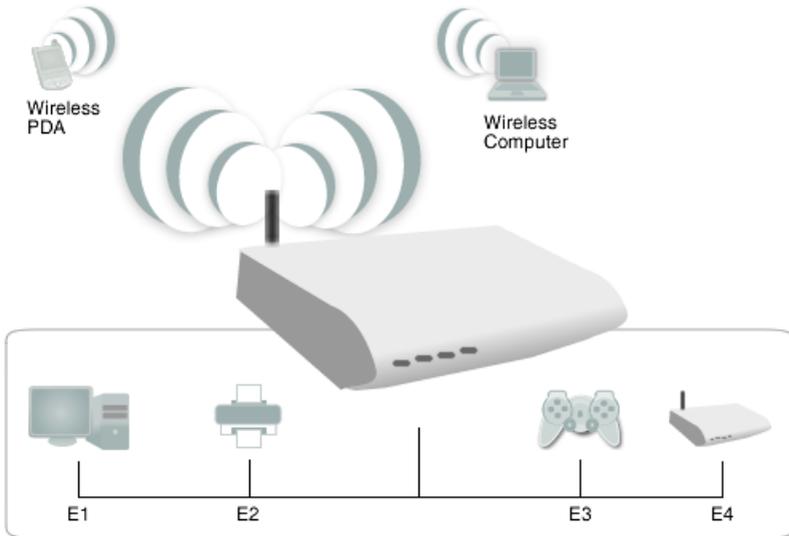
# Getting Started

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.



Each port in the router can be used for different connections. For example:

- E1 – Mom’s computer
- E2 – Network Printer
- E3 – Game Console
- E4 – Ethernet Device
- Wireless – Dad’s Computer
- Wireless – My Smart Phone

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

- Microsoft Internet Sharing

### Proxy Software

- WinGate
- WinProxy

### Security Software

- Symantec
- 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 inetcp.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.

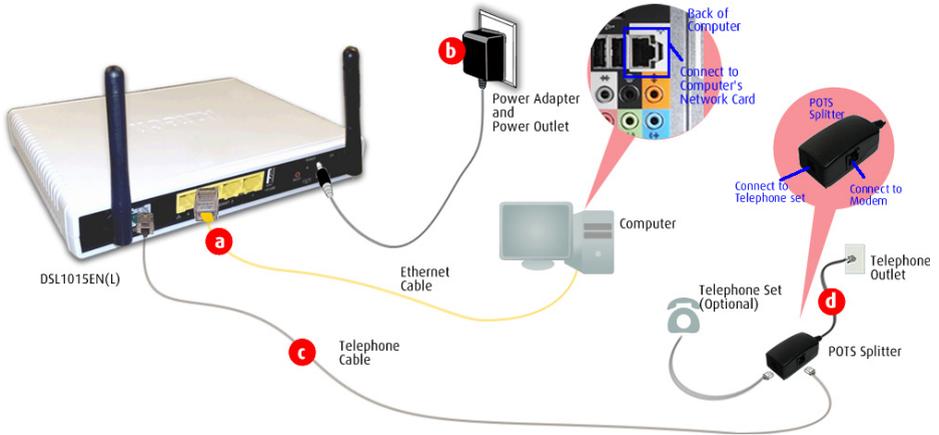
# Removing Temporary Internet Files

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.

# Hardware Setup



## Connecting to the Internet

### Connecting via Quick Setup

1. Launch the browser, the browser will bring you to the Credential Setup screen, click on SET UP NOW.

**Aztech**

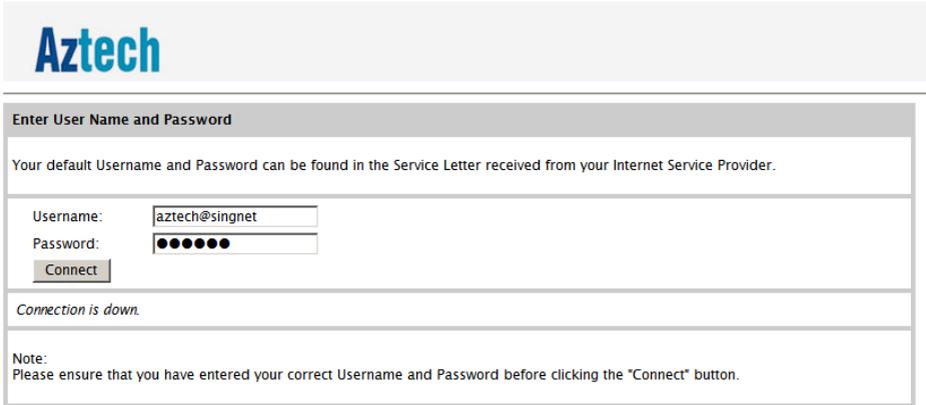
#### Credentials Setup

Welcome to Broadband Internet Setup. Click on SET UP NOW to run the Setup Wizard.

SET UP NOW

2. Input the username and password provided by the Internet Provider, and click on Connect.

Note: The username and password is normally printed on the Service Letter



**Aztech**

**Enter User Name and Password**

Your default Username and Password can be found in the Service Letter received from your Internet Service Provider.

Username:

Password:

*Connection is down.*

Note:  
Please ensure that you have entered your correct Username and Password before clicking the "Connect" button.

3. Once Internet connection is established, the following screen will be shown. Just close the browser and open it again to start surfing the Internet.

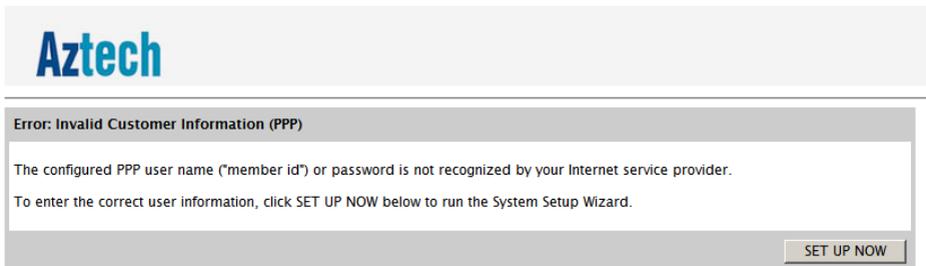


**Aztech**

**Setup Successful**

The setup is successful. Please close down your browser and restart it to continue browsing online.

4. If it failed to connect to the internet, the following screen will be shown, click on SET UP NOW, re input your username and password and click on Connect



**Aztech**

**Error: Invalid Customer Information (PPP)**

The configured PPP user name ("member id") or password is not recognized by your Internet service provider.

To enter the correct user information, click SET UP NOW below to run the System Setup Wizard.

# About the Web User Interface

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

## Accessing the Web User Interface

To access the Web User Interface:

1. Open your Internet browser.
2. Type - in `http://192.168.1.254` on the address bar and press Enter.

## Menus

The Web User Interface includes the following menus:

- Quick Setup
- Home Network Configuration
- Device Status
- Statistics
- Firewall Configuration
- Device Administration

# Quick Setup

Quick Setup includes Device Info to check basic information on your device and Internet Login Setup that allows you to control the PPP login account settings.

**Aztech**

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

QuickSetup

This page allow you to check the device information, control the device connection.

- [Device Info](#)
- [Internet Account Settings](#)
- [Wireless Settings](#)

---

**Device Info** [top](#)

Model:	DSL1015EN(L)
Board ID:	96358M
Base MAC Address:	00:26:75:1D:0D:10
Firmware Version:	230.106s.1-004
Software Version:	3.10L_02_A2pB023n8_d21k
Bootloader (CFE) Version:	1.0.37-10.1
Wireless Driver Version:	RT2860 INIC 2.0.0.0

**Internet Connection:** Connection is down.

**IPTV Connection:** Connection is down

---

**Internet Login Account Settings** [top](#)

# Home Network Configuration

Quick Setup includes Device Info to check basic information on your device and Internet Login Setup that allows you to control the PPP login account settings.

## Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. You may also configure the DHCP server and Public IP Pass Through settings of your router.

The screenshot displays the Aztech router's web management interface. At the top, the 'Aztech' logo is on the left, and a navigation bar contains icons for 'Quick Setup', 'Home Network Configuration', 'Device Status', 'Statistics', 'Firewall Configuration', and 'Device Administration'. Below the navigation bar, the 'Settings' section is active, showing the 'Local Area Network (LAN) Setup' page. The page contains the following configuration options:

- 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: 192.168.1.254
- Subnet Mask: 255.255.255.0
- Host Name: Modem
- Domain Name: Home
- Disable DHCP Server
- Enable DHCP Server
  - Start IP Address: 192.168.1.1
  - End IP Address: 192.168.1.253
  - Subnet Mask: 255.255.255.0
  - Leased Time (hour): 24
- Configure the second IP Address and Subnet Mask for LAN interface
- Enable Public IP Pass Through
  - Enable UPnP
  - Enable IGMP Snooping
  - Standard Mode
  - Blocking Mode

## DCHP Lease Information

Displays information on the DHCP clients connected to the router.

The screenshot shows the Aztech router's web interface. At the top, there is a navigation bar with icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. Below this is a 'Settings' section with 'Save' and 'Save Reboot' buttons. The main content area is titled 'Device Info -- DHCP Leases'. It contains a table of DHCP Server assigned devices, a table for Reserved Devices, and a form for Manual devices reserve.

**Device Info -- DHCP Leases**

DHCP Server assigned devices:

Hostname	MAC Address	IP Address	Expires In	Reserve
product-2c87658	00:21:70:6D:87:4D	192.168.1.1	23 hours, 54 seconds	<input type="button" value="Reserve"/>

Reserved Devices:

Hostname	MAC Address	IP Address	Delete
----------	-------------	------------	--------

Manual devices reserve:

MAC Address:  (example:00:D0:B7:23:A4:69)

IP Address:  (example:192.168.1.34)

Hostname:  (Max length:40 characters)

## Device Status

Displays the router information as well as status of different connections such as DSL, Internet and IPTV.

The screenshot shows the Aztech router's web interface. At the top, there is a navigation bar with icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. Below this is a 'System Info' section with tabs for System Info, DSL Status, Internet Status, and IPTV Status. The main content area is titled 'System Info' and contains a table of system information.

**System Info**

This information reflects the current status of your System Info.

Model:	DSL1015EN(L)
Board ID:	96358M
Base MAC Address:	00:28:75:1D:0D:10
Firmware Version:	230.106s.1-004
Software Version:	3.10L_02.A2pB023n8.d21k
Bootloader (CFE) Version:	1.0.37-10.1
Wireless Driver Version:	RT2860 INIC 2.0.0.0
Up time(hh:mm:ss):	01:04:20

# Statistics

Displays the statistics of different connections on your router.

**Aztech**

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

DSL Internet IPTV LAN

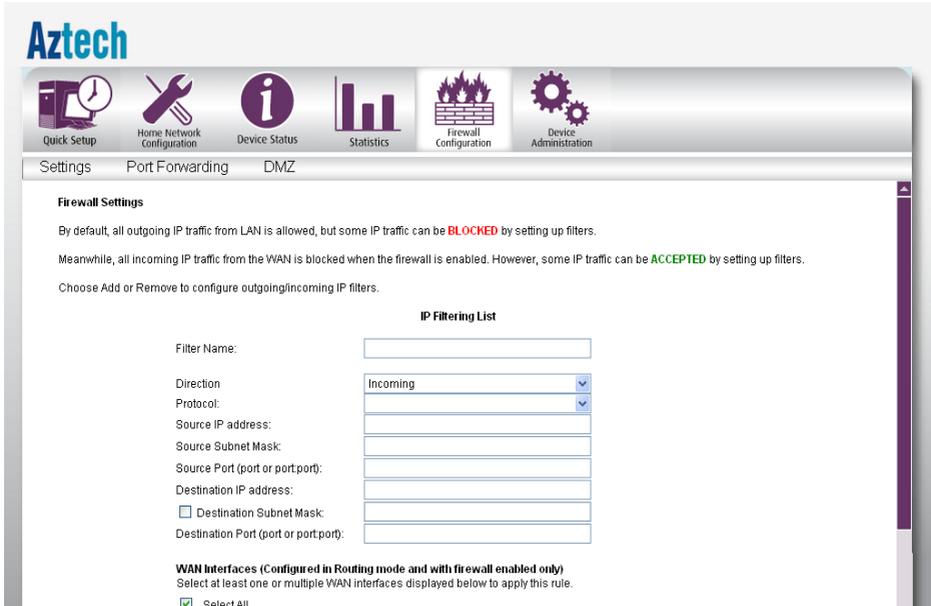
**Statistics -- ADSL**

Mode:	ADSL2+	
Line Coding:	Trellis On	
Status:	Link Up	
Link Power State:	L0	
Threshold Number Of Bins:	40	
Number Of Affected Bins:	8	
Microfilter Detection:	OK	
Retrans:	0	
	Downstream	Upstream
Attainable Rate (Kbps):	30649	1330
Current Rate (Kbps):	26221	1325
Attenuation (dB):	3.5	4.3
SNR Margin (dB):	12.7	6.9
Output Power (dBm):	11.9	12.3
MSGc (number of bytes in overhead channel message):	56	14
B (number of bytes in Mux Data Frame):	112	13
M (number of Mux Data Frames in FEC Data Frame):	1	16
T (Mux Data Frames over sync bytes):	7	9
R (number of check bytes in FEC Data Frame):	14	14
S (ratio of FEC over PMD Data Frame length):	0.1490	5.8049
L (number of bits in PMD Data Frame):	6820	328
D (interleave depth):	128	8
Delay (msec):	4	11
Super Frames:	16691	16479
Super Frame Errors:	0	0
RS Words:	7244290	185347
RS Correctable Errors:	310	0

# Firewall Configuration

## Firewall

Configure Incoming/Outgoing Filters to either Block or Accept specific data traffic to and from the Internet.



The screenshot shows the Aztech web interface for Firewall Configuration. The top navigation bar includes icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. The main content area is titled "Firewall Settings" and contains the following text:

**Firewall Settings**

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

Meanwhile, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure outgoing/incoming IP filters.

**IP Filtering List**

Filter Name:	<input type="text"/>
Direction:	<input type="text" value="Incoming"/>
Protocol:	<input type="text"/>
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"/>
<input type="checkbox"/> Destination Subnet Mask:	<input type="text"/>
Destination Port (port or port:port):	<input type="text"/>

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

# Port Forwarding

Certain applications need to access a specific port for communication over the network or Internet. You can configure the router to forward incoming and outgoing data transmissions for these applications to be forwarded to a specific port or port range on your computer. By default the router is preconfigured with the port forwarding settings of popular games and applications for easier setup.

**Aztech**

Quick Setup Home Network Configuration Device Status Statistics Firewall Configuration Device Administration

Settings Port Forwarding DMZ

### Port Forwarding

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.

Server Name:

Select a Service:

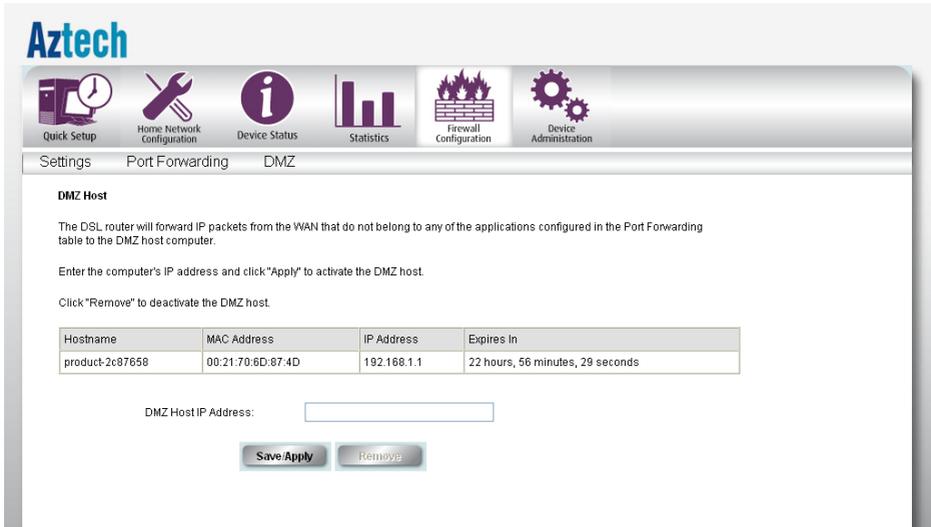
Custom Server:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
		TCP			

# DMZ

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 in Port Forwarding. Enter the LAN IP address of the PC you wish to set as DMZ Host in the DMZ Host IP Address, and then click Save/Apply. If you need to disable the DMZ Host, just click the Remove button.



The screenshot shows the Aztech web interface. At the top, there is a navigation bar with icons for Quick Setup, Home Network Configuration, Device Status, Statistics, Firewall Configuration, and Device Administration. Below this is a sub-menu with 'Settings', 'Port Forwarding', and 'DMZ'. The 'DMZ Host' section contains the following text:

**DMZ Host**

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

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

Click "Remove" to deactivate the DMZ host.

Hostname	MAC Address	IP Address	Expires In
product-2c87658	00:21:70:6D:87:4D	192.168.1.1	22 hours, 56 minutes, 29 seconds

DMZ Host IP Address:

# Device Administration

## System – Backup

You may use this utility to save the router's configuration to a file on your PC. Simply click on the Backup button and choose the folder on your PC where you want the backup file to be saved.



## Restore to Default

Reset the entire router configuration back to the original factory settings by clicking the Restore button.



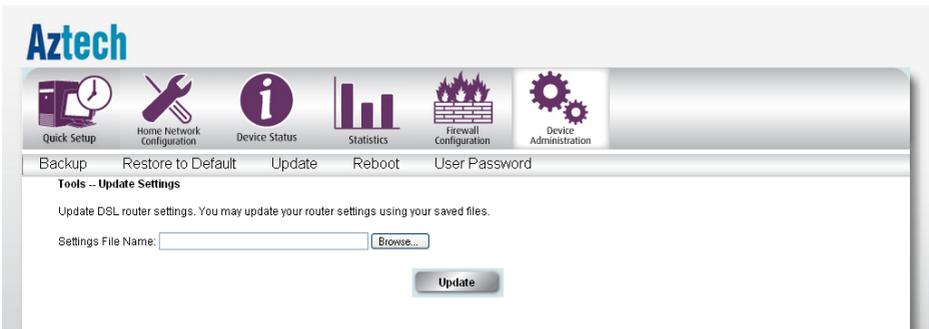
## Update Settings

Update the DSL router settings from a previously stored backup file on a computer.

Procedure:

1. Click on the Browse button.
2. Locate the backupsettings.conf file from your computer.
3. Click Open.
4. Click Update.

The router will update the settings according to the backupsettings.conf file and reboot.



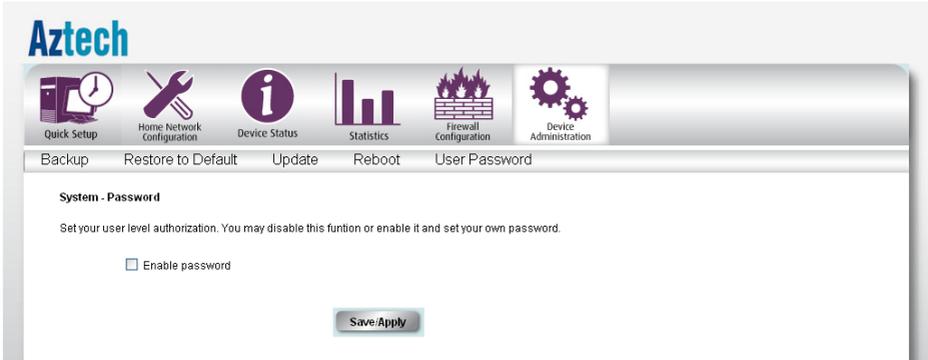
## Reboot

This will automatically save recent changes made on the router and reboot the whole system for the new settings to take effect.



# User Password

Set your user level authorization for additional security on your router. This means that anyone who wants to gain access to your router's GUI needs to key-in the password.



# Admin Mode

Advanced Setup provides configuration options for other router functions.

## Accessing the Admin Mode Web User Interface

To access the Advanced Web Interface:

1. Open your browser.
2. Type-in 192.168.1.254/admin on the address bar and then press Enter.
3. There will be an authentication request where you need to key in a username and password. Default Username: admin | Password: admin
4. Click OK



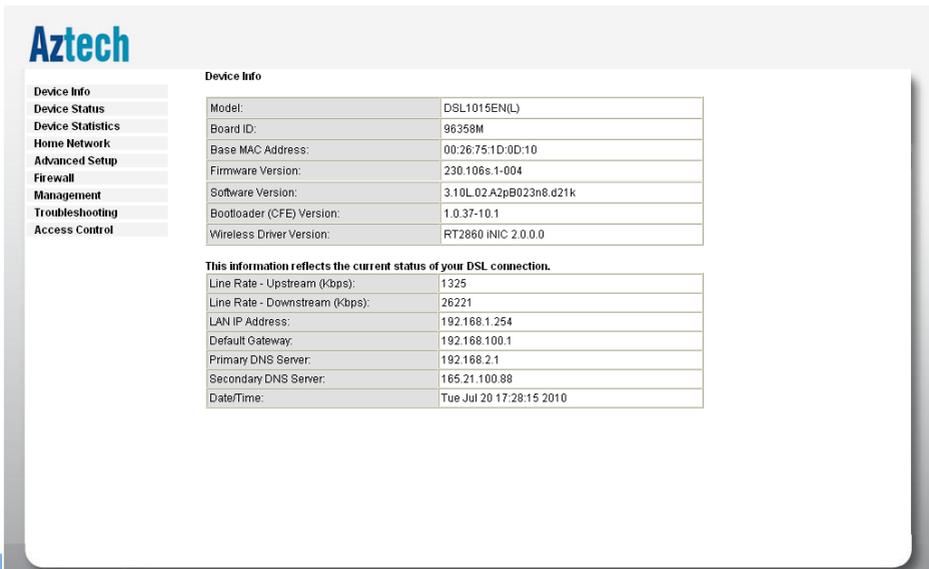
# Menus

The Admin Mode Web User Interface includes the following menus:

- Device Info
- Device Status
- Device Statistics
- Home Network
- Advanced Setup
- Firewall
- Troubleshooting
- Access Control

## Device Info

Includes hardware and software information of your device, the current status of your DSL connection, and the current system date and time.



The screenshot displays the Aztech Admin Mode Web User Interface. On the left, a navigation menu lists various options: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Troubleshooting, and Access Control. The 'Device Info' menu item is highlighted. The main content area shows the 'Device Info' section with a table of hardware and software details. Below this table, a note states 'This information reflects the current status of your DSL connection.' followed by another table showing DSL connection statistics and system information.

Device Info	
Model:	DSL1015EN(L)
Board ID:	98358M
Base MAC Address:	00:26:75:1D:0D:10
Firmware Version:	230.106s.1-004
Software Version:	3.10L.02.A2pB023n8.d21k
Bootloader (CFE) Version:	1.0.37-10.1
Wireless Driver Version:	RT2860 INIC 2.0.0.0

**This information reflects the current status of your DSL connection.**

Line Rate - Upstream (Kbps):	1325
Line Rate - Downstream (Kbps):	26221
LAN IP Address:	192.168.1.254
Default Gateway:	192.168.100.1
Primary DNS Server:	192.168.2.1
Secondary DNS Server:	165.21.100.88
Date/Time:	Tue Jul 20 17:28:15 2010

# Device Status

Shows the current status of different connections such as LAN, DSL, Internet and IPTV. There is a Reserve button that will automatically reserve the current LAN IP address assigned to your PC. You may also reserve a LAN IP address to a specific computer with the use of the Manual device reserve feature.

To Manually reserve a LAN IP address:

1. Key in the PC's MAC address
2. Key in the LAN IP Address you want to assign
3. Key in the Hostname of your PC
4. Click the Add button

**Aztech**

**Device Info**  
Device Status  
Device Statistics  
Home Network  
ARP  
Settings  
WLAN  
Advanced Setup  
Firewall  
Management  
Troubleshooting  
Access Control

**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: 192.168.1.254  
Subnet Mask: 255.255.255.0  
Host Name: Modem  
Domain Name: Home

Disable DHCP Server  
 Enable DHCP Server

Start IP Address: 192.168.1.1  
End IP Address: 192.168.1.253  
Subnet Mask: 255.255.255.0  
Leased Time (hour): 24

Configure the second IP Address and Subnet Mask for LAN interface

Enable Public IP Pass Through  
 Enable UPnP  
 Enable IGMP Snooping  
 Standard Mode  
 Blocking Mode

**Save** **Save/Reboot**

---

**Device Info -- DHCP Leases**

DHCP Server assigned devices:

# Device Statistics

The router will show you detailed statistical information regarding the different connections on your router. This will include statistics for ATM, DSL, Internet, IPTV and your Local Area Network.

**Aztech**

- Device Info
- Device Status
- Device Statistics
- ATM
- DSL
- Internet
- IPTV
- LAN
- Home Network
- Advanced Setup
- Firewall
- Management
- Troubleshooting
- Access Control

**Statistics -- ATM**

**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 OFC Errors
185568	468096	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
185568	468096	988	2423	0	0	0	0

**AAL5 VCC Statistics**

CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0	0	0	0	0

## Home Network

### Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. You may also configure the DHCP server and Public IP Pass Through settings of your router

## DCHP Lease Information

Displays information on the DHCP clients connected to the router.

**Aztech**

**Device Info**  
**Device Status**  
**Device Statistics**  
**Home Network**  
ARP  
**Settings**  
**WLAN**  
**Advanced Setup**  
**Firewall**  
**Management**  
**Troubleshooting**  
**Access Control**

**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: 192.168.1.254  
Subnet Mask: 255.255.255.0  
Host Name: Modem  
Domain Name: Home

Disable DHCP Server  
 Enable DHCP Server

Start IP Address: 192.168.1.1  
End IP Address: 192.168.1.253  
Subnet Mask: 255.255.255.0  
Leased Time (hour): 24

Configure the second IP Address and Subnet Mask for LAN interface

Enable Public IP Pass Through  
 Enable UPnP  
 Enable IGMP Snooping  
 Standard Mode  
 Blocking Mode

**Save** **Save/Reboot**

**Device Info -- DHCP Leases**

DHCP Server assigned devices:

# Advanced Setup

## WAN

The initial page will show all the existing WAN interfaces configured on your router. You have an option to Add, Remove, and Edit WAN interface configurations.

**Aztech**

**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	ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/100	Off	1	UBR	quickstart	ppp_0_0_100_1	PPPoE	Disabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/1/100	Off	1	UBR	IPTV	nas_0_1_100	MER	Enabled	Enabled	Enabled	<input type="checkbox"/>	Edit

**Add** **Remove** **Save/Reboot**

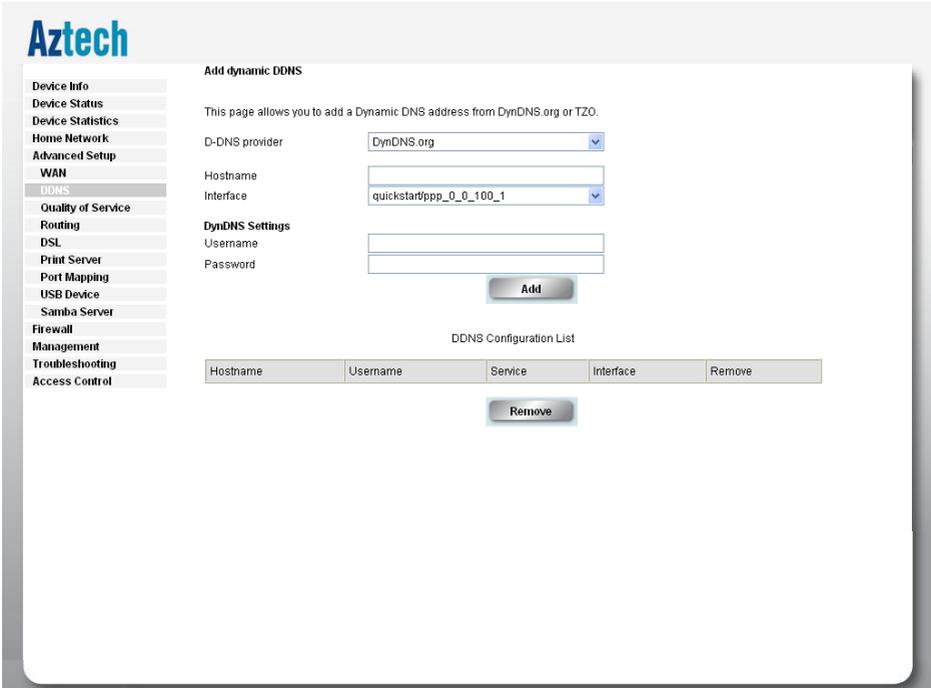
- Device Info
- Device Status
- Device Statistics
- Home Network
- Advanced Setup
- WAN**
- DDNS
- Quality of Service
- Routing
- DSL
- Print Server
- Port Mapping
- USB Device
- Samba Server
- Firewall
- Management
- Troubleshooting
- Access Control

## DDNS

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)



### Using DynDNS.org

1. Key in the following parameters:
  - D-DNS provider Select DynDNS.org
  - Hostname Enter the hostname
  - Interface Select an interface
2. DynDNS Settings Enter your dyndns.org Username and password.

## ***Using TZO***

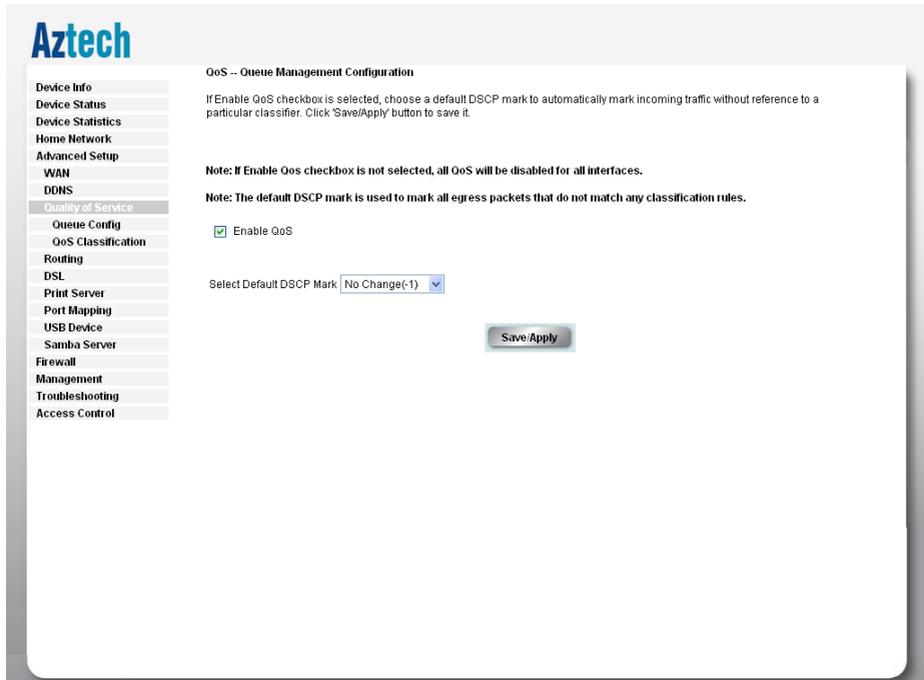
1. Key in the following parameters:
  - D-DNS provider Select TZO
  - Hostname Enter the hostname
  - Interface Select an interface
2. TZO Settings Enter your TZO e-mail and key

## ***To remove a DDNS setting***

1. Put a check on the Remove box
2. Click the Remove button

## Quality of Service

Quality of Service or QoS provides different priority to different applications, users, or data flows, to guarantee a certain level of performance. For example, QoS is important for real-time streaming multimedia applications such as voice over IP, online games and IPTV to provide fixed bit rate and prevent delay.

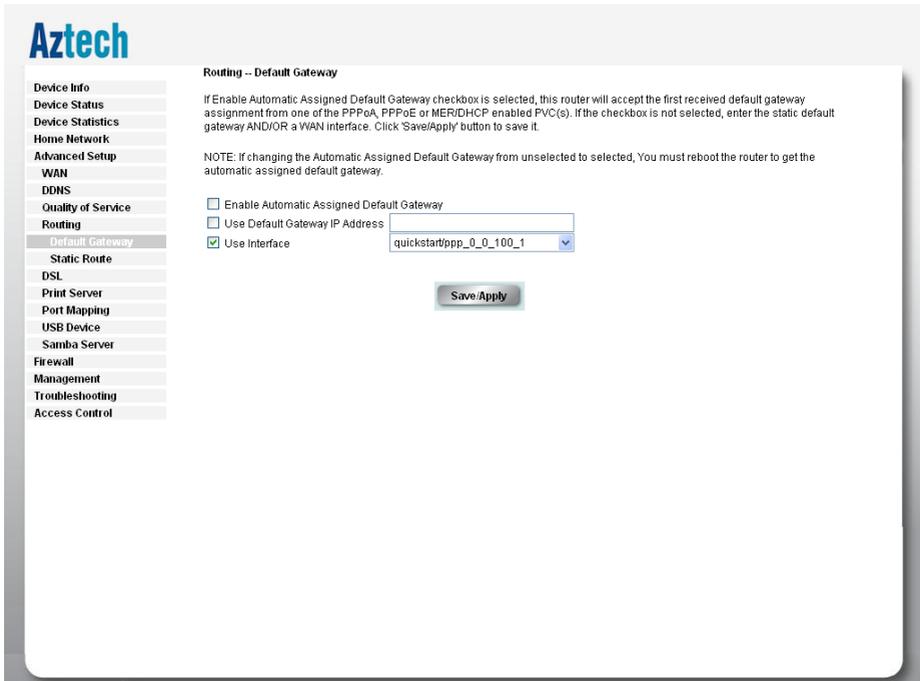


The screenshot displays the Aztech web interface for configuring Quality of Service (QoS). On the left is a navigation menu with the following items: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, WAN, DDNS, Quality of Service (highlighted), Queue Config, QoS Classification, Routing, DSL, Print Server, Port Mapping, USB Device, Samba Server, Firewall, Management, Troubleshooting, and Access Control. The main content area is titled "QoS -- Queue Management Configuration". It contains the following text: "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." Below this is a note: "Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces." Another note states: "Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules." There is a checked checkbox labeled "Enable QoS". Below it is a dropdown menu for "Select Default DSCP Mark" with the value "No Change(-1)". At the bottom right of the configuration area is a "Save/Apply" button.

## Routing – Default Gateway

If Enable Automatic Assigned Default Gateway checkbox is selected, the 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.



## 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.

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.

- Device Info
- Device Status
- Device Statistics
- Home Network
- Advanced Setup
- WAN
- DDNS
- Quality of Service
- Routing
- Default Gateway
- Static Route
- DSL
- Print Server
- Port Mapping
- USB Device
- Samba Server
- Firewall
- Management
- Troubleshooting
- Access Control

## Routing -- Static Route

Enter the destination network address, subnet mask then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface quickstart/ppp\_0\_0\_100\_1 ▾

**Save/Apply**

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

Destination	Subnet Mask	Gateway	Interface	Remove
10.238.0.0	255.255.0.0		nas_0_1_100	<input type="checkbox"/>
10.239.0.0	255.255.0.0		nas_0_1_100	<input type="checkbox"/>
10.197.0.0	255.255.0.0		nas_0_1_100	<input type="checkbox"/>
10.198.0.0	255.255.0.0		nas_0_1_100	<input type="checkbox"/>
10.199.0.0	255.255.0.0		nas_0_1_100	<input type="checkbox"/>

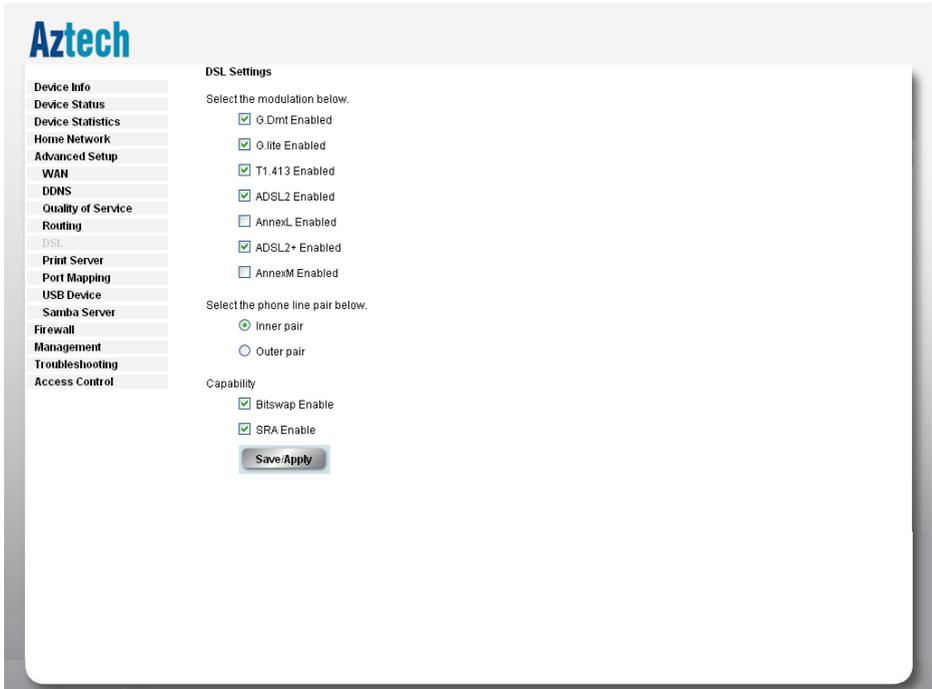
**Remove**

Click Save/Apply to save the settings.

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

# DSL Settings

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



# Port Mapping

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.

**Aztech**

- Device Info
- Device Status
- Device Statistics
- Home Network
- Advanced Setup
- WAN
- DDNS
- Quality of Service
- Routing
- DSL
- Print Server
- Port Mapping
- USB Device
- Samba Server
- Firewall
- Management
- Troubleshooting
- Access Control

**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.

Enable virtual ports on

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default				eth0	<input checked="" type="checkbox"/>
				Wireless	<input checked="" type="checkbox"/>
				eth1.2	<input checked="" type="checkbox"/>
				eth1.3	<input checked="" type="checkbox"/>
				eth1.4	<input checked="" type="checkbox"/>

**Save/Apply**

Group Name:

**Grouped Interfaces**

->  
<-

**Available Interfaces**

eth0  
eth1.2  
eth1.3  
eth1.4  
Wireless

**Automatically Add Clients With the following DHCP Vendor IDs**

DHCP Vendor ID 1:

# Firewall

## 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.

**Aztech**

**Device Info**  
Device Status  
Device Statistics  
Home Network  
Advanced Setup  
Firewall  
IP Filtering  
Parental Control  
TCP/IP Session  
Port Forwarding  
Port Triggering  
DMZ Host  
Management  
Troubleshooting  
Access Control

**IP Filtering Setup**

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

Meanwhile, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure outgoing/incoming IP filters.

**IP Filtering List**

Filter Name:

Direction:

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 only)**  
Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

quickstart/ppp\_0\_0\_100\_1

Filter Name	Direction	Interface	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	-----------	-----------	----------	-----------------------	-------------	----------------------	------------	--------

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 save 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.

## 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.

**Aztech**

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

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:

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):

**Save/Apply**

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
											<b>Remove</b>

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).

## TCP/IP Sessions

**Aztech**

- Device Info
- Device Status
- Device Statistics
- Home Network
- Advanced Setup
- Firewall
- IP Filtering
- Parental Control
- TCP/IP Session
- Port Forwarding
- Port Triggering
- DMZ Host
- Management
- Troubleshooting
- Access Control

**TCP/IP sessions**

Note/When a connection has seen traffic in both directions, the conntrack entry will erase the [UNREPLIED] flag, and then reset it. The [ASSURED] flag tells us that this connection is assured and that it will not be erased if we reach the maximum possible tracked connections. Thus, connections marked as [ASSURED] will not be erased.

tcp/ftp sessions(used/available): 36/1000

Protocol	Time Out	SourceIP/Port (Outgress)	DestIP/Port (Outgress)	Status	DestIP/Port (Ingress)	Status	use
tcp/6	53	192.168.1.1/3366	192.168.1.254/80	-	192.168.1.1/3366	[ASSURED]	1
tcp/6	31	192.168.1.1/3358	192.168.1.254/80	-	192.168.1.1/3358	[ASSURED]	1
tcp/6	89	192.168.1.1/3373	192.168.1.254/80	-	192.168.1.1/3373	[ASSURED]	1
tcp/6	431992	192.168.1.1/3189	192.168.1.254/139	-	192.168.1.1/3189	[ASSURED]	1
tcp/6	31	192.168.1.1/3362	192.168.1.254/80	-	192.168.1.1/3362	[ASSURED]	1
tcp/6	119	192.168.1.1/3385	192.168.1.254/80	-	192.168.1.1/3385	[ASSURED]	1
tcp/6	31	192.168.1.1/3360	192.168.1.254/80	-	192.168.1.1/3360	[ASSURED]	1
tcp/6	89	192.168.1.1/3375	192.168.1.254/80	-	192.168.1.1/3375	[ASSURED]	1
tcp/6	119	192.168.1.1/3388	192.168.1.254/80	-	192.168.1.1/3388	[ASSURED]	1
tcp/6	53	192.168.1.1/3365	192.168.1.254/80	-	192.168.1.1/3365	[ASSURED]	1
tcp/6	431964	192.168.1.1/3023	72.241.224.254/62457	-	192.168.100.7/3023	[ASSURED]	1
tcp/6	53	192.168.1.1/3364	192.168.1.254/80	-	192.168.1.1/3364	[ASSURED]	1
tcp/6	77	192.168.1.1/3368	192.168.1.254/80	-	192.168.1.1/3368	[ASSURED]	1
tcp/6	119	192.168.1.1/3390	192.168.1.254/80	-	192.168.1.1/3390	[ASSURED]	1
tcp/6	107	192.168.1.1/3382	192.168.1.254/80	-	192.168.1.1/3382	[ASSURED]	1
tcp/6	77	192.168.1.1/3372	192.168.1.254/80	-	192.168.1.1/3372	[ASSURED]	1
tcp/6	90	192.168.1.1/3377	192.168.1.254/80	-	192.168.1.1/3377	[ASSURED]	1
tcp/6	119	192.168.1.1/3389	192.168.1.254/80	-	192.168.1.1/3389	[ASSURED]	1
tcp/6	89	192.168.1.1/3376	192.168.1.254/80	-	192.168.1.1/3376	[ASSURED]	1
tcp/6	431999	192.168.1.1/3391	192.168.1.254/80	-	192.168.1.1/3391	[ASSURED]	1
tcp/6	107	192.168.1.1/3379	192.168.1.254/80	-	192.168.1.1/3379	[ASSURED]	1
tcp/6	77	192.168.1.1/3370	192.168.1.254/80	-	192.168.1.1/3370	[ASSURED]	1
tcp/6	107	192.168.1.1/3383	192.168.1.254/80	-	192.168.1.1/3383	[ASSURED]	1
tcp/6	89	192.168.1.1/3374	192.168.1.254/80	-	192.168.1.1/3374	[ASSURED]	1
tcp/6	90	192.168.1.1/3378	192.168.1.254/80	-	192.168.1.1/3378	[ASSURED]	1
unknown/?	531	192.168.1.254/6	724.0.0.1/6	[UNREPLIED]	192.168.1.254/6	-	1

# Port Forwarding

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

**Aztech**

**Device Info**  
Device Status  
Device Statistics  
Home Network  
Advanced Setup  
Firewall  
IP Filtering  
Parental Control  
TCP/IP Session  
Port Forwarding  
Port Triggering  
DMZ Host Management  
Troubleshooting  
Access Control

**Port Forwarding**

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.

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
		TCP			

**Save/Apply**

Remaining number of entries that can be configured:32

**Port Forwarding list**

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 Port Forwarding rule.

# Port Triggering

Some applications require that the remote parties open the specific ports in the router's firewall for access. 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 that initiated the request. A maximum of 32 entries can be configured.

**Aztech**

**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:  
 Select an application:   
 Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

**Save/Apply**

Remaining number of entries that can be configured: 32

**Port Triggering list**

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

**Remove**

# 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 in Port Forwarding. Enter the LAN IP address of the PC you wish to set as DMZ Host in the provided box. If you need to disable the DMZ Host, just click the remove button.

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

The screenshot shows the Aztech router's web interface. On the left is a navigation menu with the following items: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, IP Filtering, Parental Control, TCP/IP Session, Port Forwarding, Port Triggering, DMZ Host (highlighted), Management, Troubleshooting, and Access Control. The main content area is titled "DMZ Host" and contains the following text: "The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer." and "Enter the computer's IP address and click 'Apply' to activate the DMZ host." Below this is a table with the following data:

Hostname	MAC Address	IP Address	Expires In
product-2c87658	00:21:70:6D:87:4D	192.168.1.1	21 hours, 49 minutes, 49 seconds

Below the table, there is a label "DMZ Host IP Address:" followed by an empty text input field. At the bottom of the configuration area are two buttons: "Save/Apply" and "Remove".

# Management

## Firmware Upgrade

Allow you to update the firmware of your router.

To Update the router's firmware:

1. Click Browse
2. Choose the firmware file and click OK
3. Click the Upload button

**Aztech**

**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.

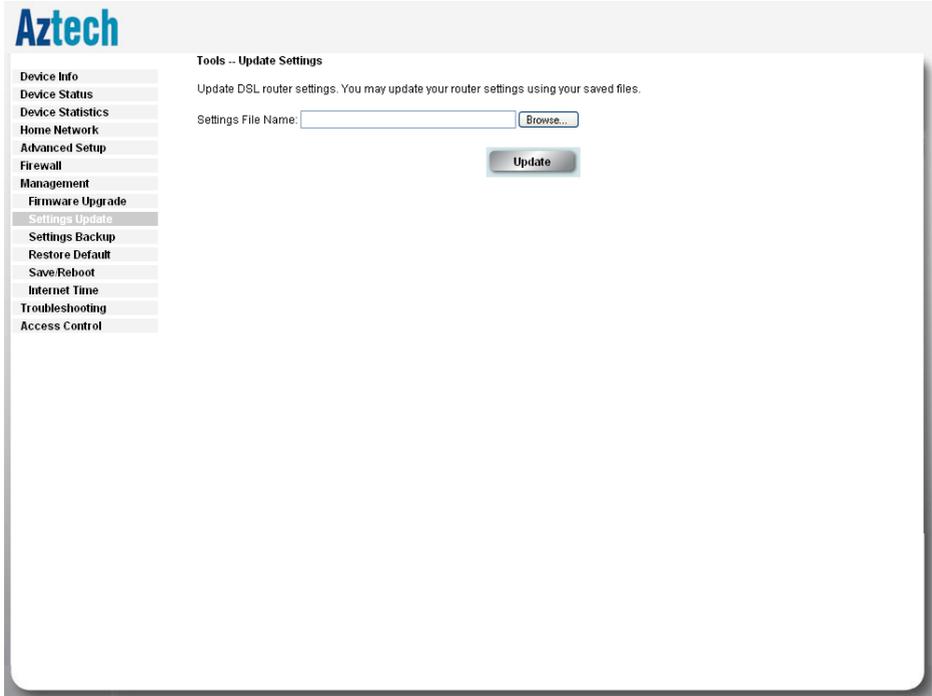
**Step 3:** Click the "Update Software" button once to upload the new image file.

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

Software File Name:

# Settings Update

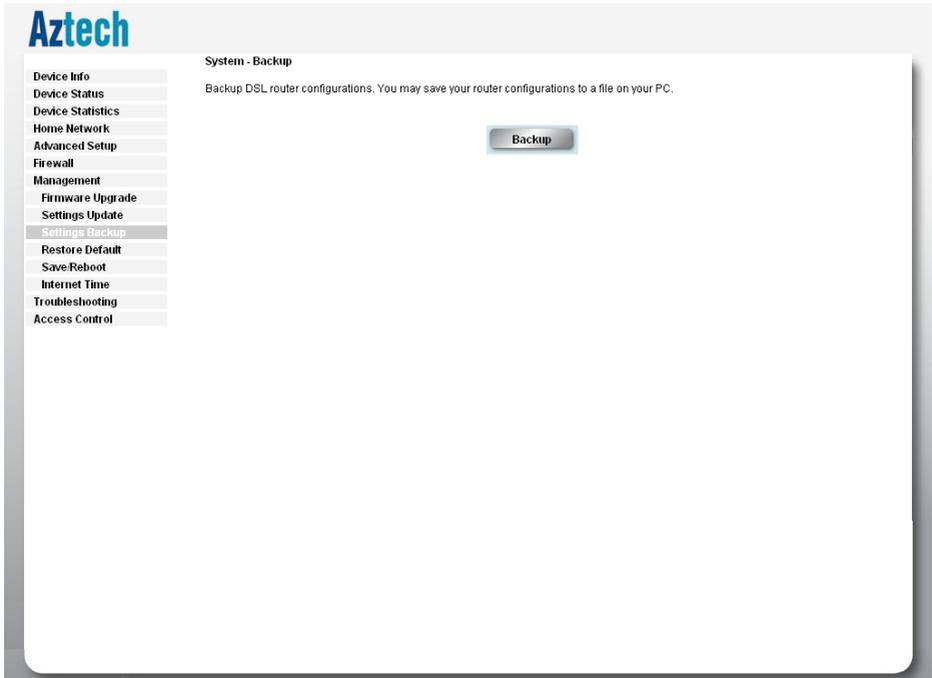
To import a previously saved configuration file from your PC and update the settings of your router, click Browse to locate the backupsettings.conf upgrade file. Then click the Update button.



# Settings Backup

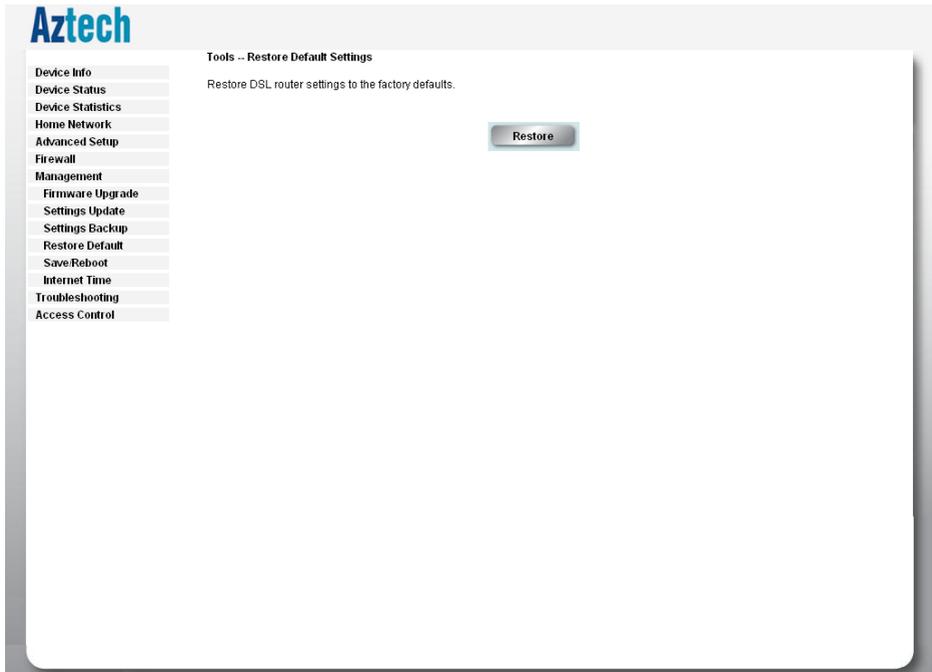
To backup the settings as a configuration file saved on your PC, click the Backup button.

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



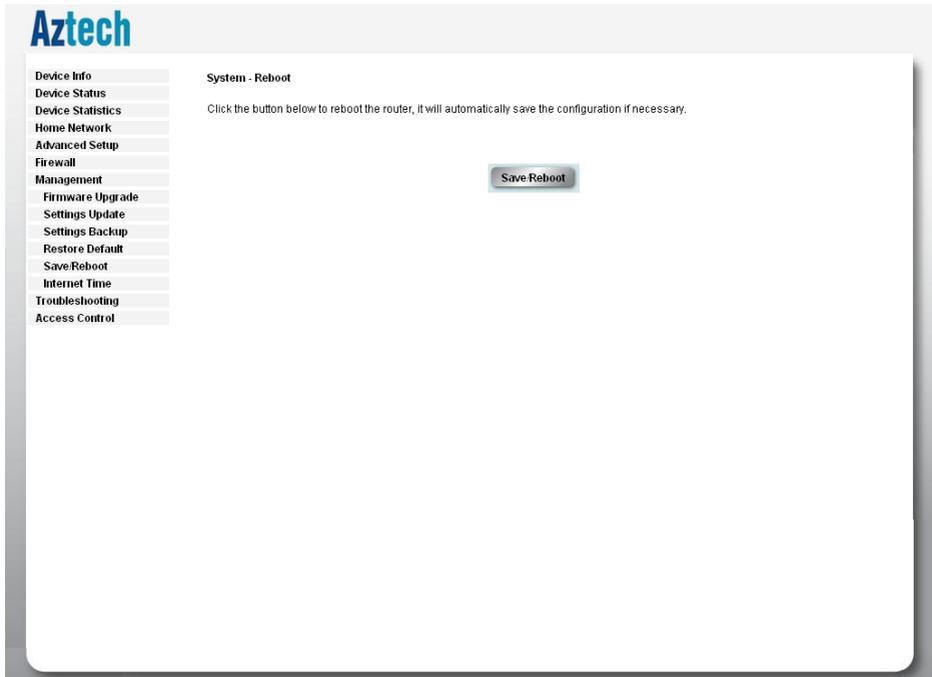
## Restore Default

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



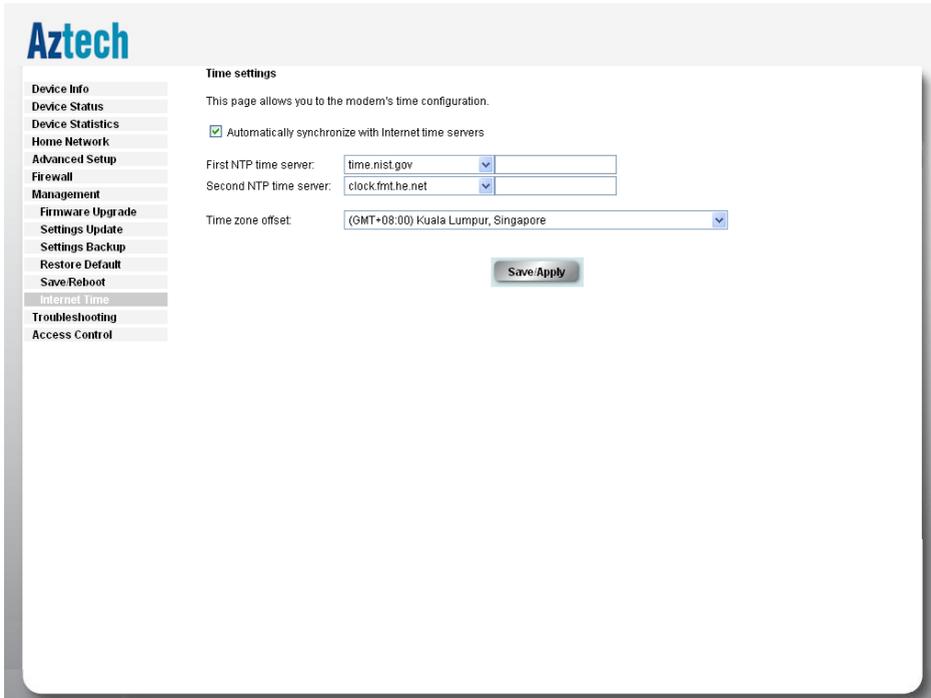
## Save/Reboot

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



# Internet Time

Enable Internet Time to automatically synchronize your modem's time with a time-server when connected to the Internet.



The screenshot shows the Aztech modem's web interface. On the left is a navigation menu with the following items: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Firmware Upgrade, Settings Update, Settings Backup, Restore Default, Save/Reboot, Internet Time (highlighted), Troubleshooting, and Access Control. The main content area is titled "Time settings" and contains the following text: "This page allows you to the modem's time configuration." Below this is a checked checkbox labeled "Automatically synchronize with Internet time servers". There are three input fields: "First NTP time server:" with a dropdown menu showing "time.nist.gov", "Second NTP time server:" with a dropdown menu showing "clock.fmt.he.net", and "Time zone offset:" with a dropdown menu showing "(GMT+08:00) Kuala Lumpur, Singapore". At the bottom right of the settings area is a "Save/Apply" button.

# Troubleshooting

## System Log

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

**Aztech**

**System Log -- Configuration**

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log:  Disable  Enable

Log Level:

Display Level:

Mode:

**Save/Apply**

**System Log**

Date/Time	Facility	Severity	Message
Jul 20 17:18:52	user	err	kernel: sda: assuming drive cache: write through
Jan 1 01:05:47	daemon	crit	pppd[1236]: Received valid IP address from server. Connection UP.
Jan 1 01:05:47	daemon	crit	pppd[1236]: PPP LCP UP.
Jan 1 01:05:47	daemon	crit	pppd[1236]: PPP session established.
Jan 1 01:05:47	daemon	crit	pppd[1236]: PPP server detected.
Jan 1 01:02:03	user	crit	kernel: ADSL link up, Path 0, us=1325, ds=26221
Jan 1 01:02:03	user	crit	kernel: ADSL G.992 message exchange
Jan 1 01:01:55	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 01:01:51	user	crit	kernel: ADSL G.992 started
Jan 1 01:01:43	user	crit	kernel: xDSL G.994 training
Jan 1 01:01:15	user	crit	kernel: ADSL link down
Jan 1 01:01:09	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 01:01:05	user	crit	kernel: ADSL G.992 started
Jan 1 01:00:56	user	crit	kernel: xDSL G.994 training
Jan 1 00:03:08	user	crit	kernel: eth0 Link UP.

# 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.

**Aztech**

**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 eth1.2 Connection:	FAIL	<a href="#">Help</a>
Test your eth1.3 Connection:	FAIL	<a href="#">Help</a>
Test your eth1.4 Connection:	FAIL	<a href="#">Help</a>
Test your eth0 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:	FAIL	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping:	FAIL	<a href="#">Help</a>

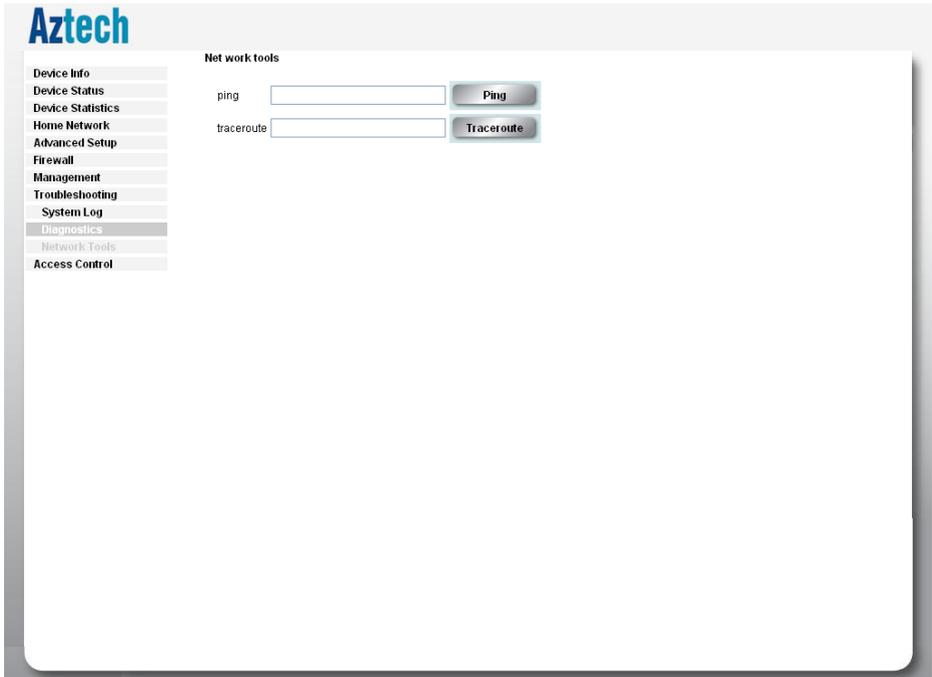
Test the connection to your Internet service provider

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>

[Next](#)   [Test](#)   [Test oam F4](#)

# Network Tools

Network tools will help you troubleshoot Internet connection problems by verifying your connection.



# Access Control

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

## Services

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

**Aztech**

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	<input type="checkbox"/> 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

**Save/Apply**

The screenshot shows the Aztech router's web interface. On the left is a sidebar menu with options: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Troubleshooting, Access Control (selected), Services, and Passwords Settings. The main content area is titled 'Access Control -- Services' and contains a table for configuring service access. The table has three columns: 'Services', 'LAN', and 'WAN'. Each row represents a service with checkboxes and the word 'Enable' for each interface. Below the table is a 'Save/Apply' button.

## Password Settings

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.

The screenshot shows the Aztech router's web interface. On the left is a navigation menu with the following items: Device Info, Device Status, Device Statistics, Home Network, Advanced Setup, Firewall, Management, Troubleshooting, Access Control, Services, and Passwords Settings (which is highlighted). The main content area is titled 'Access Control - Passwords'. It contains the following text: 'Access to your DSL router is controlled through three user accounts: admin, support, and user.' followed by three paragraphs explaining the roles of 'admin', 'support', and 'user'. Below this is a note: 'Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.' There are four input fields: 'Username:' (a dropdown menu), 'Old Password:', 'New Password:', and 'Confirm Password:'. A 'Save/Apply' button is located at the bottom of the form.

# 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.

