Aztech

innovate to connect

USER MANUAL v1.0

DSL1015EN(L)

4 Port ADSL 2/2+ Wireless N Modem Router

LIMITATION OF LIABILITY AND DAMAGES

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

Table of Contents

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

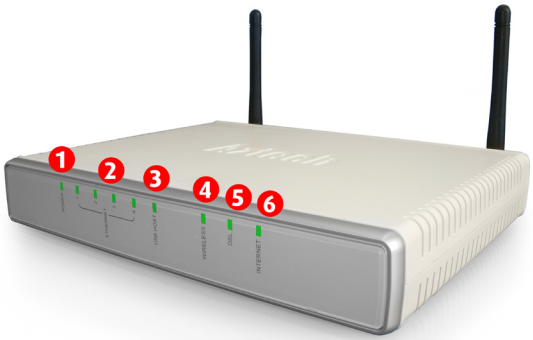
Package Contents

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

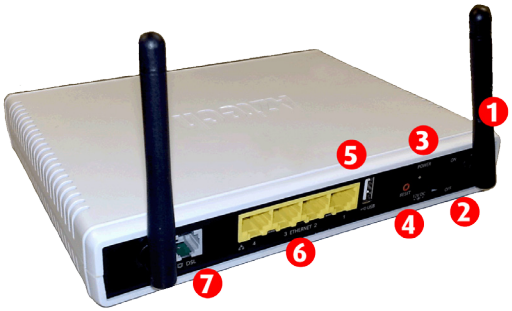
Device Overview

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

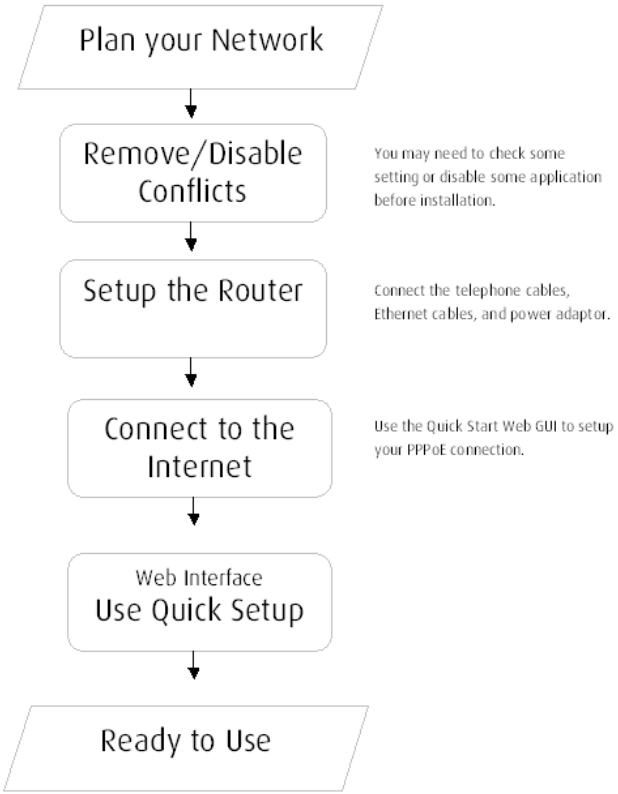
Back Panel



	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

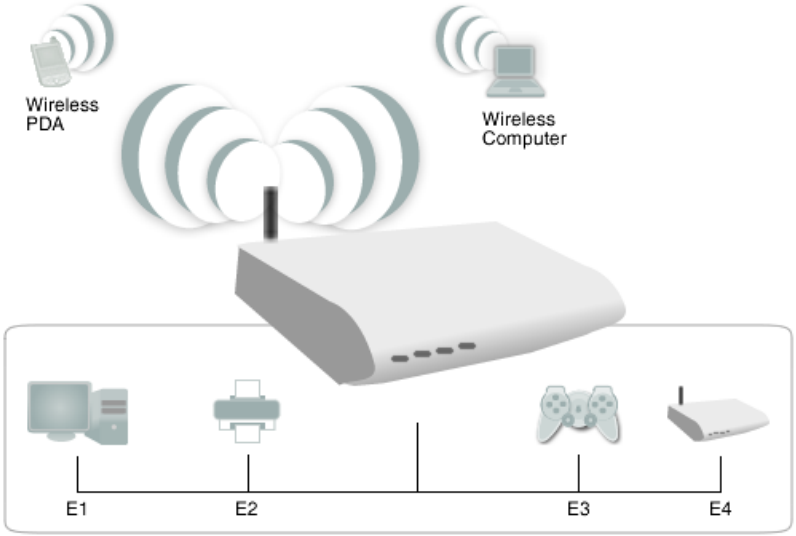
Getting Started

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 inetcpl.cpl and then click OK. This opens Internet Properties.
3. Click Connections tab.
4. In the Dial-up and Virtual Private Network settings pane, select Never dial a connection.
5. Click OK to close Internet Properties.

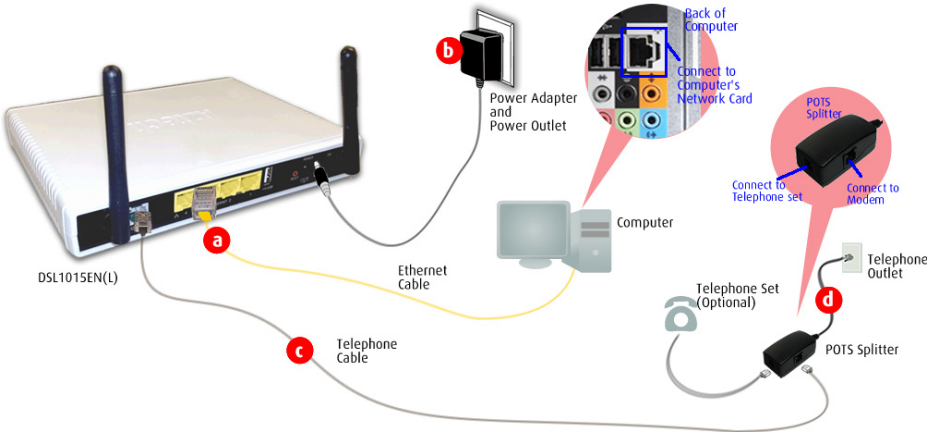
Removing Temporary Internet Files

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

To remove temporary Internet files:

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

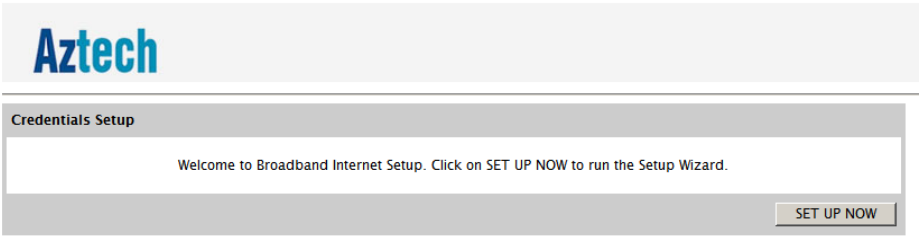
Hardware Setup



Connecting to the Internet

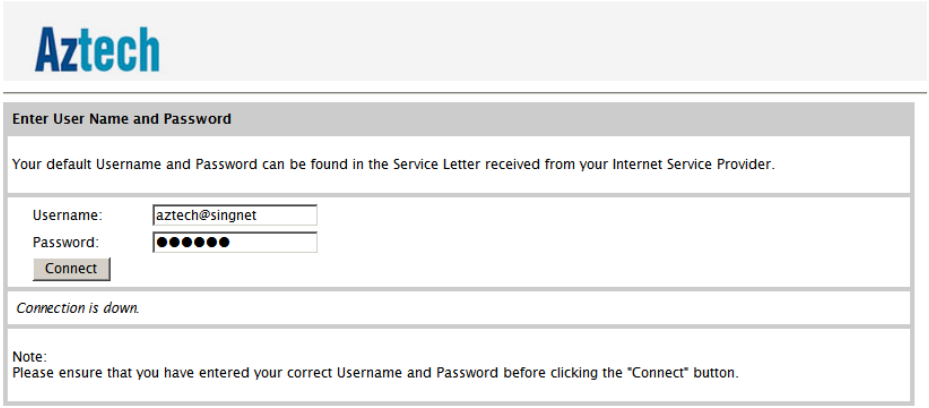
Connecting via Quick Setup

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



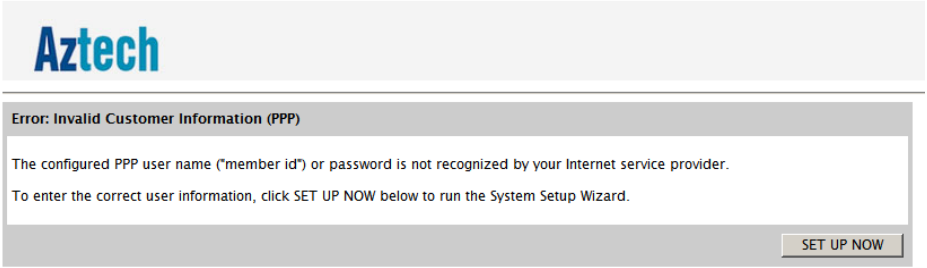
2. Input the username and password provided by the Internet Provider, and click on Connect.

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



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.

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



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.

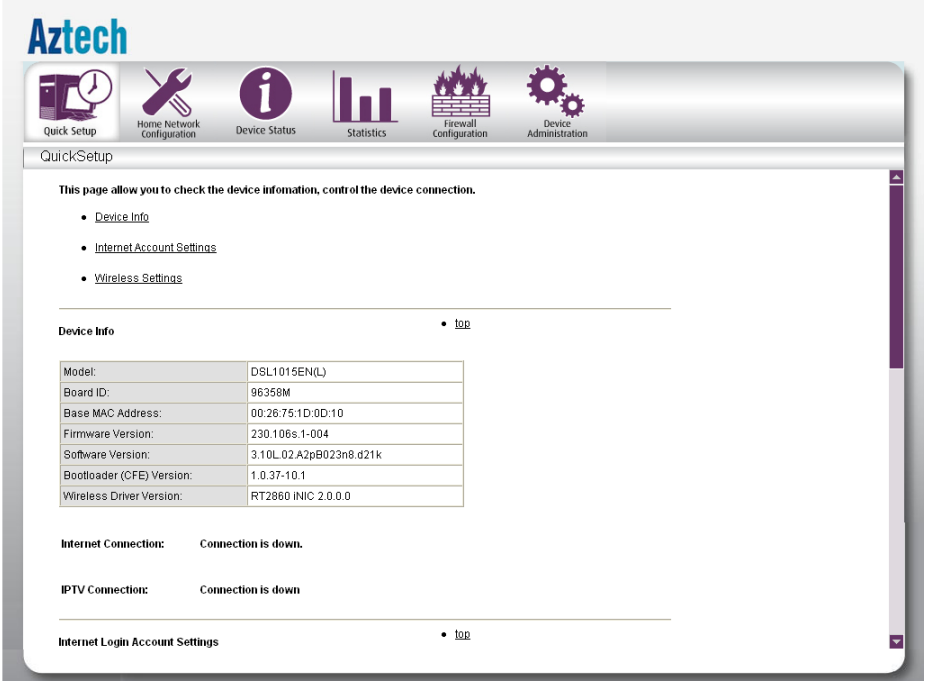
Menus

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.

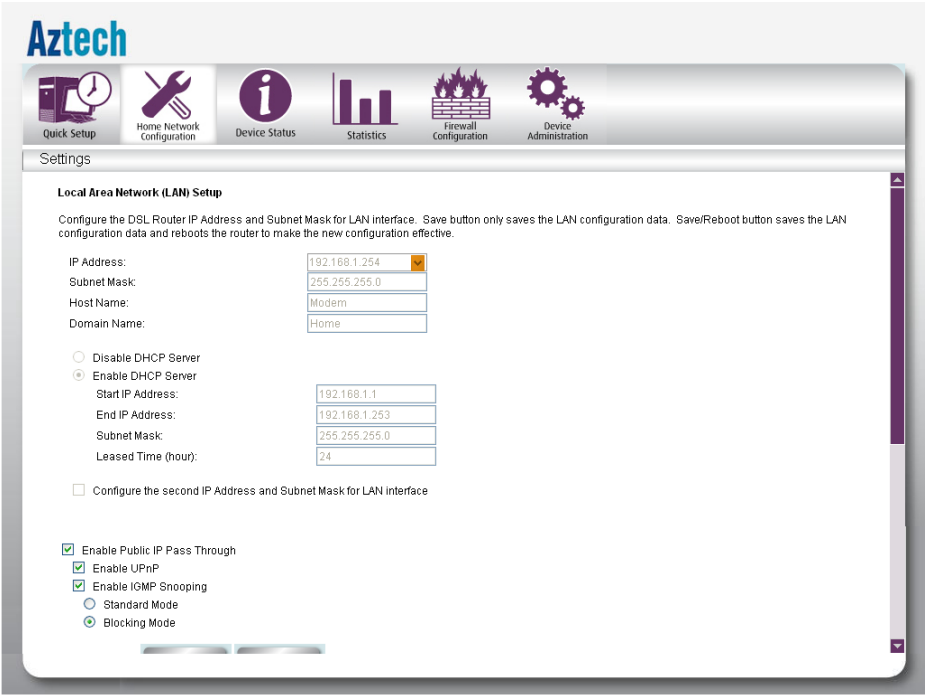


Home Network Configuration

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.

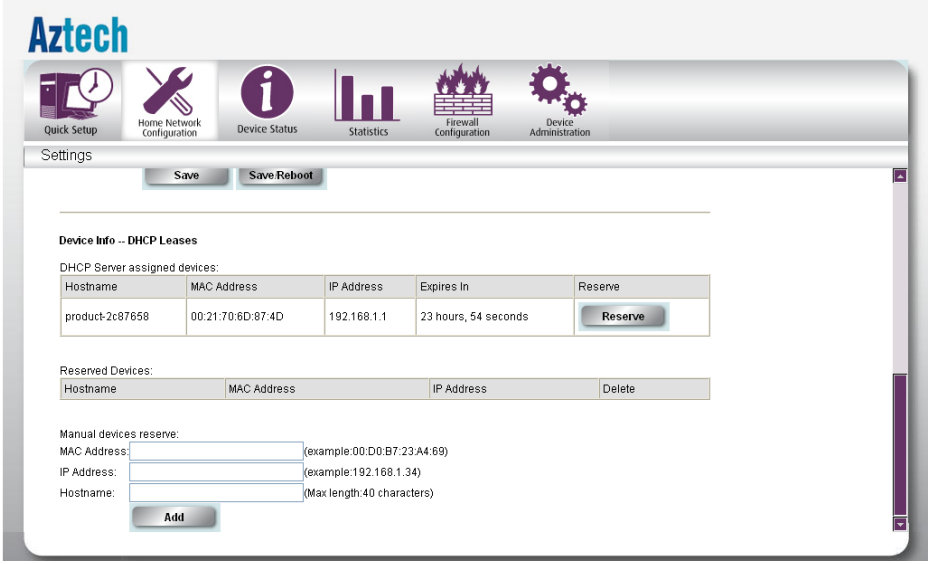
Local Area Network (LAN) Setup

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.



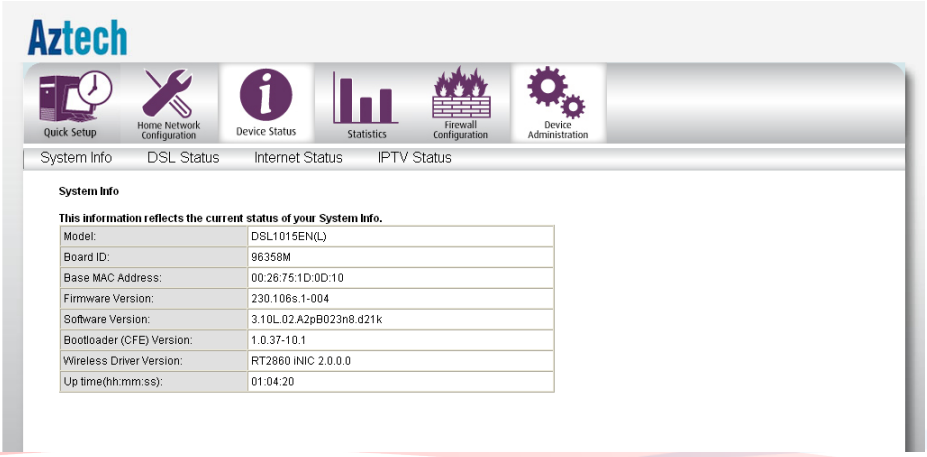
DCHP Lease Information

Displays information on the DHCP clients connected to the router.



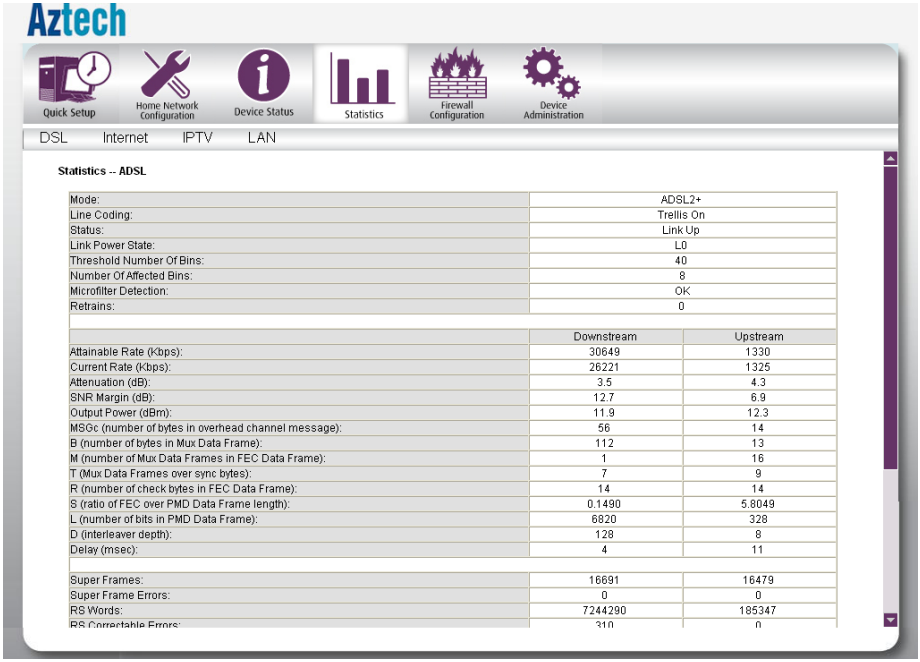
Device Status

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



Statistics

Displays the statistics of different connections on your router.



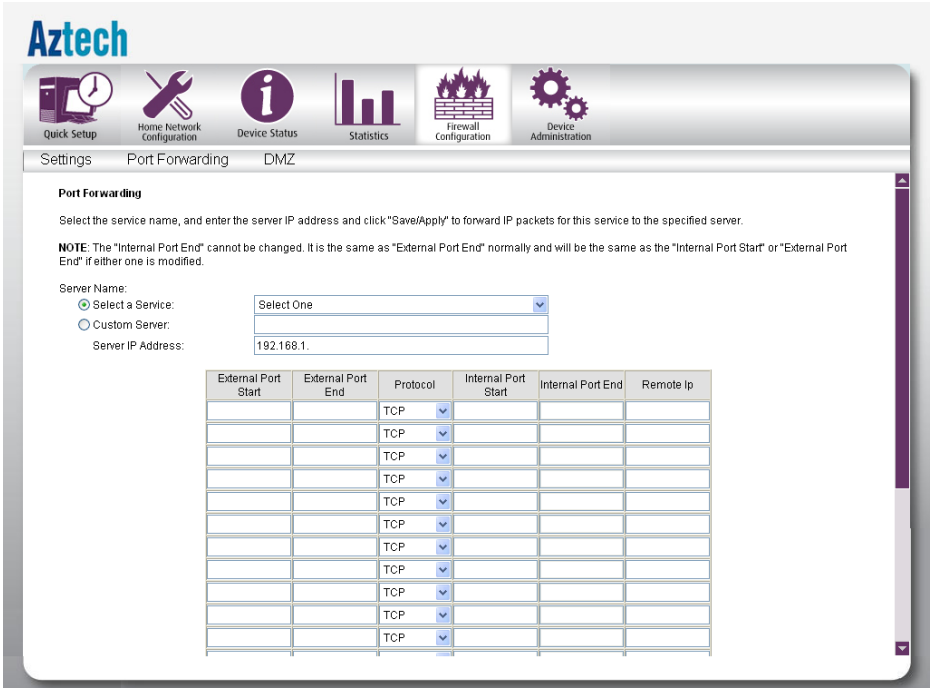
Firewall Configuration

Firewall

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

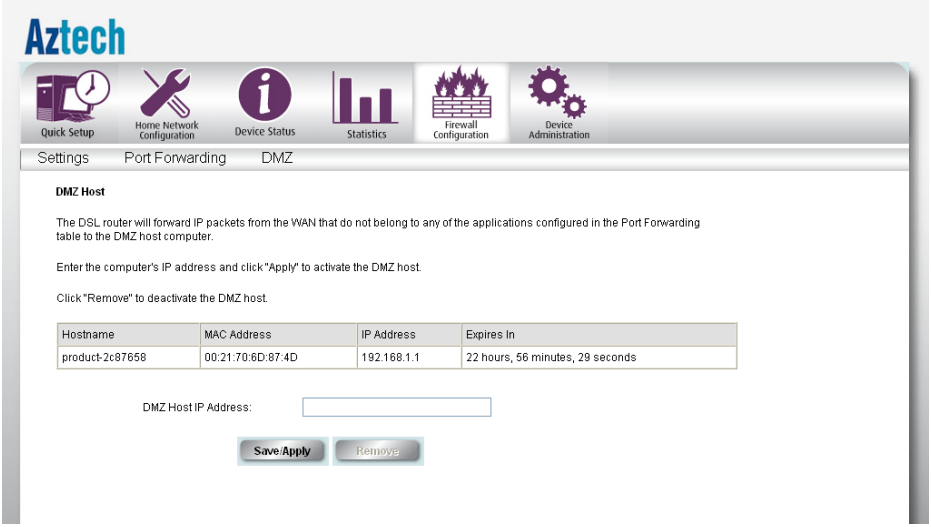
Port Forwarding

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.



DMZ

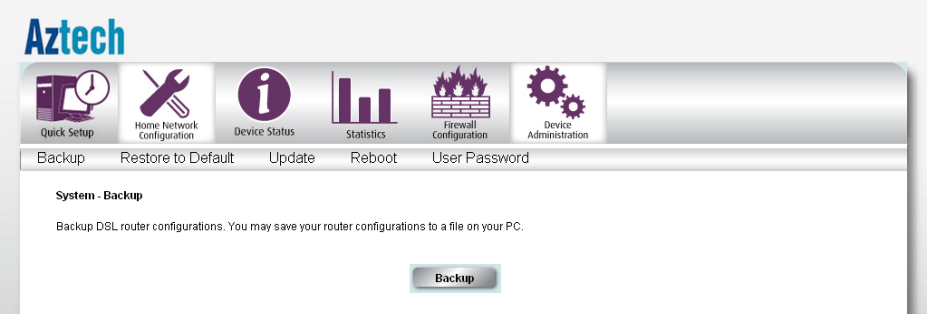
If a computer is assigned as a DMZ Host, it will receive all the data from the Internet that do not belong to the list of applications configured in Port Forwarding. Enter the LAN IP address of the PC you wish to set as DMZ Host in the DMZ Host IP Address, and then click Save/Apply. If you need to disable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



Device Administration

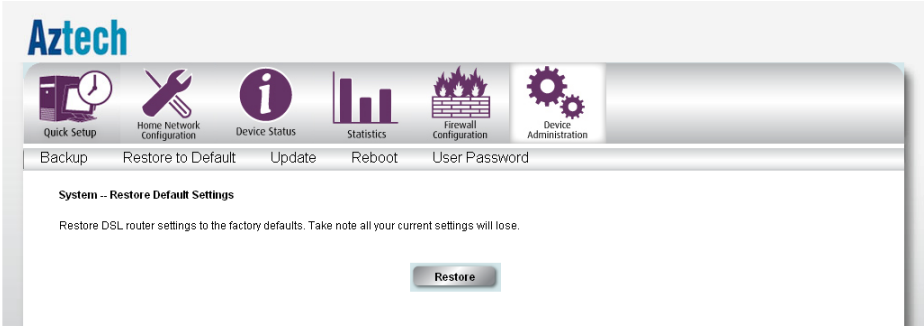
System – Backup

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.



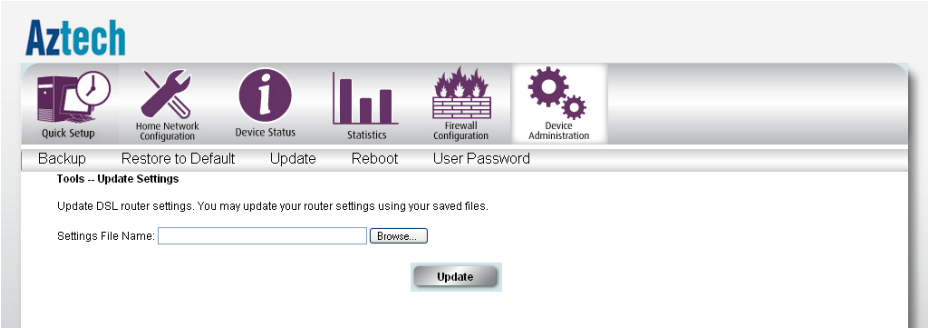
Update Settings

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

Procedure:

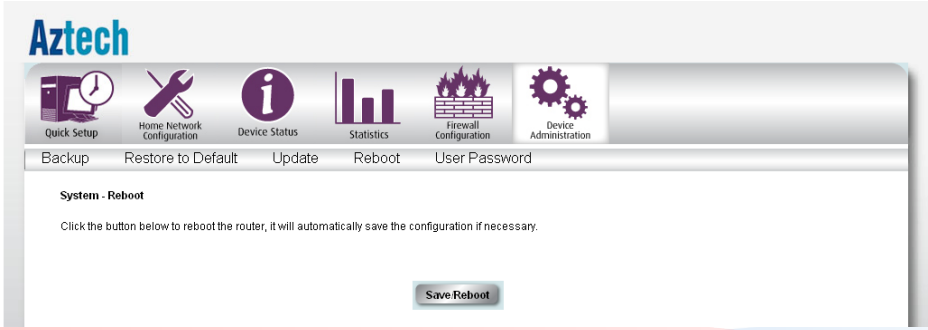
1. Click on the Browse button.
2. Locate the backupsettings.conf file from your computer.
3. Click Open.
4. Click Update.

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



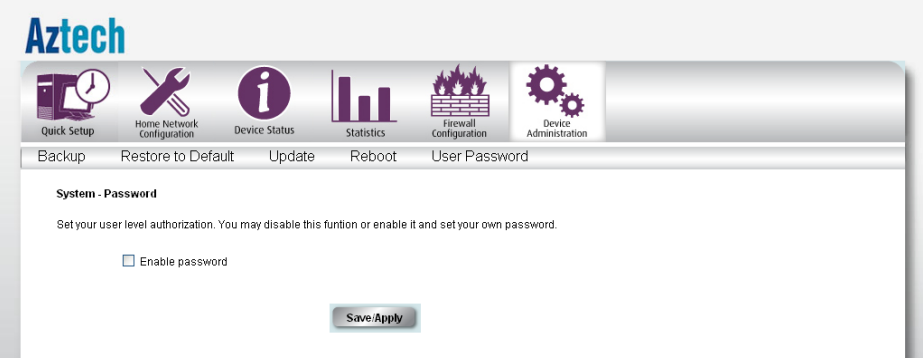
Reboot

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.



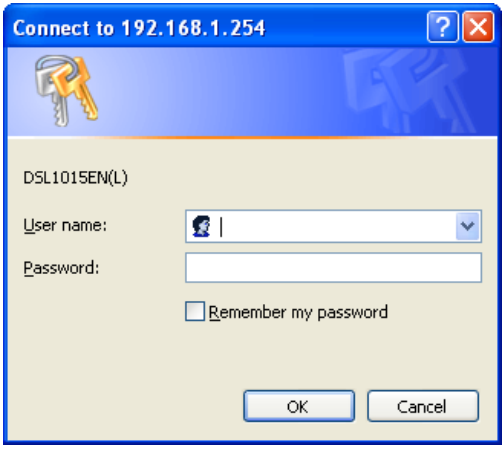
Admin Mode

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



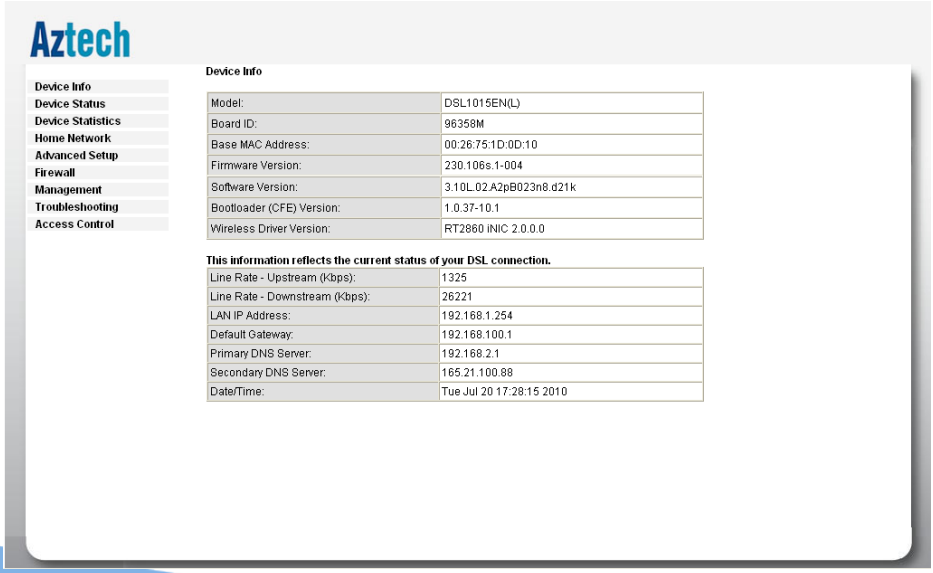
Menus

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.

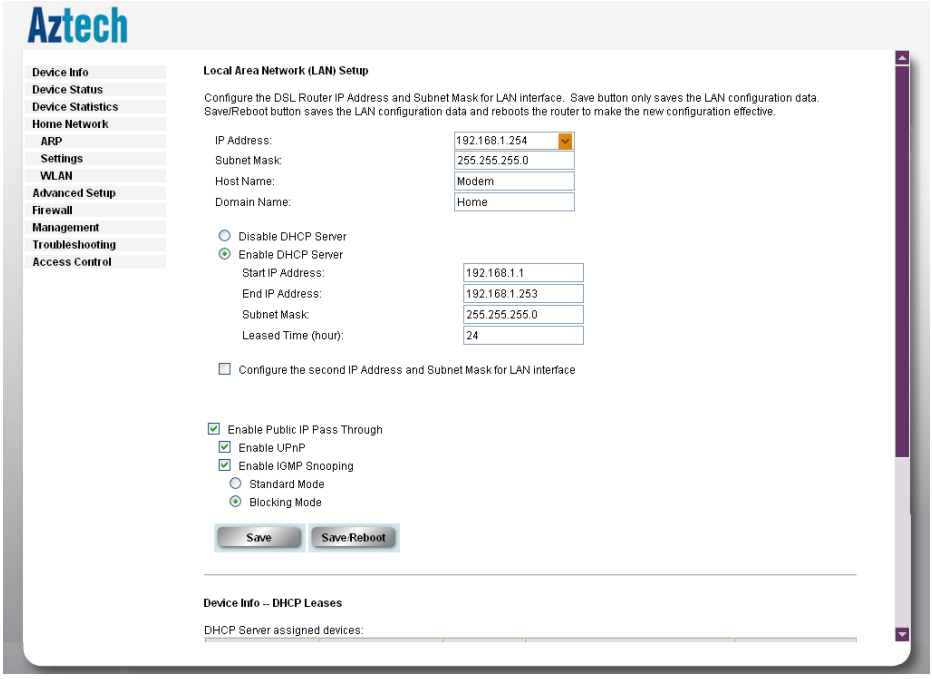


Device Status

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.

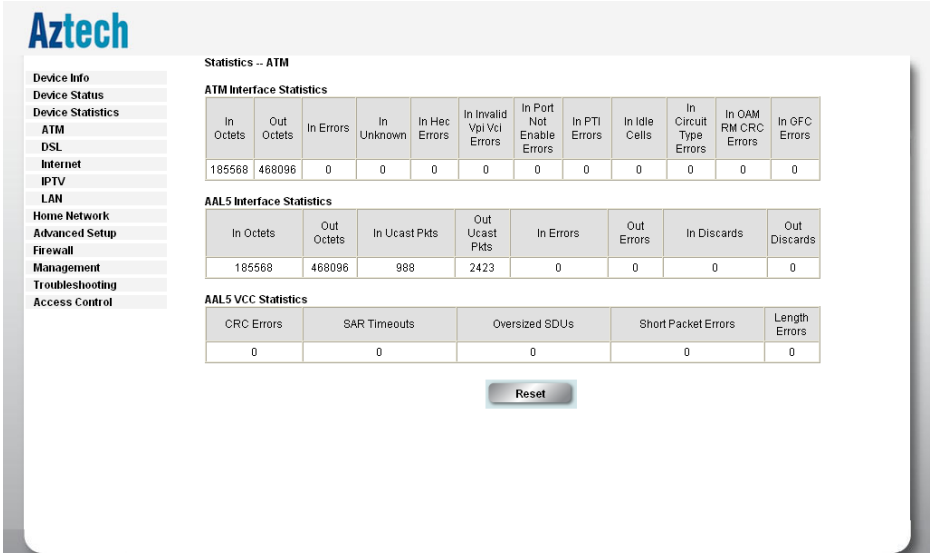
To Manually reserve a LAN IP address:

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



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.



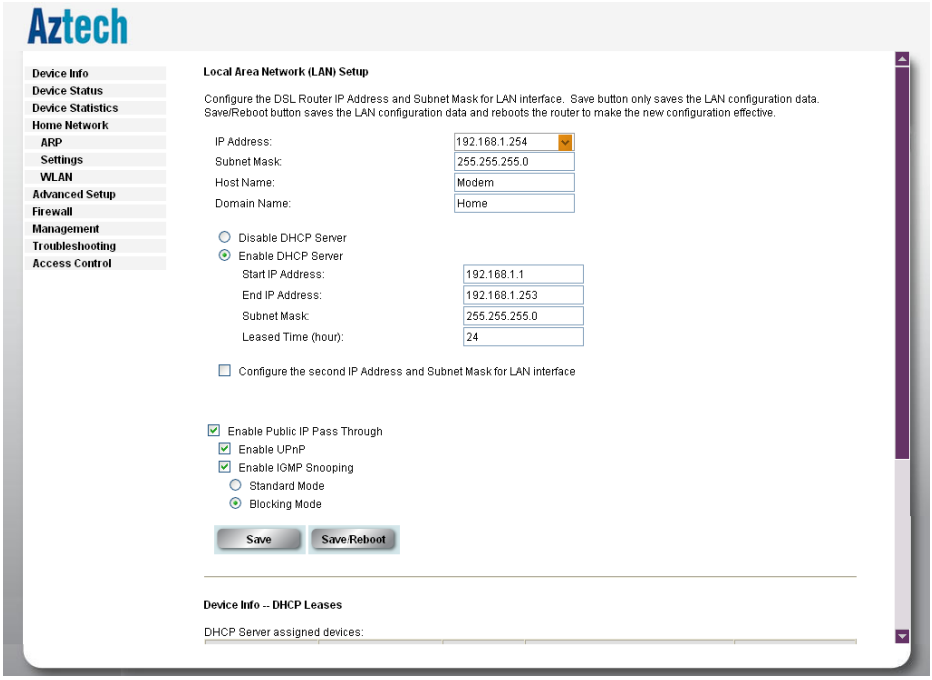
Home Network

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

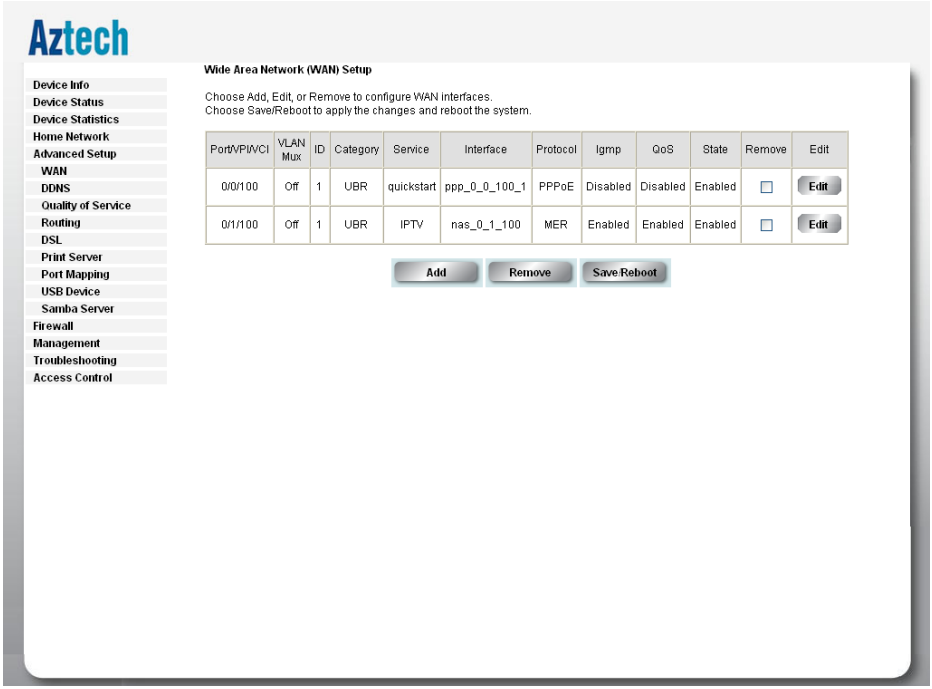
DCHP Lease Information

Displays information on the DHCP clients connected to the router.



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.

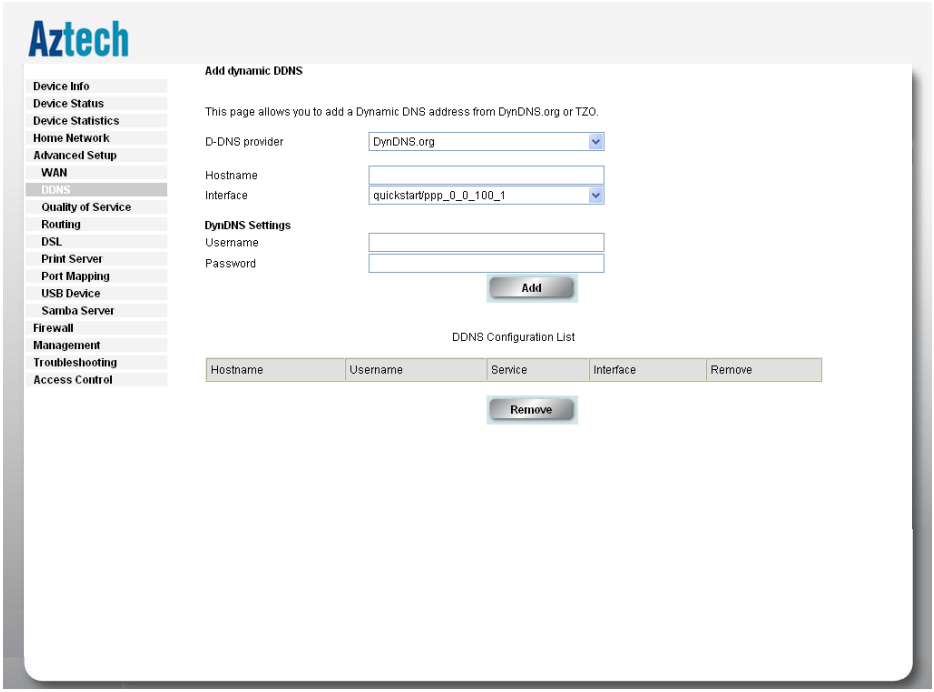


DDNS

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
- 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

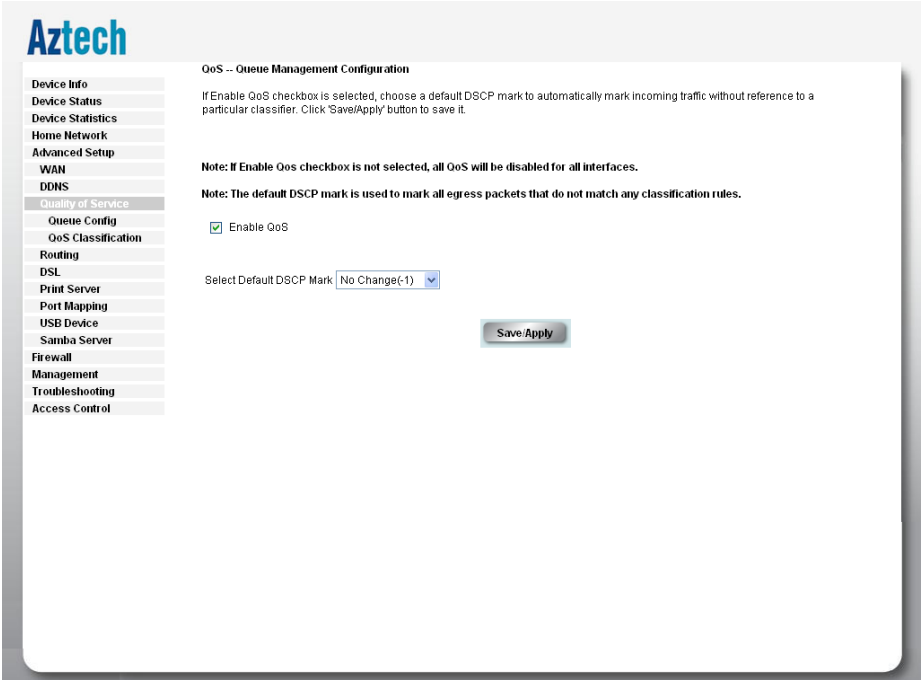
2. TZO Settings Enter your TZO e-mail and key

To remove a DDNS setting

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

Quality of Service

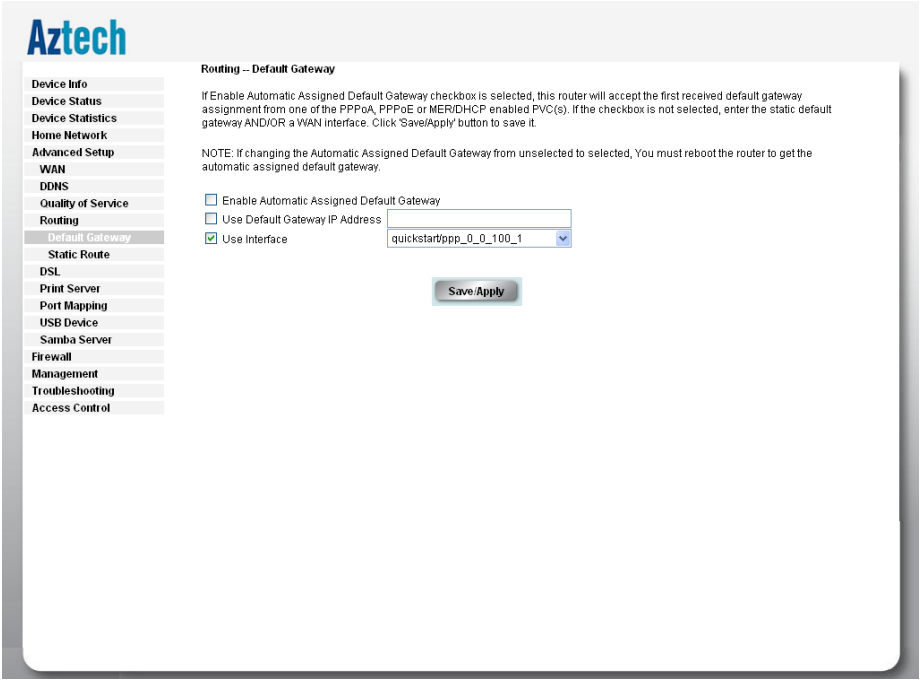
Quality of Service or QoS provides different priority to different applications, users, or data flows, to guarantee a certain level of performance. For example, QoS is important for real-time streaming multimedia applications such as voice over IP, online games and IPTV to provide fixed bit rate and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



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.

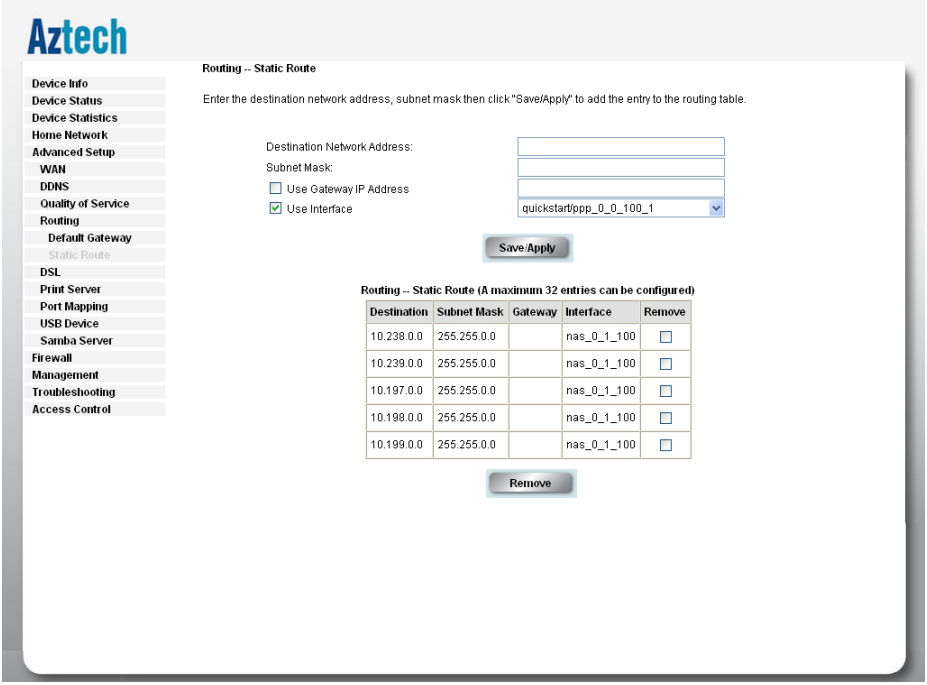


Static Route

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.

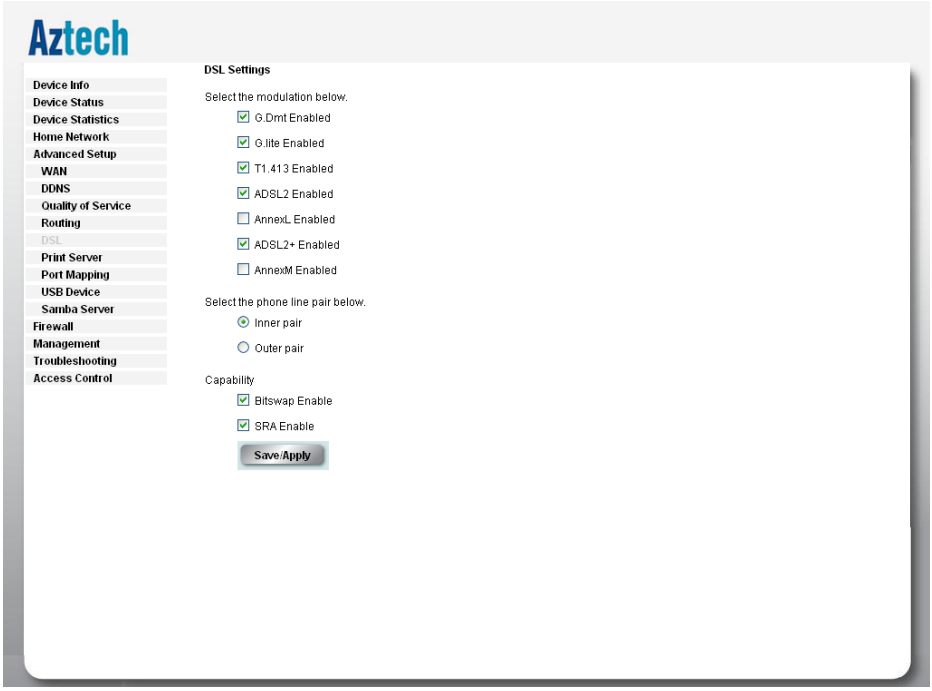


Click Save/Apply to save the settings.

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

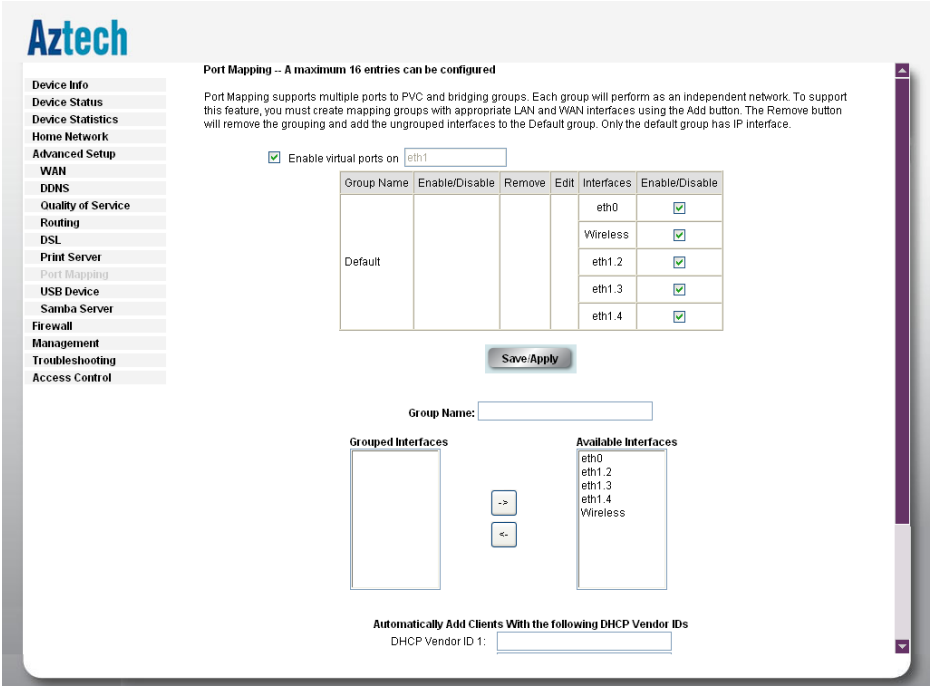
DSL Settings

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



Port Mapping

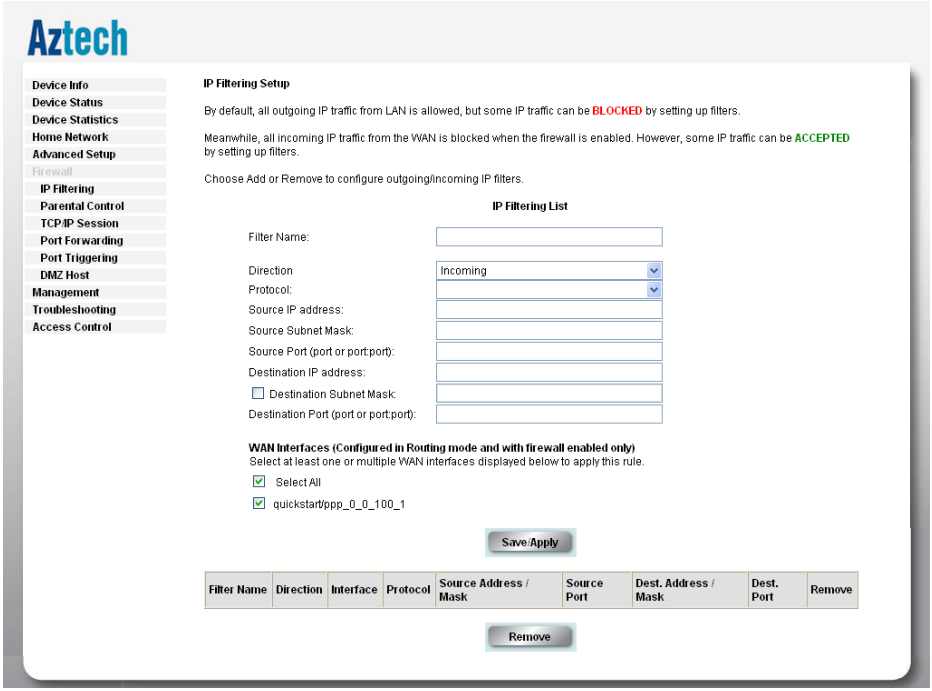
Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces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



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.



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.

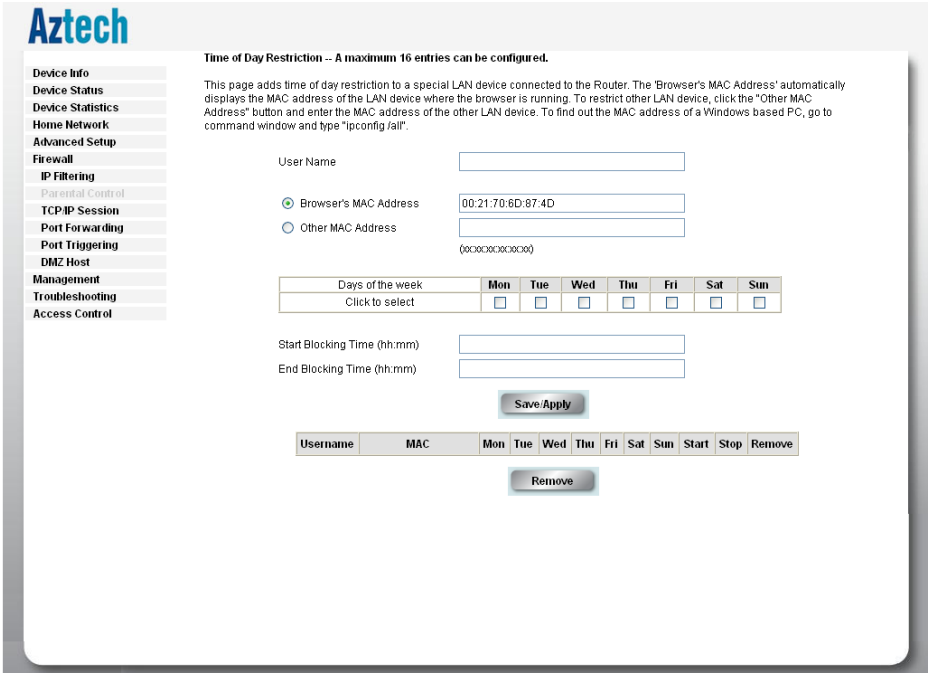
- **Destination Port** Enter the destination port number used by the application to block.

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

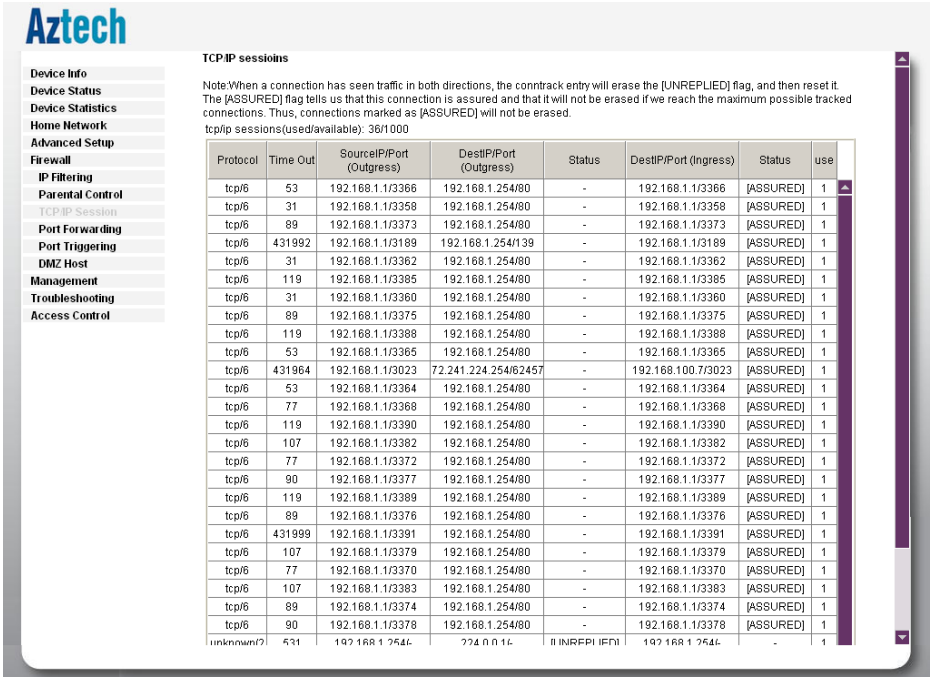
Parental Control allows you to apply router access restrictions among LAN devices within specific times in a day. A maximum of 16 restriction rules can be created.



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).

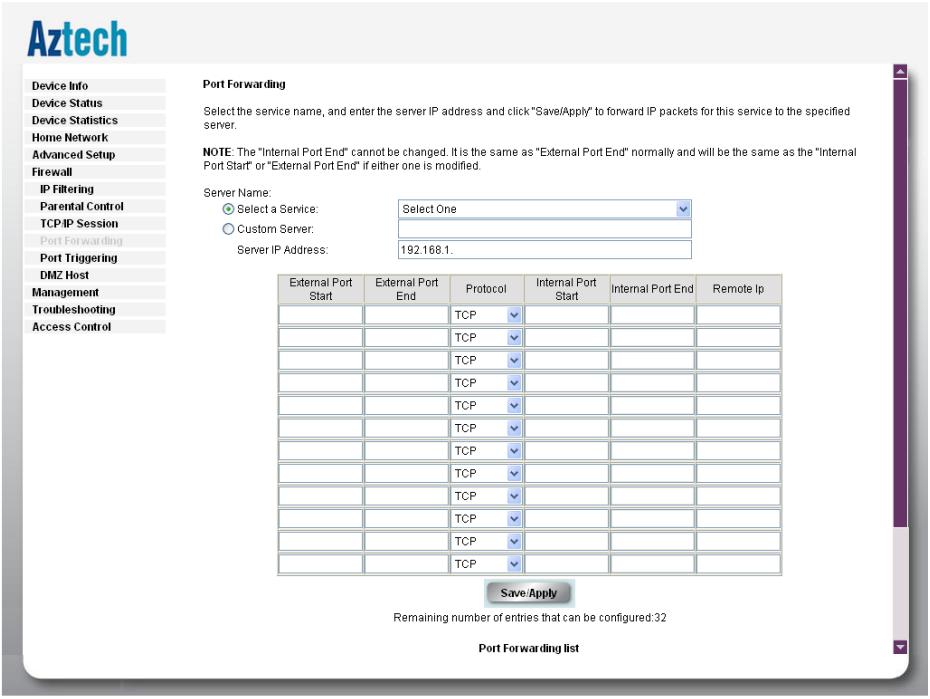
TCP/IP Sessions



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/2	531	192.168.1.254/6	224.0.0.14	[UNREPLIED]	192.168.1.254/6	-	1

Port Forwarding

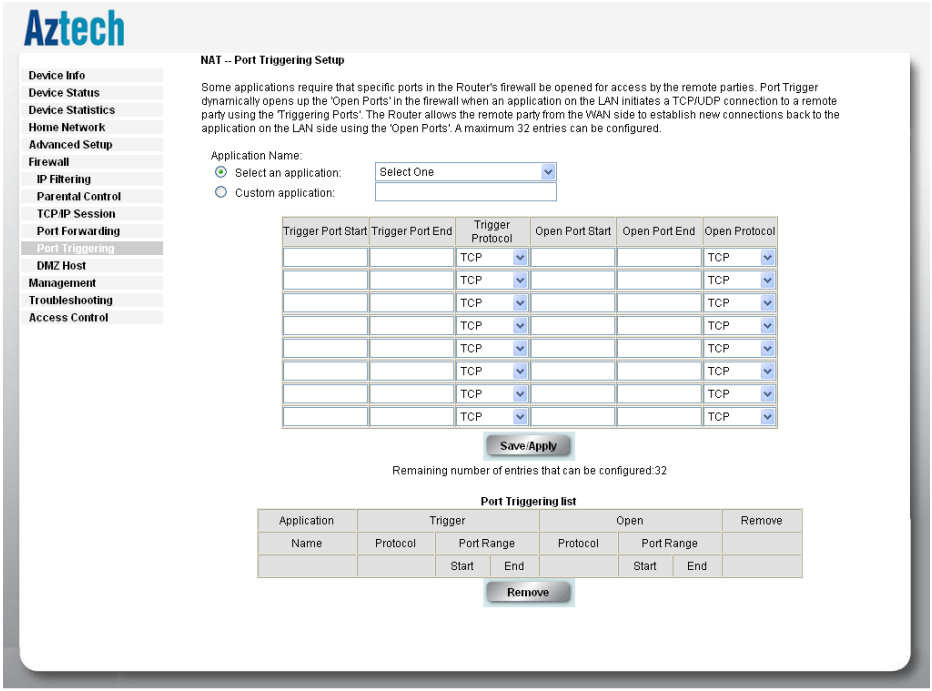
Port Forwarding allows you to direct incoming traffic from the Internet to a specific computer in your local network. A maximum 32 entries can be configured.



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

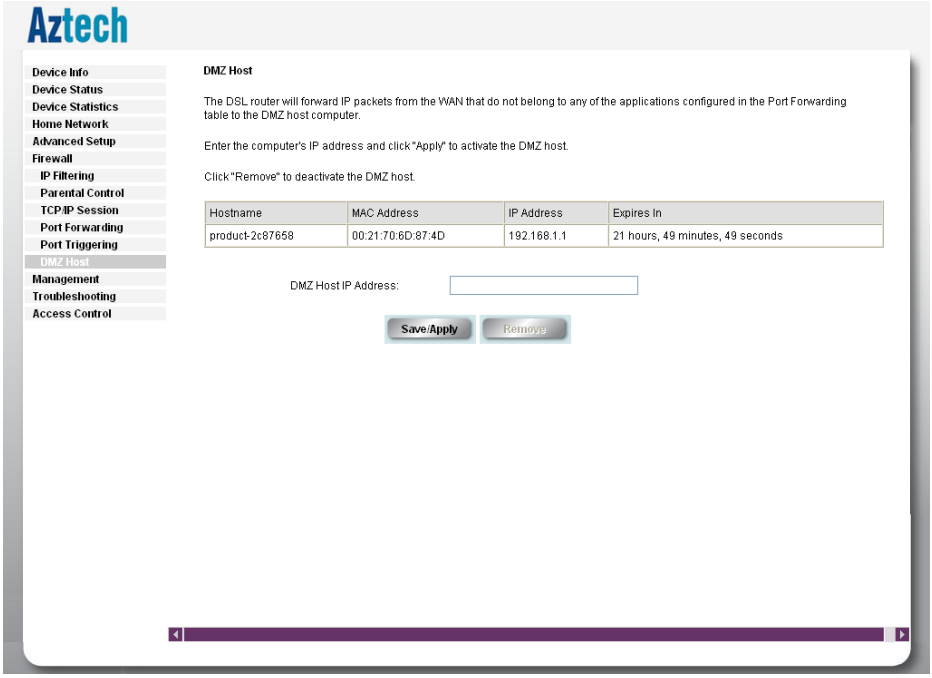
Some applications require that the remote parties open the specific ports in the router's firewall for access. For instance, an application uses port 25 for requests and port 113 for replies. If a computer on the LAN connects to port 25 on a remote server hosting this application, using Port Triggering 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.



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.

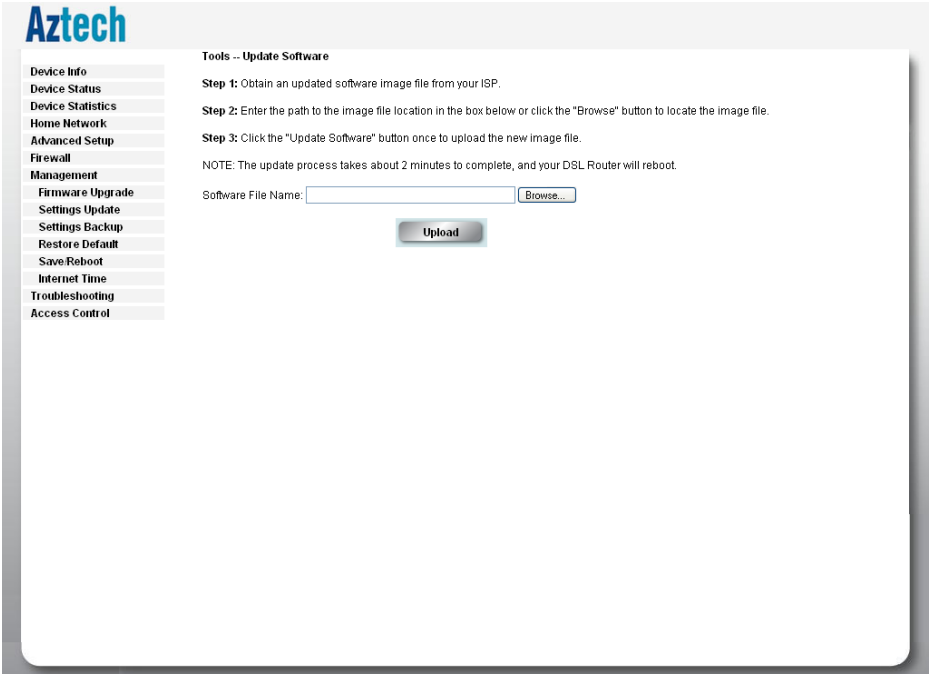


Firmware Upgrade

Allow you to update the firmware of your router.

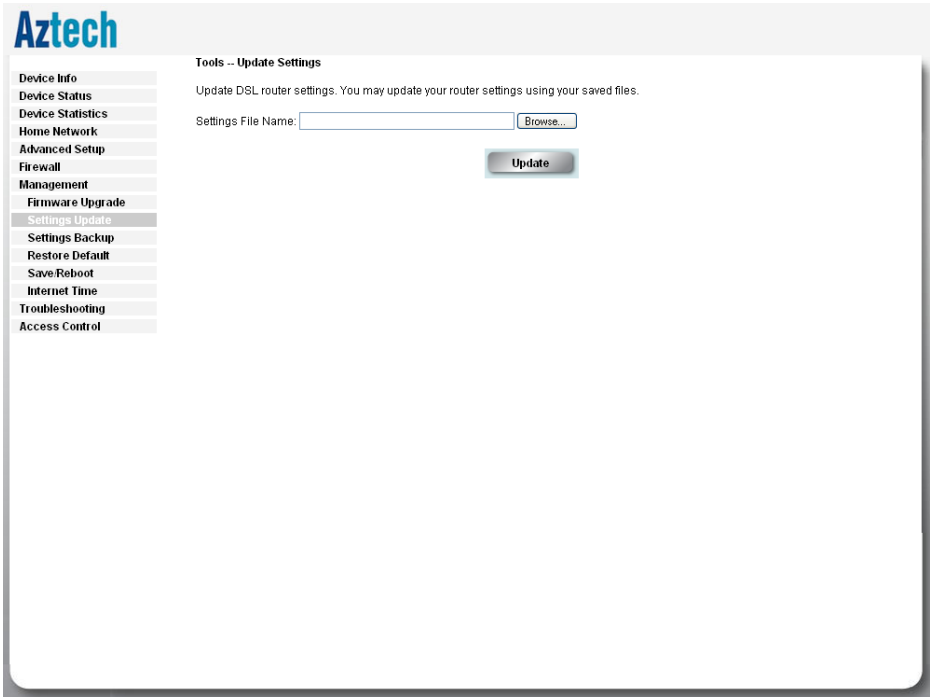
To Update the router's firmware:

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



Settings Update

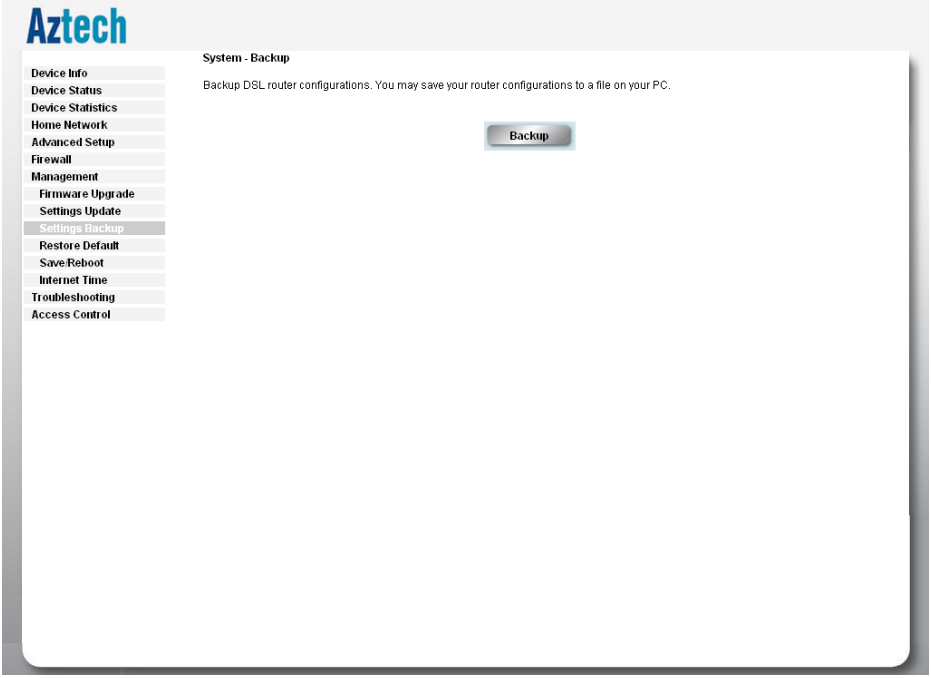
To import a previously saved configuration file from your PC and update the settings of your router, click Browse to locate the backupsettings.conf upgrade file. Then click the Update button.



Settings Backup

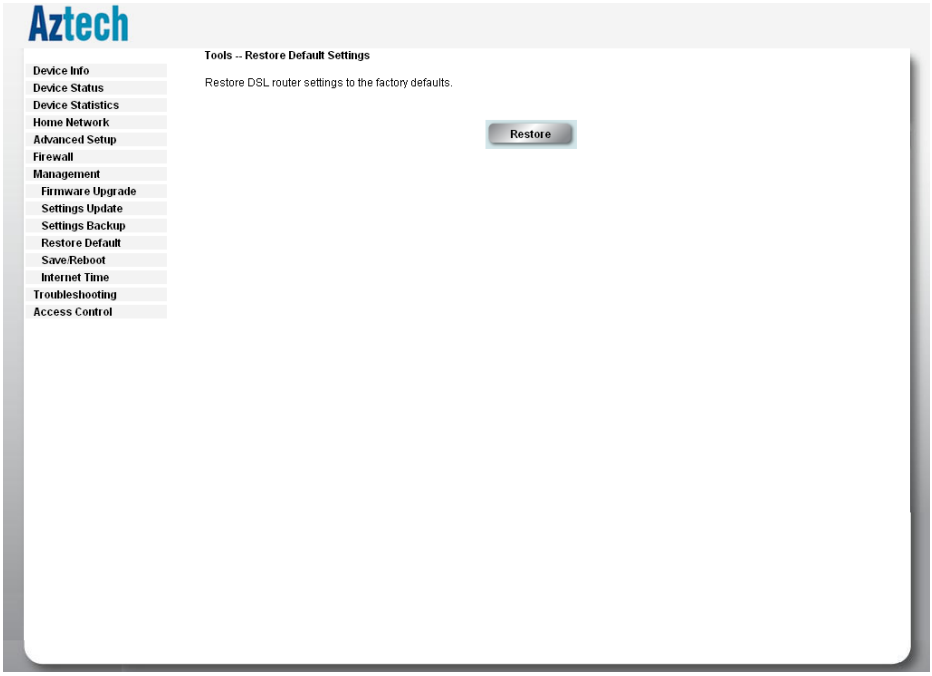
To backup the settings as a configuration file saved on your PC, click the Backup button.

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.



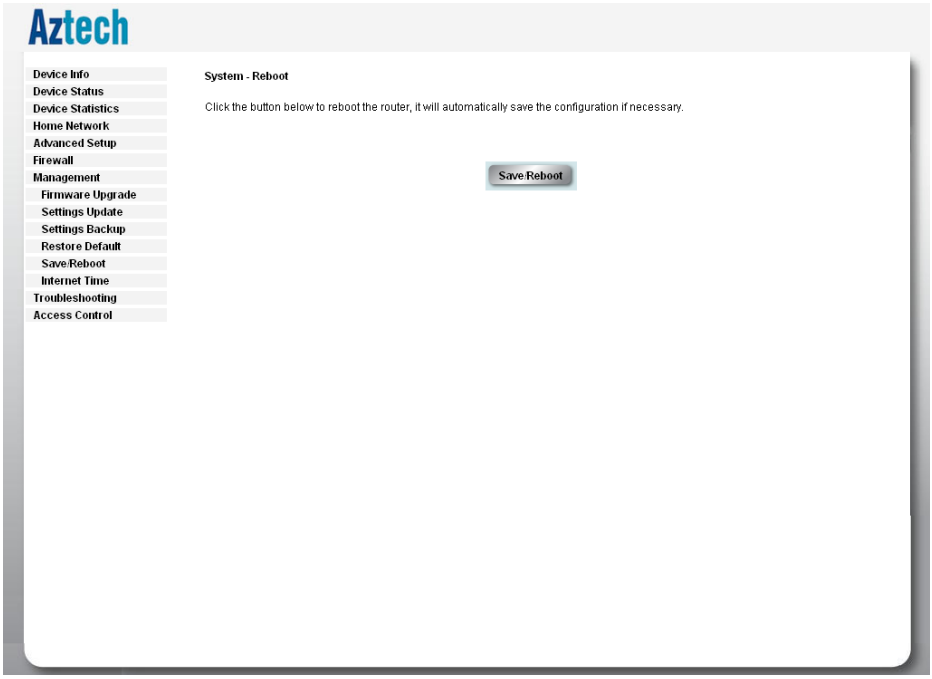
Restore Default

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



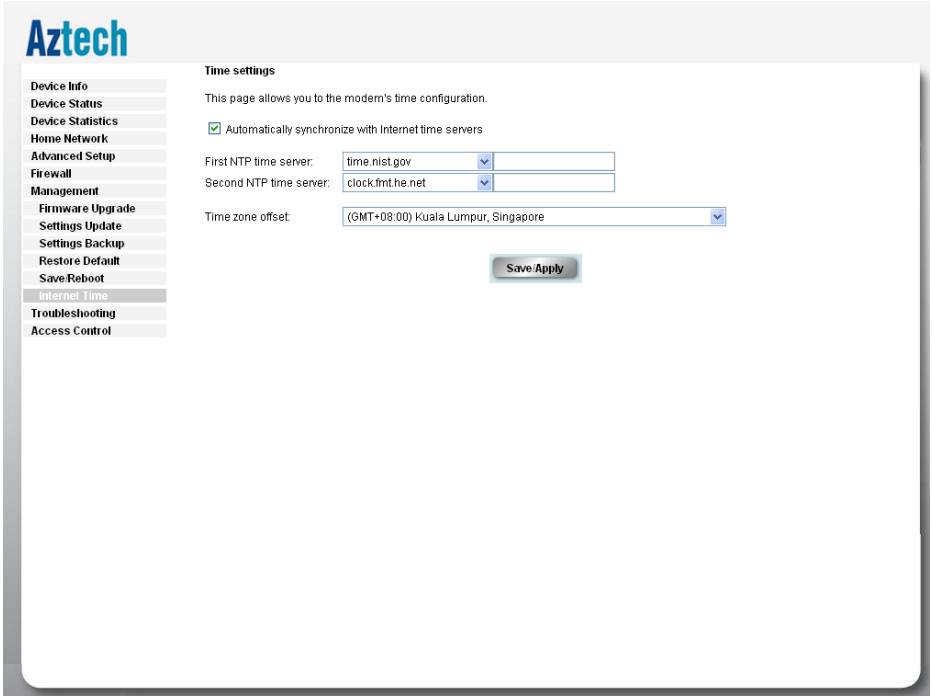
Save/Reboot

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

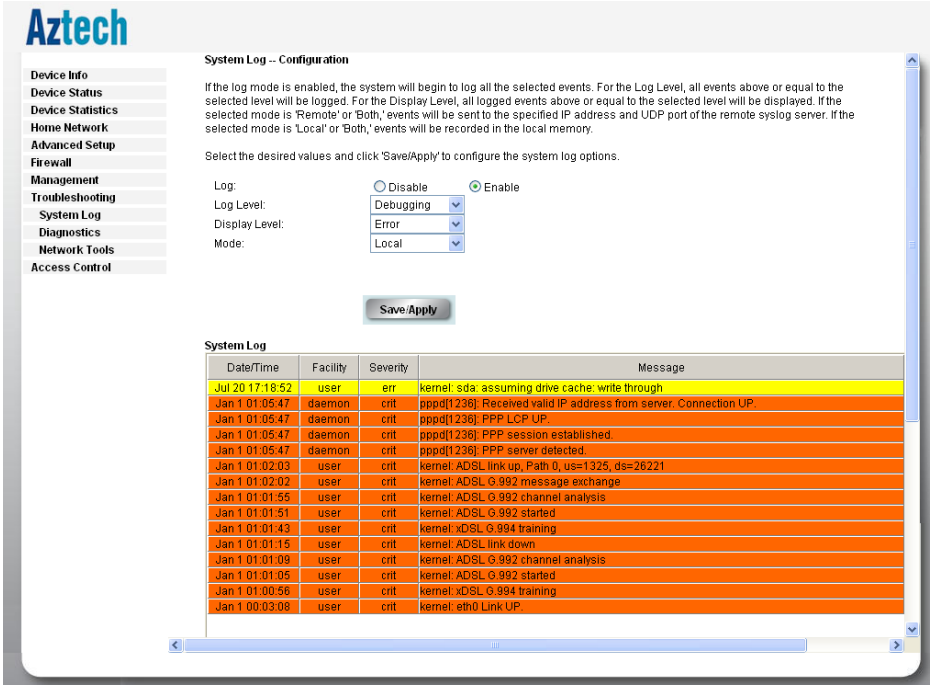
Enable Internet Time to automatically synchronize your modem's time with a time-server when connected to the Internet.



System Log

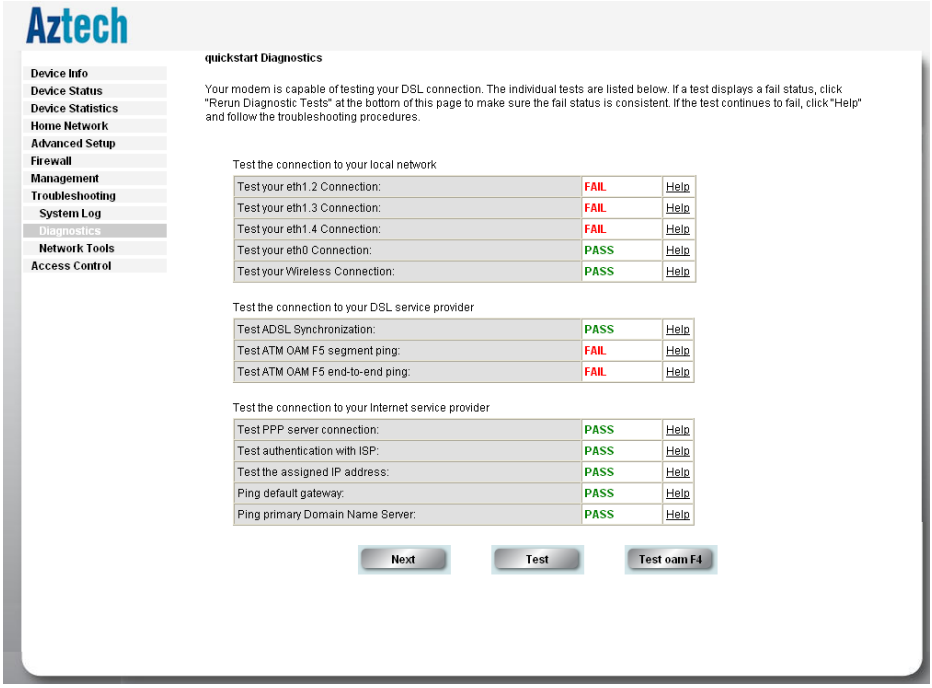
If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' 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.



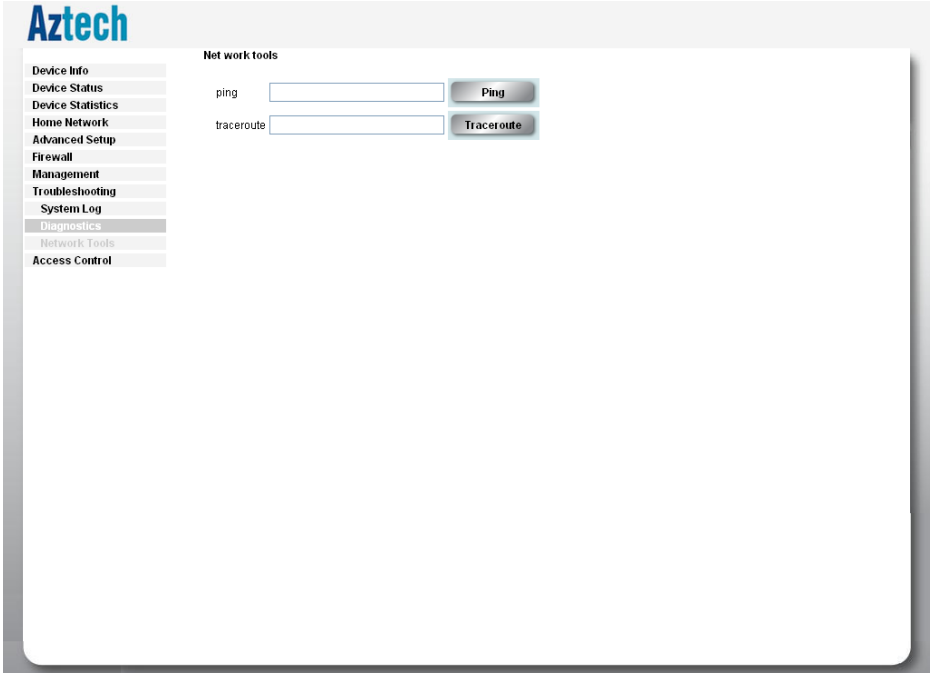
Diagnostics

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.



Network Tools

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

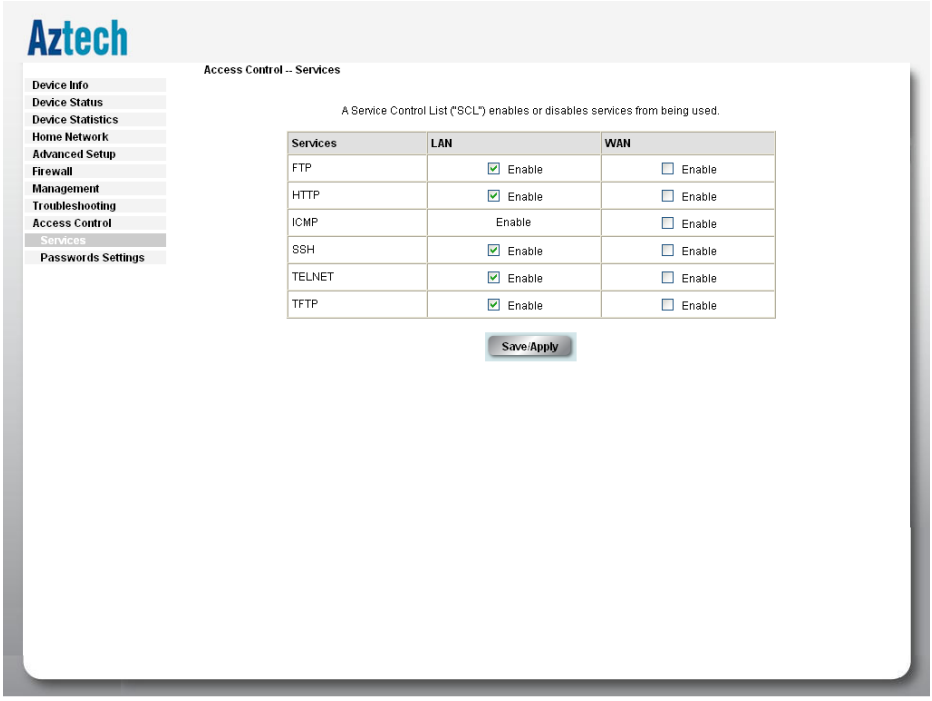


Access Control

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.



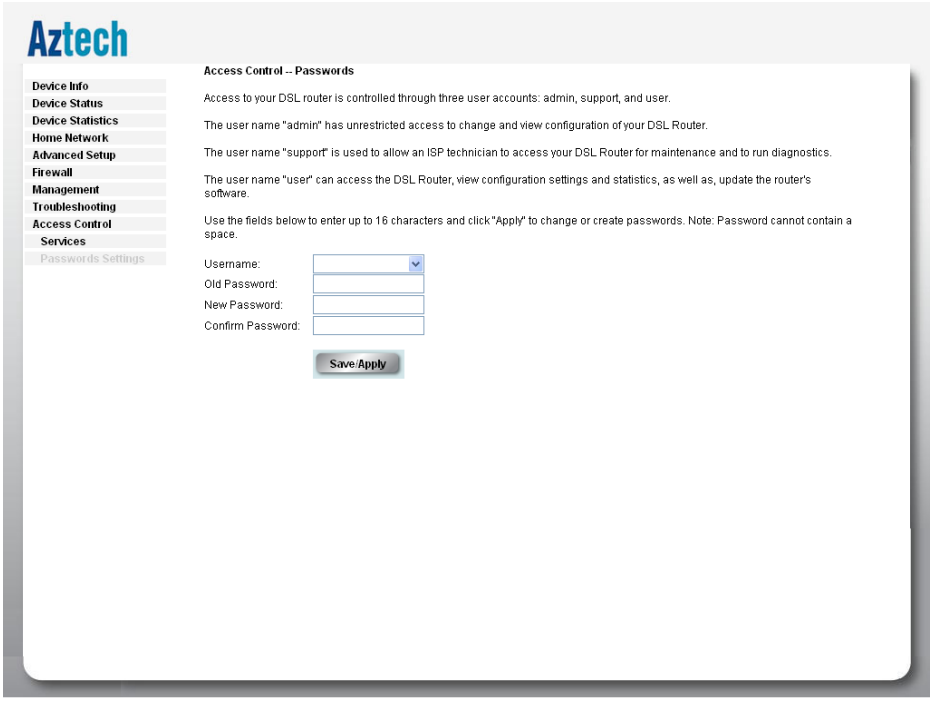
Password Settings

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.



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.