

User Manual

700WR-3G

ADSL2+ 4-Ports 300Mbps Wireless-N
Router with USB Host

Version 1.0

For the latest version of this manual, please visit www.telkomphones.co.za

© Copyright 2014 All rights reserved.

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission. We reserve the right to revise this document at any time without the obligation to notify any person and/or entity. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

LIMITATION OF LIABILITY AND DAMAGES

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

Contents

About the Router.....	4
Requirements.....	5
Package Contents	5
Device Design	6
Front Panel	6
Back Panel.....	7
Getting Started	8
Planning Your Network	9
Remove or Disable Conflicts	10
Internet Sharing, Proxy, and Security Applications.....	10
Configuring TCP/IP Settings	11
Configuring Internet Properties.....	11
Removing Temporary Internet Files	12
Set up the Device.....	13
Connecting to the Internet	14
Connecting Via Setup Wizard.....	14
Basic Page.....	20
Advanced Setup	22
Accessing the Advanced Web Interface.....	22
Menus	23
Network.....	23
Wireless.....	37
Applications	39
System	48
Status.....	52
ADSL Status.....	52
FCC Notice	56

About the Router

The 700WR-3G ADSL2+ 4-port 300Mbps Wireless-N Modem Router with USB Host uses complete Ralink chipset solution that fully complies with ADSL2/ADSL2+ standard. The 700WR-3G supports 2T2R Wi-Fi up to a speed of 300Mbps.

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+ built in modem, Routing functionality for multi-user sharing, double-layer NAT/SPI firewall, 4 port 10/100 AutoMDI/MDIX Managed Switch for video application QoS, high speed IEEE802.11b/g/n Wireless LAN Access point and two USB host ports for network printing, NAS and 3G failover.

The 700WR-3G is TR-069 compliant. TR-069 is a DSL forum technical specification report that defines the remote control/configuration of CPE from ACS (Auto Configuration Server), TR-069 is also well-known as "CPE WAN Management Protocol". The benefits of TR-069 include, remote management, auto-configuration, dynamic service activation, as well as saving cost on customer support and logistics.

Security is provided via a 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. Dynamic DNS 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.

Requirements

Your computer must meet the following minimum requirements.

- Any operating system can be used
- Web Browser
- CDROM drive (For using the included CD, If required)
- 233MHz processor
- Ethernet or Wi-Fi network adapter
- An active DSL line and Internet account

Package Contents

Package contents are listed below. For any missing items, please contact your dealer immediately.

- Router
- Ethernet cable
- Telephone cable
- POTS Splitter
- 12V 1.0A DC Power Adapter
- Quick Start Guide
- Resource CD

Device Design



Front Panel

	Label	Icon	Action	Description
1	WIRELESS ON/OFF button/LED		Off Steady green	Wireless interface disabled Wireless interface enabled
2	POWER		Off Steady green Steady red	No power is supplied to the device Connected to an AC power supply Error on the device
3	ETHERNET LAN 1-4		Off Steady green Blinking green	No Ethernet connection Connected to an Ethernet port Transmitting/Receiving data
4	USB Host		Off Steady green	No USB device connected USB device connected
5	WIRELESS		Off Steady green Blinking green	Wireless interface disabled Wireless Interface enabled Transmitting/Receiving data
6	BROADBAND		Blinking green Steady green	Establishing or No DSL signal DSL signal is established
7	INTERNET		Off Steady green Blinking green Steady red Orange	No connection to the Internet Internet connection established Transmitting/Receiving data PPP authentication failed 3G Connection Active
8	WPS button		Off Blinking green	WPS off or idle WPS association on going

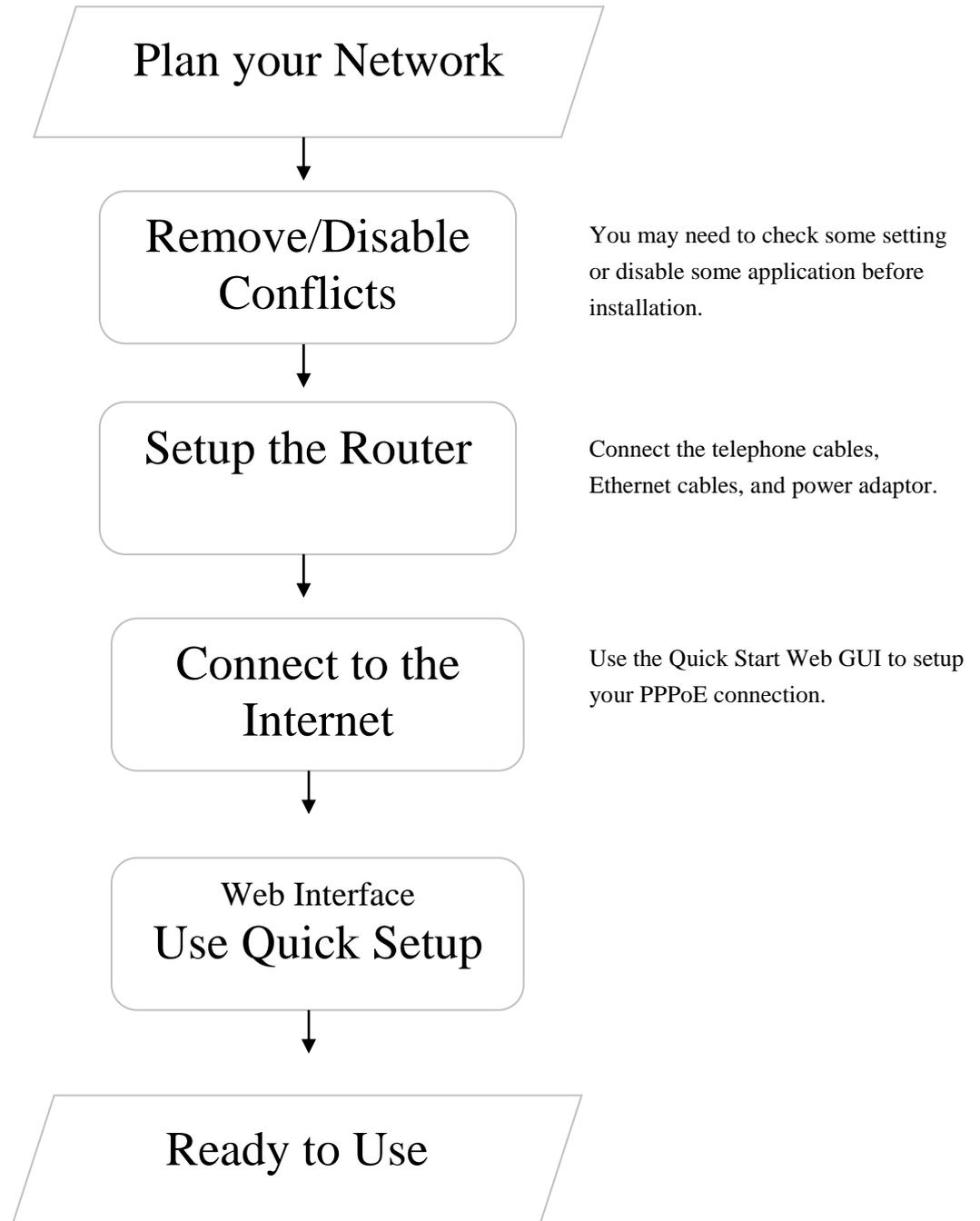
Back Panel



	Label	Description
9	POWER	Power ON/OFF button
10	DC In	12V 1.0A DC Input
11	RESET	To reset the modem to the factory default configuration
12	USB	For USB devices such as printers and USB external hard drives
13	ETHERNET 1 – 4	Connecting computers and other Ethernet LAN devices Note: Port 4 can also be used as a WAN port, if configured as such
14	DSL	Connecting the modem to an ADSL line

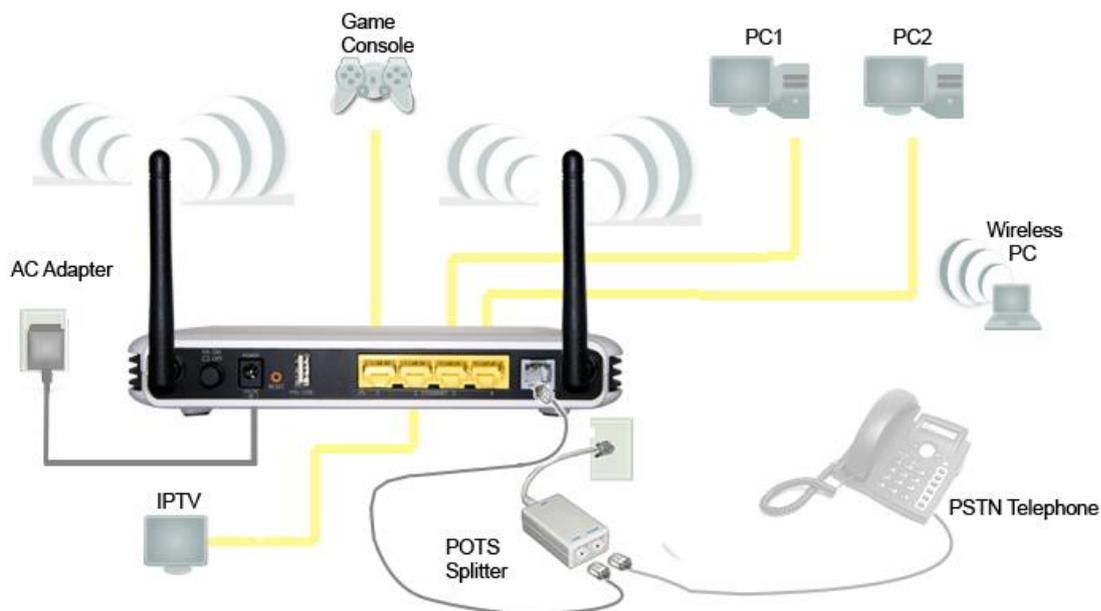
Getting Started

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:

- Ethernet 1 – Game Console
- Ethernet 2 – Dad’s Computer (PC1)
- Ethernet 3 – Mom’s Computer (PC2)
- Ethernet 4 – IPTV Set Top Box

To create a network diagram:

- For wireless devices, identify the wireless devices you want to include in the network
- For wired devices, identify which router port you want to use for each device.

Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before start the installation.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

Internet Sharing Applications	Proxy Software	Security Software
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

Configuring TCP/IP Settings

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

To check the TCP/IP properties (This example is for Windows OS):

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 (This example is for Windows OS):

1. Select Start > Run. This opens the Run dialog box.
2. Enter control inetctl.cpl and then click OK. This opens Internet Properties.
3. Click **Connections** tab.
4. In the Dial-up and Virtual Private Network settings pane, select **Never dial a connection**.
5. Click OK to close Internet Properties.

Removing Temporary Internet Files

Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to clean the cache and remove footprints left by the Web pages you visited. This may be necessary to prevent cache conflicts if you had a previous router on the same IP address as your 700WR-3G

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.

Set up the Device

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

To setup the router:

1. Plug one end of the Ethernet cable into the router's **ETHERNET** port and plug the other end into the Ethernet port into your computer.
2. If you have another device you need to connect directly to the router, use another Ethernet cable. Plug one end of the Ethernet cable from the computer's Ethernet port and then plug the other end into an available Ethernet port in the router.
3. Plug one end of the telephone cable into the POTS Splitter's **ADSL** port and plug the other end into the PSU's **LINE IN** port. Plug the **LINE OUT TO MODEM** cable into the router's **DSL** port.

POTS Splitter

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

To setup a telephone on the POTS Splitter:

- a. Locate the phone jack in your house.
- b. Insert the POTS Splitter into the phone jack.
- c. Plug one end of the telephone cable from the POTS Splitter's **TEL** port and then plug the other end into the telephone.

4. Connect the power adapter from the router's 12V 1.0A DC port into the electrical outlet.
5. Turn ON.

Connecting to the Internet

You can either use the utility on the provided CD to configure your router (Windows OS only) or you can use the built in Web Interface to setup your Internet connection.

To use the CD utility, you should insert the CD, and follow the click the install button.

Otherwise, for any operating system, continue as follows:

Connecting Via Setup Wizard

To connect to the Internet via the User mode GUI:

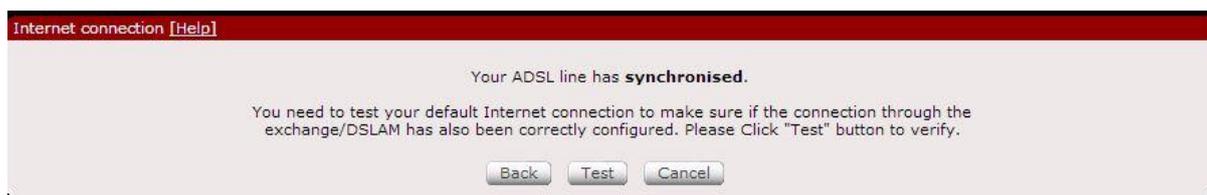
1. Launch your chosen web browser (Firefox, Internet Explorer, Safari etc) and input 10.0.0.2 on the address bar.
2. If your router is in the Factory Default Reset state, the Setup wizard will automatically be opened when you access the router. If the router has already been configured, you will need to enter the username and password (default username/password is **admin/admin**) and select the Wizard Tab.



3. Click **Next** to continue, or **Cancel** to exit utility.



4. Select your Time Zone
5. Click **Next** to continue, **Back** to return to the previous screen or **Cancel** to continue.



6. Before you continue, your router will test if your phone line has been correctly connected to your router, and it will also check if the ADSL service is enabled on your telephone line. Click **Test** to continue, **Back** to return to the previous screen or **Cancel** to continue.



7. If your Telephone line has the ADSL service enabled, and has been correctly connected, you will receive confirmation of this. If not, you will see a screen helping you to fault-find the problem. Your next step will be to verify that you are connected, so as to enable your internet username/password. This is applicable to Telkom internet customers who are configuring an internet connection using a previously unused account only, and is a security measure to ensure that your account is not used before you verify that you are in a position to use it. If Telkom is your ISP and you have already used your username/password or you are with an ISP other than Telkom, you can close the pop-up window without entering in details, and continue with the setup wizard. Click **verify** to continue, **Back** to return to the previous screen or **Cancel** to continue.

ADSL Verify

The ADSL Verify is for customers who have selected the ADSL modem self install option. Once you have completed the modem installation process, submit the form below and your ADSL account will be activated and operational. Should you require assistance, free access to the Telkom helpdesk is available.

If you would prefer a Telkom technician to complete the installation for you, this option is also available at a call out fee. Please contact us on (10210) for any of these options.

★ Telephone number: Eg: 0121234567

★ Order number: Eg: 123456

★ Required Fields

Submit >

Three promotional banners for high-performance connections. Each banner features a blue and green gradient background and the text: "Get high-performance connections for your home." "Give customers real value with high-performance connections." "Enjoy added value on the move with high-performance connections." Below each banner, it says "With South Africa's only full-service telecommunications provider."

8. In the screen that pops up in your internet browser, enter your telephone number and order number for this ADSL installation and click **submit**, and close the window once the details have been verified. If you are not a Telkom ISP client, or are using a previously verified username/Password, you can close this window and continue.

WAN Connection[Help]

WAN Connection

Connection Type: PPPoE - LLC

User Name: guest@telkomadsl

Password: *****

Buttons: Back, Next, Cancel

9. Once your username/password have been verified, you will be able to use them to access the internet. You are now in a position to enter them into your router. Click **Next** to continue, **Back** to return to the previous screen or **Cancel** to continue.

Second WAN Connection [Help]

This screen allows you to configure your router with a second Internet account should you have one. It also allows you to configure your router as a VPN LITE node if you have subscribed to this service.

Second WAN Connection

Configure a second internet account Configure an VPN LITE node

User Name

Password

Back Skip Next Cancel

10. Once your username and password have been entered, the router will test to confirm that they are functional. If not, you will be prompted to re-enter them correctly, if you did not the first time around. You will now be given a chance to enter a second accounts details, or to configure this router as a VPN lite node should you wish to. If neither option is required, please press the **Skip** button.

Wireless Access Point settings [Help]

On this page you are able to change the settings for your routers 'Wireless Access Point'. These changes are optional, and if you leave these settings as they are, you will still have good security for your Wireless connection. If you do not change your default WiFi key, remember that it is printed on the base of the router for your convenience. If you are currently connected to this router via a WiFi connection, and make any changes on this page, you will need to reconnect once you finish this Wizard and the changes are applied.

WLAN Enabled

Broadcast SSID

SSID

WPA/WPA2 Enabled

Key (8 to 63 characters)

Country

Back Skip Next Cancel

11. On this page you will be able to configure your Wi-Fi access point. By default your access point is enabled, and protected by a unique key (password). If you are not going to be using the Wi-Fi function, we suggest you disable it on this page. If you do require Wi-Fi functionality, we suggest that you select a more suitable name, and key (password) for your connection, as a security measure. Click **Skip** if you do not wish to make any changes, or **Next** if you have altered some setting on this screen.

Network->WAN Fail Over

This page allows you to configure your router to support an alternative internet connection for use should your primary connection fail. you can choose either ADSL or 3G as your primary or backup connection. To make use of the 3G connection type, please make sure that you have a supported USB dongle with an activated SIM card plugged into one of the USB ports before continuing.

Mode

Primary Connection

Back Skip Next Cancel

12. You can now configure the WAN failover function. This is applicable if you have a supported 3G dongle installed in addition to your ADSL line, and wish the router to automatically fail over to the alternative connection when your primary connection fails. You can select either 3g or ADSL as the primary connection, or you can disable the connection entirely. Click **Skip** if you do not wish to make any changes, or **Next** if you have altered some setting on this screen.



System->Password [Help]

On this page you are able to change your password for logging in to this router. We recommend that you do this as a security measure. Please do not forget your new password as you will need to reset and reconfigure your router should you forget this and need access to your router.

Administrator

Username

New Password

Confirm Password

13. As a security measure, we suggest that you change the routers default password. Please remember your password, because without it you will not be able to access your router configuration to make any changes. If you forget your username/password, you will need to configure your router from scratch again should you need to modify any settings. Click **Skip** if you do not wish to make any changes (not recommended), or **Next** if you have altered some setting on this screen.

Summary [Help]

Language and Time Zone	
Language	English
Time Zone	(GMT+02:00) South Africa, Istanbul, Cairo, Eastern Europe, Israel
WAN Connection	
Connection Type	WAN
Connection Method	PPPoE/PPPoA
Username	guest@telkomadsl
Password	*****
Second Wan Connection	
Username	
Password	*****
Wireless	
Wireless Enabled	YES
Broadcast SSID Enabled	YES
SSID	MyNetworkName
WPA/WPA2 Enabled	ON
Key	*****
Country	SOUTH AFRICA

Back Apply Cancel

14. On this final page, you will see a summary of your settings. As a security precaution, passwords have been omitted from this page. Once you click **Apply** the router will save all settings and apply them. This may result in the router needing to reconnect to your ISP, and as a result you may see your internet connection drop for a moment. This is normal. You can now log out of the web GUI, and enjoy using your router.

Basic Page

On the basic page, you have three tabs. These are **Home**, **Wizard** and **Quick setup**.

The **Home** tab contains a summary of all the critical information. The **Internet connection** frame contains the details of any active data connection. This list details such as IP address, Connection status, Wan MAC address, default gateway DNS server and connection Up-time. All active connections are listed, regardless of whether they are 3G, ADSL or Eth Wan.



Aztech

Advanced Mode Reboot Logout 1/1/2000 12:05:52 AM

Home Wizard Quick Setup

Internet Connection

ADSL Line Status	DOWN
Connection Type	WAN
Node	PVC0
Connection Status	Not Connected
Connection Mode	PPPoE

LAN Connection

LAN MAC Address	00:AA:BB:01:23:45
LAN IP Address	10.0.0.2
LAN Net Mask	255.255.255.0
DHCP Server	Enable

Wireless Connection

SSID	MyNetworkName
Broadcast SSID	Enable
WLAN MAC Address	00:AA:BB:01:23:46
Wireless Mode	802.11b+g+n
Security	WPA-PSK/WPA2-PSK

Local Network

Hostname	IP Address	MAC Address	Expire Time
WS-LAMEEZ	10.0.0.3	6C:3B:E5:13:58:F3	0 Days 23:55:29

Storage

No storage device found.

Printer

No printer device found.

The **Wizard** tab will return you to the setup wizard that you first encountered when you logged into the router for the very first time. This can be used to reconfigure your router from scratch should you wish to, and contains an option to reset the settings to the Factory Default state.

The **Quick Setup** tab shows a summary of your primary internet connections, and can be used as a quick way to change key parameters. This will affect PVC8,PVC0 and PVC7 which are the primary connections for 3G,ADSL and Eth WAN respectively.

The screenshot displays the 'Quicksetup [Help]' window with the following configuration details:

Section	Parameter	Value
Region	Language	English
	Time Zone	(GMT+02:00) Athens, Helsinki, Istanbul, Cairo, Eastern Europe, I: ▼
	NTP Server	Custom NTP Server ▼
	Custom NTP Server	igubu.saix.net
	DayLight Saving	Disable ▼
WAN Connection	Internet Connection	<input type="radio"/> Mobile Broadband <input checked="" type="radio"/> WAN
	Connection Method	PPPoE - LLC ▼
	User Name	guest@telkomadsl
	Password	*****
	VPI	8
	VCI	35
	Wireless	
WLAN Enabled	<input checked="" type="checkbox"/>	
Broadcast SSID	<input checked="" type="checkbox"/>	
SSID	MyNetworkName	
WPA/WPA2 Enabled	<input checked="" type="checkbox"/>	
Passphrase (8 to 63 characters)	8076082884220356	

Buttons:

Advanced Setup

Advanced Setup provides configuration options for other router functions.

Accessing the Advanced Web Interface

To access the Advanced Web Interface:

1. Launch your web browser.
2. Input 10.0.0.2 on the address bar and 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 Login
5. Click Advanced Mode



Menus

The Web User Interface includes the following menus:

- Network
- Wireless
- Applications
- System
- Status

Network

Local

On this page you can configure the DSL Router's IP Address and Subnet Mask for the LAN interface. You may also configure the DHCP server settings of your router. If you make any changes to the Router's IP address, you will need to log in again using the new IP address.

Aztech

Basic Mode Reboot Logout 1/1/2000 12:15:47 AM

Network Wireless Applications System Status

Local Internet ADSL QoS Management Routing MAC-IP Reservation Auto Wan Fail Over

Network->Local [Help]

Router IP Address	<input type="text" value="10.0.0.2"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
DHCP	Enabled ▾
Start IP	<input type="text" value="10.0.0.3"/>
IP Pool Count	<input type="text" value="252"/>
Lease Time	<input type="text" value="86400"/> seconds (0 sets to default value of 259200)
DNS Relay	Auto ▾
Primary DNS	<input type="text" value="N/A"/>
Secondary DNS	<input type="text" value="N/A"/>

Apply

Internet

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

There are three different WAN connection methods that your router can use to connect to the internet.

1. Mobile Broadband
2. ADSL
3. Ethernet WAN (Eth WAN)

Each connection required PVC number (0 – 8). By default, the ADSL internet connection is PVC0 and the Ethernet WAN is on PVC7. If Eth Wan mode is not enabled, PVC7 can also be used to configure an ADSL account. PVC1 and PVC6 are reserved for VPN lite (on ADSL and Eth WAN respectively) if this function is enabled. If Eth WAN access is not configured, you can use PVC0-PVC7 for different ADSL accounts. PVC8 is reserved for Mobile broadband and is not usable for ADSL or Eth WAN.

The following describes the configuration of each of these 3 WAN connection modes.

Mobile Broadband

This access mode is to connect using the mobile broadband network. This includes technologies such as 3G and LTE. In order to use this mode, you will need one of the supported Mobile Broadband dongles. A up-to-date list of the currently supported dongles is available for download from www.telkomphones.co.za

Once you have places a SIM card into your supported dongle, you can plug it into either of the USB sockets on the rear of the router. The router is set to automatically configure the connection with the network supplied configuration. You will be able to see this configuration if you click on the **Mobile Broadband** radio button.



If the default settings are not suitable for your configuration, they can be easily changed by selecting the **Manual** radio button.

You should note that if you are using this router to connect using mobile broadband only (no ADSL or Eth WAN connection), it is a good idea to disable the Auto WAN fail over function. This is accessed by way of the **Auto Wan Fail over** tab on the **Network** page

ADSL

Your router is configured by default to connect using the Telkom Guest account. This is set up on PVC0, and will allow the basic connectivity required to test your connection. This allows access to most parts of the Telkom website. In order to have full internet access, you will need to enter your own Username and Password. This is typically done using the Wizard as described above, but can also be changed by selecting the **ADSL** radio button on the **Internet** tab on the **Network** page.

Network->Internet [Help]

Internet Connection	<input checked="" type="radio"/> Mobile Broadband <input type="radio"/> ADSL <input type="radio"/> Ethernet WAN	
Virtual Circuit	PVC 0 ▾	PVCs Summary
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated	
Shared	<input checked="" type="checkbox"/> Shared	
VPI	<input type="text" value="8"/>	(range: 0~255)
VCI	<input type="text" value="35"/>	(range: 1~65535)
Connection Type	PPPoA/PPPoE ▾	
Username	<input type="text" value="guest@telkomadsl"/>	
Password	<input type="password" value="*****"/>	
Encapsulation	PPPoE LLC ▾	
PPPoE Pass-through	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated	
Connection	Always On (Recommended) ▾	
Idle Time	<input type="text"/>	(minutes)
TCP MSS Option	<input type="text" value="0"/>	bytes(0: default)
TCP MTU Option	<input type="text" value="0"/>	bytes(0: default)
Interface Status	Down	

IP common Options

Default Route Yes No

IPv4 Options

Get IP Address Static Dynamic

Static IP Address

IP Subnet Mask

Gateway

NAT ▾

Firewall ▾

Dynamic Route ▾

Dynamic Route Direction ▾

IGMP Proxy Enable Disable

ATM QoS ▾

PCR cells/second

SCR cells/second

MBS cells

[Apply](#)

Note: If Ethernet WAN is enabled, you will not be able to use PVC 7 for a ADSL connection.

Unless you have disabled it in the Wizard, the default account on PVC0 will be active. This screenshot shows the default guest account, but it is quite likely that you have changed it to your own username/password when you set your router up using the wizard.

Activate / Deactivate: You can use these to deactivate your connection. This will prevent the configured username and password from being used to access the internet. This is particularly useful if you have configured multiple ADSL accounts on your router and wish to switch between them, or to switch between ADSL/Mobile broadband/Eth Wan accounts.

Shared See below

VPI See below

VCI See below

Connection type See below

PPP encapsulation. See below

The above five items define how the connection to your ISP is configured.

As a result of this, it is not recommended that you alter these settings unless directed to by your ISP for a particular purpose. **Shared** is to allow more than one connection on a VPI/VCI channel. The VPI/VCI settings are used to define the “communication channel” that your ISP uses to communicate with your router. By default, these should be 8 and 25 respectively, and are set to this by default. If you change these settings, you may be unable to connect to your ISP. Some specific services may require you to set up a connection with different VPI/VCI settings, but your ISP will directly inform you if this is the case.

PPP pass-through. This setting is to allow you to connect another device on the LAN network that uses its own internet account to connect. This could be another router, or even your PC that has been configured with a PPP “dial up” connection. This is set to ON by default.

Connection This is where you set the timeout for your ADSL connection. When there has been no activity on the ADSL line for the pre-defined time, the connection will be dropped. The connection will automatically reconnect once it is needed. The default setting is for the connection to never drop, and to remain connected even when there is no ADSL traffic.

Interface status This is an indication of whether the ADSL line is ready to route traffic using this Username and password. It will indicate if the connection is **UP** or **DOWN**.

Default route This option is enabled by default for the first ADSL PPP account. If enabled, the router will route all internet traffic that is not otherwise configured in the routing table over this connection. If disabled, only the traffic defined to use this connection will be routed over it. Unless

you have configured a highly complex routing list, it is recommended that at least one of your internet connections is listed as **Default Route**.

Get IP Address In most cases your ISP will automatically assign an IP address for your ADSL connection. In the rare case where you are provided with a static address, you are able to configure it here.

NAT If you wish to disable Network Address Translation mode of the firewall, it can be done on this drop-down menu. We do not recommend that you do this unless absolutely needed. An example of where you would need to do this is if you are using the VPN Lite service, in which case you would disable this function for the VPN lite interface.

Firewall This can be disabled if desired, however we strongly recommend not doing so unless you are absolutely sure of the need for it. As is the case with NAT, a typical example of this would be when using the VPN lite function.

You can add more than one internet connection on the ADSL interface. You may however experience difficulty with packet routing when doing this if you select both as the default connection, so it should be used with care. Typically, this sort of setup would be done to either allow for quick switching between internet accounts using the **Activated/Deactivated** radio button, or by adding an entry for a specific IP address range into the routing table.

To add a WAN interface:

1. Select an available Virtual Circuit from the drop-down box

NOTE: PVC0 is the default first ADSL connection. PVC1 is automatically used if you configure the VPN lite function, and should be avoided for general use. PVC6 and PVC7 will not be available to the ADSL connection if Eth WAN is enabled.

2. Enter VPI/VCI settings – in South Africa, these are typically 8 and 35 unless otherwise specified.
3. Select the Connection Type (Typically PPPoA/PPPoE for ADSL connections)
4. Enter PPP Username and Password (provided by your ISP)
5. Ensure Default Route is selected as Yes for at least one of the connections
6. Ensure Get IP Address is set to Dynamic unless you have been provided an ADSL account that has a static IP.
7. Click the Apply button to commit the settings

To edit an existing WAN interface:

1. Select the Virtual Circuit that you want to Edit from the drop down box.
2. Make the necessary amendments.
3. Click the Apply button to commit the settings.

PVC Summery This button will show a summary of the connection details of all the PVC connections in a pop-up window.

Ethernet WAN

The Ethernet WAN radio button will allow you to change the LAN 4 Ethernet part from a LAN port into a WAN port. This would be useful if you wish to use your router to connect via a Fiber-to-the-Home (FTTH) router, or as an access point on a Ethernet network.

This function has been pre-configured with the Telkom Guest account. If you have not used the Wizard to configure this as an internet connection (firmware 246.70.7 onwards), then you will need to do so manually.

There are two pre-configured setups for Ethernet WAN connections. Eth-WAN (PVC7) is the default internet access configuration, and VPN-Lite (PVC6) is preconfigured for the VPN lite service. It is recommended that should you be using the VPN lite service that you configure as per the VPN Lite chapter in this guide, and do not do so manually.

Configuration of the Eth-WAN (PVC7) connection is as follows :

Set LAN4 as WAN port

This is a vital part of the configuration process. By default, the physical Ethernet port 4 is part of the LAN network, and is on the “inside” of the firewall. Any device connected to it will be supplied with a 10.0.0.x IP address from the internal DHCP server, and will be able to connect to any device on the local network. Obviously this will not allow for it to be used as a WAN port to give the router internet access. It is a vital part of setting up the Ethernet WAN connection to make sure that this block is selected to change Port 4 into a WAN port. This will be done automatically the first time you enable the WAN configuration, and it is important to ensure that this setting is in tune with your physical Ethernet wiring – for instance, should you wish to use Port 4 temporarily as a LAN port again, you will need to not only deactivate the connection, but also deselect this block to return the port to the LAN.



Aztech

Basic Mode Reboot Logout 2014/11/10, 12:19:05 PM

Network Wireless Applications System Status

Local Internet ADSL QoS Management Routing MAC-IP Reservation Auto Wan Fail Over

Network->Internet [Help]

Internet Connection Mobile Broadband ADSL Ethernet WAN

Set Lan4 as Wan Port

Ethernet WAN Type ETH-WAN (PVC7)

Status Activated Deactivated

Connection Type PPPoE

Username guest@telkomadsl

Password

Encapsulation PPPoE LLC

PPPoE Pass-through Activated Deactivated

Connection Always On (Recommended)

Idle Time 0 (minutes)

TCP MSS Option 0 bytes(0: default)

TCP MTU Option 0 bytes(0: default)

Interface Status Down

IP common Options

Default Route Yes No

IPv4 Options

Get IP Address Static Dynamic

Static IP Address 0.0.0.0

IP Subnet Mask 0.0.0.0

Gateway 0.0.0.0

NAT Enable

Firewall Enable

Dynamic Route RIP1

Dynamic Route Direction None

IGMP Proxy Enable Disable

Apply

Note: Please select "Set Lan4 as Wan Port" to use the Ethernet Wan.

Ethernet WAN type

As described before, ETH WAN (pvc7) uses the connection PVC7 and is pre-configured for turning LAN port 4 into a Wan port to give internet access, and VPN LITE(PVC6) is preconfigured to use LAN port 4 to connect as a VPN LITE node over an Ethernet connection.

Connection Type

Use PPPoE if you need to connect via a username/password as is the case when connecting the Ethernet port to a FTTH or another xDSL router. You should use Static/or dynamic as appropriate when connecting to corporate network of Ethernet port of a 3G/LTE router.

Bridge mode is used to pass a PPP connection from a device on the LAN side across to the WAN port.

The following settings will be present and/or change order depending on the connection type settings shown above. We have listed them all here, but some will only be applicable in certain cases.

Username/password These are provided by your ISP for use when a PPPoE connection is required.

PPP pass-through This is enabled by default, and is a way to allow bridge mode connections from devices on the LAN network at the same time as the router is connecting using an independently selected method.

Connection By default the connection is set to remain active even when there is no traffic over it. In some cases it might be beneficial to select **Connect on Demand** and set an **Idle Time**. In this case, the connection will be dropped once no traffic has passed for the length of time specified.

Interface status This is an indication as to whether the selected connection type has successfully connected or not. **UP** or **DOWN** will be shown.

Default Route If this is enabled, all traffic not set up to route via an alternative interface in the routing table (see the chapter on this below) will be routed over this interface. It is recommended that only one interface be selected as the default route.

Get IP address Depending on your connection type, you may be able to configure your IP address manually. PPPoE connections typically use dynamic IP addresses, though on some high-end ISP accounts you may get a static address. If you select **Static IP** on the **Connection** type, you will not have the option to change this setting, and if you select **Dynamic IP**, on the **Connection** type, you will not be able to have your IP dynamically assigned.

For static mode, you will need to specify **IP Address, Netmask and Gateway**. For dynamic mode, these will be assigned for you from your router or ISP.

Nat and Firewall These settings should only be disabled if you understand **ALL** the implications. We do not recommend this except when using this device behind another firewall, or as a VPN lite node.

ADSL Settings

The ADSL tab allows you to select the modulation and ADSL type. By default you should select **Auto Sync-up** or **ADSL2+**, and **Annex A**



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.

Aztech

Basic Mode Reboot

Network Wireless Applications System Status

Local Internet ADSL QoS Management Routing MAC-IP Reservation

Network->QoS [Help]

QoS

Discipline

WRR weight

Highest (valid 1-15)

High (valid 1-15)

Medium (valid 1-15)

Low (valid 1-15)

Rule Index

Active

Application

Physical Ports eth0 eth1 eth2 eth3 ra0

Destination MAC

Dest IP Physical Ports eth0 eth1 eth2 eth3 ra0

Destination MAC

Dest IP

Dest Mask

Dest Port Range ~

Source MAC

Source IP

Source Mask

Port Range ~

Protocol ID

Vlan ID Range ~

IPP/DS Field

IP Precedence Range ~

Type of Service

DSCP Range ~ (Value Range: 0 ~ 63)

802.1p ~

IPP/DS Field

IP Precedence Remarking

Type of Service Remarking

DSCP Remarking (Value Range: 0 ~ 63)

802.1p Remarking

Queue #

You are able to give priority based on many factors, such as **Physical connection, IP address, MAC address, port number, application** etc. You can set up to 15 independent rules.

Management

TR-069 client – Configuration (CWMP)

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. This page is set up to the required settings, and it is not recommended that you make any changes. TR-069

allows your ISP to provide remote support, firmware upgrades, Configuration backup etc should you require this.

The screenshot shows two configuration panels from the Aztech router's web interface. The top panel is titled "Network->TR-069 [Help]" and contains the following settings:

- TR-069 Settings**
- CWMP:
- URL:
- User Name:
- Password:
- CPE Path:
- CPE User Name:
- CPE Password:
- Periodic Inform:
- Interval:
- Apply button

The bottom panel is titled "Network->SNMP [Help]" and contains the following settings:

- SNMP:
- Get Community:
- Set Community:
- Apply button

Routing

By default, the routing table is quite simple and is configured automatically as required. If your router configuration becomes more complex, such as when you are using multiple LAN subnets, or multiple WAN connections, you may need to manually define the data transmitting paths. In this case you can add static routes. By clicking the **Add** button.

The screenshot shows the "Aztech" router configuration interface. The "Network" menu is selected, and the "Routing" sub-menu is active. The "Network->Routing [Help]" panel displays a table of static routes:

Destination IP	Network Mask	Gateway	Interface	Metric	Delete
192.168.2.0	255.255.255.0	0.0.0.0	PVC0	0	
192.168.1.0	255.255.255.0	0.0.0.0	PVC0	0	
127.0.0.0	255.255.0.0	0.0.0.0	PVC0	0	
239.0.0.0	255.0.0.0	0.0.0.0	PVC0	0	
239.0.0.0	255.0.0.0	0.0.0.0	PVC0	0	

Below the table are buttons for "Add", "Apply", and "Cancel".

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

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

Subnet Mask Enter the subnet mask for this destination.

Gateway If you wish to use a specific gateway to reach the destination network, enter the IP address of the gateway. If not, enter 0.0.0.0 for Internet routing, you would typically need to add a Gateway IP, and for local addresses, 0.0.0.0 is typically used.

Interface If you wish to route your packets over a particular WAN interface, select the interface from the dropdown list.

Click **Apply** to save the settings.

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

MAC-IP Reservation

You can force the DHCP server on your router to assign a particular static IP address when a device with a specified MAC address connects. This is useful particularly when using the port forwarding function for a device that is not able to have its IP address defined on in its firmware.



To manually reserve a LAN IP address:

1. Enter the devices MAC address.
2. Key in the LAN IP Address you want to assign to this device.
3. Click the Add button.

The device can be deleted from the table by clicking on the delete icon

Auto Wan Failover

You can configure your router to provide internet connection backup. You are able to select your 3G or ADSL connection as the primary connection mode, and in the event that this connection fails, your internet access will automatically be transferred to the alternative connection.



Obviously, in order to use this mode, you will need a 3G dongle, with a valid SIM card inserted, connected to one of your USB sockets. You will also need to ensure network coverage.

Wireless

Settings

This page allows you to configure basic features of the wireless LAN interface. By default, the Wi-Fi is enabled, with the SSID “**MyNetworkName**” and its own unique password (key). You will be able to securely make use of a Wi-Fi connection right away. Should you wish to make any changes, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID), restrict the channel set based on country requirements, and all other configurations relating to the wireless LAN interface.

The screenshot shows the 'Wireless->Settings [Help]' page. It contains the following settings:

Wireless Enabled	<input checked="" type="checkbox"/>
SSID	<input type="text" value="MyNetworkName"/>
Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Mode	802.11b+g+n ▼
Beacon Interval	<input type="text" value="100"/> (range: 20~1000)
Data Beacon Rate (DTIM)	<input type="text" value="1"/> (range 1 - 255, default 1)
Fragment Threshold	<input type="text" value="2346"/> (range: 256~2346, even numbers only)
RTS/TCS Threshold	<input type="text" value="2347"/> (range: 1500~2347)
Channel	SOUTH AFRICA ▼ 06 ▼ Current Channel : <input type="text" value="6"/>
HT Channel Bandwidth	20/40 MHz ▼
HT Guard Interval	AUTO ▼
MCS	AUTO ▼
Extension Channel	below the control channel ▼

Apply

Click Apply to commit the wireless settings.

Security

This page allows you to set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. By default, the router uses WPA-PSK/WPA2-PSK security. This is a good level of security that requires a user to have a pre-defined key (password) in order to connect. Your router is supplied with its own unique key, which you will see in on this page. Should you wish to make this something more memorable, you are able to make the change on this page. Click "Apply" to commit wireless security settings.

The screenshot shows the 'Wireless->Security [Help]' page. It contains the following settings:

SSID index	1 ▼
SSID	<input type="text" value="MyNetworkName"/>
Security Mode	WPA-PSK/WPA2-PSK ▼
Encryption	TKIP/AES ▼
Pre-Shared Key (8~63 characters)	<input type="text" value="8076082884220356"/>
WPS	<input type="radio"/> Yes <input checked="" type="radio"/> No

Apply

MAC Filter

This page allows you to set a filter to Allow or Deny specific wireless clients by entering the MAC address and selecting the Access Control List mode. To add a wireless client to this list, Enable the **WLAN MAC filter** checkbox, select from **Access Control List Mode** whether you wish to allow or block the clients listed, and enter the MAC address of the relevant

device in the format AA:BB:CC:DD:EE:FF Once you have entered you MAC address, click on **Apply**

Wireless->MAC Filter [Help]

WLAN MAC Filter

Access Control List Mode (ACL Mode) Allow ▾

MAC Address 1

MAC Address 2

MAC Address 3

MAC Address 4

MAC Address 5

MAC Address 6

MAC Address 7

MAC Address 8

MAC Address 9

MAC Address 10

MAC Address 11

MAC Address 12

MAC Address 13

MAC Address 14

MAC Address 15

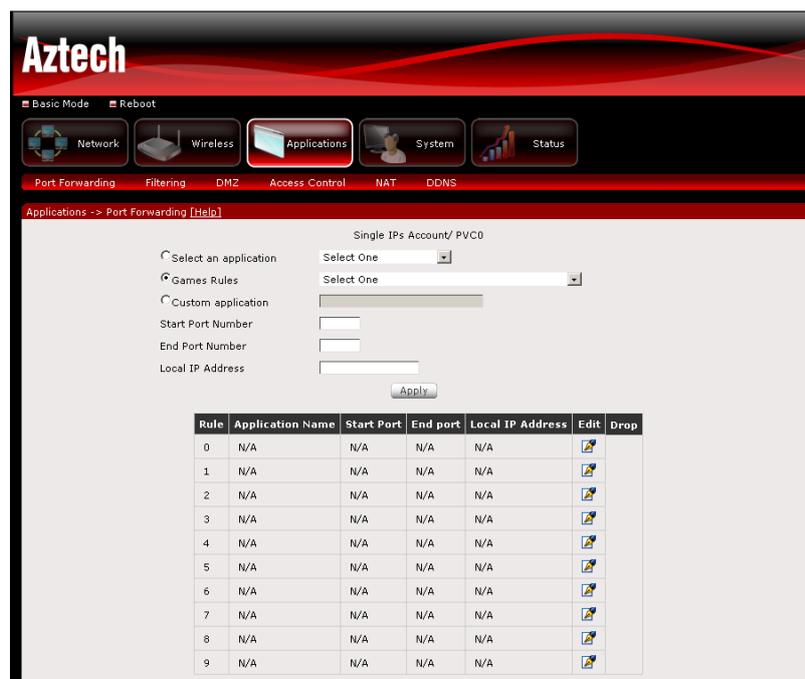
MAC Address 16

Apply

Applications

Port Forwarding

Port Forwarding allows you to direct incoming traffic from the Internet to a specific computer in your local network. A maximum 9 entries can be configured.



As an example, to setup a FTP server on a computer using 10.0.0.88 as its IP Address, select a suitable **Rule Index**, Select the **Select an Application radio** button, select FTP Server as Service and enter 10.0.0.88 as the Server **Local IP Address**. Select TCP, UDP or Both from the **Protocol** list as appropriate, and click **Apply**. If the service you want to setup is not available from the **Select a Application** or **Game Rules** drop-down list, you can define your own Port Forwarding rule by selecting **Custom Application** and giving the rule a name in the provided text box. Then you should enter the **Public** (ports that are accessed on the Wan IP) and **Private** port (ports that the WAN ports will be forwarded to on the LAN) ranges. You should then select the appropriate **Protocol** and click **Apply** to save.

IP Filtering

The router supports IP Filtering, which allows you to easily set up rules to control incoming and outgoing Internet traffic. This filter is able to block both incoming and outgoing traffic based on MAC address, IP address, URL or certain applications. This can be a useful function for instance to prevent your children/employees from accessing social networking during homework/work time, or restricting FTP downloads to after hours.

IP/MAC Filtering

The router supports IP/MAC Filtering, which allows you to easily set up rules to control incoming and outgoing Internet traffic. Choose IP/MAC from the Rule Type drop down box to configure IP/MAC Filtering.

#	Active	Interface	Direction	Src Address/ Mask	Dest Address/ Mask	MAC Address	Src Port	Dest Port	Protocol	Block Schedule	Delete
1	Yes	PVC0	Both	192.168.1.2/ 255.255.255.0	0.0.0.0/ 0.0.0.0	N/A	0 ~ 0	0 ~ 0	ALL	Wed 17:00~17:05	
2	Yes	PVC0	Both	N/A/ N/A	N/A/ N/A	00:11:11:B5:FC:95	N/A	N/A	N/A	Wed 17:15~17:20	

IP Filter Rule Index Select a suitable index for the filter rule.

Interface Select the WAN interface that you wish the filter rule to be active on.

Direction Select the direction that the filter rule will filter traffic in – Incoming, Outgoing or Both.

Rule Type Select whether you will be filtering on IP or MAC. If you select MAC, then all you will need to do is enter the MAC address of the device to be blocked, and the day/time that the blocking must start and stop. If you select to filter on **IP** you will need to fill in the following:

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.

Protocol Select the IP protocol to block.

You can also select a time schedule should you wish this to be a time –conditional rule.

Day Click to select the days on which to apply the restriction.

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

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

Click **Add Rule** to save the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

Click Delete button to delete a corresponding rule.

Application Filter

Application Filter provides control on popular applications to be allowed or denied access to local clients. Check the box of applications that you want to allow to be accessed by local clients and uncheck those that you want to deny.



URL Filter

URL Filter enables you to block certain websites. Select a URL Index, activate the service, and enter the URL of the website that you want to block. Click the Apply button to commit the settings. A maximum of 16 entries can be configured.



Click Delete button to delete a corresponding rule.

DMZ Host

If a computer is assigned as a DMZ Host, it will receive all the data from the Internet that does not belong to the list of applications configured in Port Forwarding. Essentially all requests to any port that is not otherwise used by the router will be forwarded to the DMZ IP. Enter the LAN IP address of the PC you wish to set as DMZ Host in the provided box and click Apply. 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.



Access Control

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



By default, all listed services are accessible from the LAN, and none are accessible from the WAN. If for instance you wish to be able to Telnet into your router from the Internet, you would need to select the Telnet checkbox under the WAN column. This should be used with caution since the router configuration is then at risk of attack from hackers.

Click Delete button to delete a corresponding rule.

NAT (Network Address Translation)

This page allows you to enable/disable NAT on the router.



Should you wish to enable/disable NAT on only one particular WAN interface, this can be done on the **Network, Internet** page of the relevant connection.

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 Dynamic DNS service from one of the listed providers.



Each provider requires a slightly different configuration, so you may need to consult your DDNS provider's website to confirm how to set your router up.

Port Mapping

Port mapping is a useful method for mapping a particular physical port to a particular ATM virtual circuit. If you are using a ATM VC connection to provide an isolated channel, you will be able to use this function to allocate a particular Ethernet (or WLAN) port as an endpoint to this channel.

Router Features -> Port Mapping [Help]

Active Activated Deactivated

Group Index 0 ▾

ATM VCs Port # 0 1 2 3 4 5 6 7

Ethernet Port # 1 2 3 4

WLAN Port # 1

Apply Delete

Router Features -> Port Mapping Summary

Group ID	Group port
----------	------------

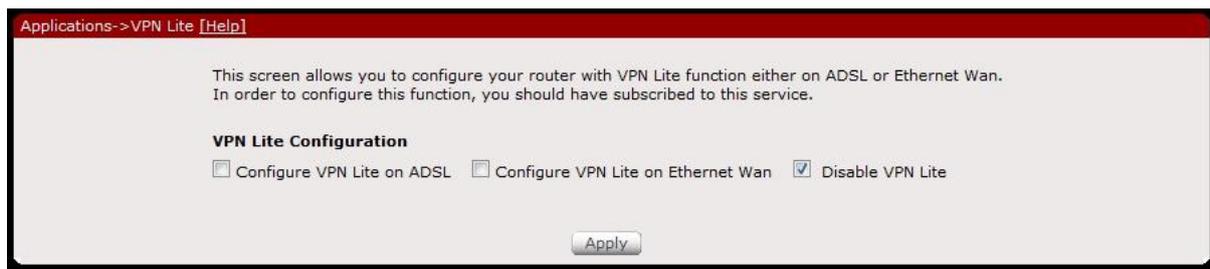
VPN Lite

VPN lite is a service provided by Telkom to allow you to connect multiple sites (nodes) together as if they were on the same physical LAN. These sites can be physically anywhere on the Telkom ADSL network, but will from a data point of view appear as if they are all on the same physical site. This will allow the use of a common server and server based applications, direct printing to local printers, and sharing of data without affecting your internet cap.

Before you configure this, you will need to subscribe to the function, and be provided with a set of PPP username and password as well as IP address and netmask for each node.

The VPN lite function is configured exactly the same as you would configure an internet PPP connection, except that there is also a set of rules that must be added to the routing table to allow all nodes to be able to talk to each other. This is essentially that all of the non-internet routable IP address ranges (for example 10.x.x.x, 192.168.x.x), except the local network are router over the WPN lite PPP connection. There are also some changes required to the firewall.

Fortunately, we have provided a utility to make this configuration easier.



Applications->VPN Lite [Help]

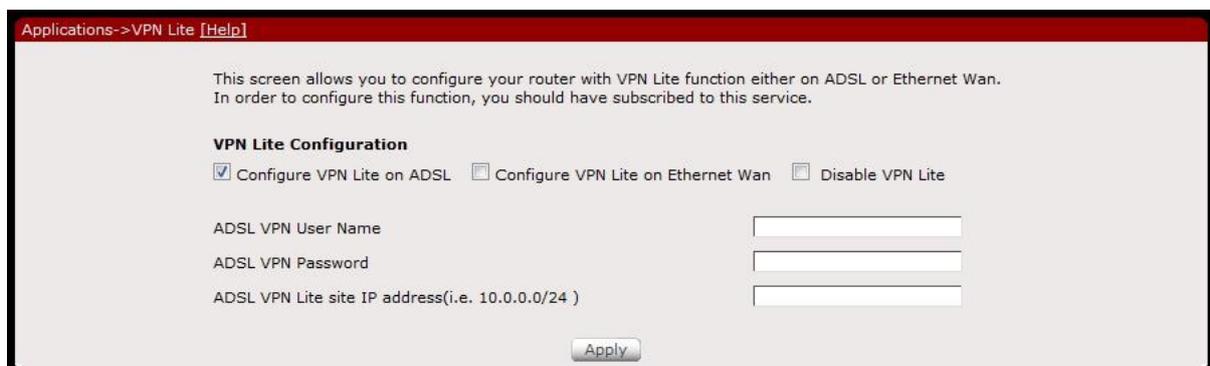
This screen allows you to configure your router with VPN Lite function either on ADSL or Ethernet Wan.
In order to configure this function, you should have subscribed to this service.

VPN Lite Configuration

Configure VPN Lite on ADSL Configure VPN Lite on Ethernet Wan Disable VPN Lite

Apply

This configuration can be easily set using the **Applications, VPN Lite** page. On this page you can configure the VPN Lite node. You have the choice of setting this function on The ADSL port, ETH WAN port, or disabling it. Due to routing constraints, you cannot have it active on both WAN types at the same time, though you can configure both and use the utility to switch between them, if required. Our ADSL connection will automatically be set up using PVC1 and the Eth WAN connection will be set up on PVC6. Although you will be able to make changes in the Internet page to these PVC configuration, we do not suggest that you do this since the routing table will not be updated accordingly. We suggest that you only use this utility to make any changes to the VPN Lite configuration.



Applications->VPN Lite [Help]

This screen allows you to configure your router with VPN Lite function either on ADSL or Ethernet Wan.
In order to configure this function, you should have subscribed to this service.

VPN Lite Configuration

Configure VPN Lite on ADSL Configure VPN Lite on Ethernet Wan Disable VPN Lite

ADSL VPN User Name

ADSL VPN Password

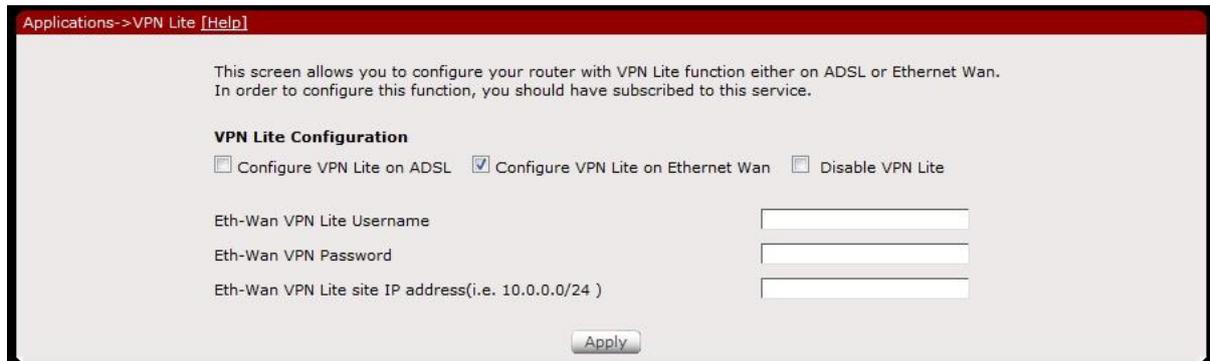
ADSL VPN Lite site IP address(i.e. 10.0.0.0/24)

Apply

To configure VPN lite on the ADSL interface, select **Configure VPN Lite on ADSL** and enter the details provided.

Click **Apply** to save

For configuring the service on the Eth Wan line, select Configure VPN lite on Ethernet WAN tab, and fill in the supplied details



Click **Apply** to save

System Information

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



UPnP

This page allows you to enable/disable UPnP feature on the router.



Settings

This page helps you do work with your user defined settings.

Backup:

To back your routers settings up 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 romfile.cfg.

Restore:

To import a previously saved configuration file from your PC and update the settings of your router, click **Browse** to locate the **romfile.cfg** settings file. Then click the **Restore** button.

Factory Reset:

To restore your router to its original factory default settings, click the **Reset** button. When prompted, click **OK**. Your router will restart, and once it is booted up again, it will have lost any settings changes that you have made, and will have the same settings that were configured when you purchased it.



Firmware

Should you wish to upgrade the firmware in your router to allow support for any additional features, you can do the following.



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

NB: Do not remove the power from your router while updating the firmware. This could result in a corrupted memory, and may mean that your router is not recoverable.

Reboot

This feature allows the router to enable new network configuration to take effect or to clear problems with the router's network connection. Click on **Reboot** and the router will restart with the user defined configuration.



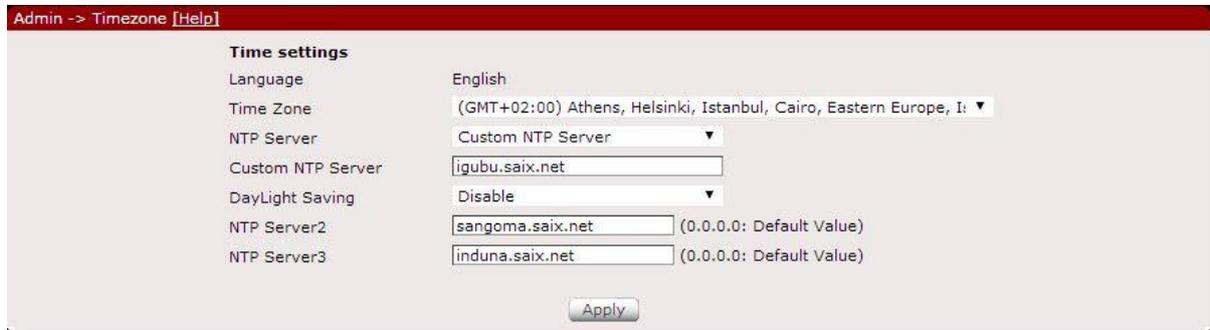
Password

Access to your DSL router Web interface is controlled through a login password. You may change the default password on this page. You may also change the default username.



Timezone

Your router is set to automatically synchronize to the pre-configured internet time servers. On this page you can change the routers time zone or the default servers.



Admin -> Timezone [Help]

Time settings

Language	English
Time Zone	(GMT+02:00) Athens, Helsinki, Istanbul, Cairo, Eastern Europe, I: ▼
NTP Server	Custom NTP Server ▼
Custom NTP Server	<input type="text" value="igubu.saix.net"/>
DayLight Saving	Disable ▼
NTP Server2	<input type="text" value="sangoma.saix.net"/> (0.0.0.0: Default Value)
NTP Server3	<input type="text" value="induna.saix.net"/> (0.0.0.0: Default Value)

FTPAccess

If you have plugged a USB drive into the USB socket, you are able to use this page to control login details and access.



System->FTP Access Control [Help]

FTP User Access	<input type="checkbox"/>
Select User	USER1 ▼
Username	<input type="text" value="user"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>
FTP Access Control	<input type="radio"/> READ <input checked="" type="radio"/> READ/WRITE

Status

Device Statistics

The router will show you detailed statistical information regarding the different connections on your router. This will include statistics for ADSL, WLAN and your LAN

The screenshot shows the Aztech router's web interface. At the top, there are navigation tabs for Network, Wireless, Applications, System, and Status. Below these are sub-tabs for Statistics, ADSL Status, System Log, Diagnostics, and Network Tools. The main content area displays three tables of statistics:

LAN Statistics [Help]										
Interface	Packets	Bytes	TX			RX				
			Multicast Frames	Collision	Error Frames	Packets	Bytes	Multicast Frames	CRC Errors	Under-size Frames
LAN	126753	49384295	1644	0	0	12787	1870067	627	0	0

ADSL Statistics [Help]									
Interface	Packets	TX			RX				
		Bytes	Errors	Blocks	Packets	Bytes	Errors	Blocks	
ADSL	17	1190	123	N/A	0	0	0	0	N/A

WLAN Statistics [Help]						
Interface	Packets	TX		RX		
		Errors	Dropped	Packets	Errors	Dropped
Wireless	3	0	0	1519769	205999	0

ADSL Status

The router shows detailed status information of its DSL connection.

The screenshot shows the Aztech router's web interface with the ADSL Status page selected. The page displays detailed information about the DSL connection in two tables:

ADSL Description	Status
ADSL Mode	UP
ADSL Status	ITU G.992.5(ADSL2PLUS)
Cell Delin	0
Link Retrain	4
Init Errors	3
Init Timeouts	0
Loss Of Framing	0
Errored Seconds	0
Severely Error Seconds	0
HEC Error	0

Information	DownStream	Upstream
SNR Margin	6.6 db	5.9 db
Attenuation	1.9 db	4.6 db
Data Rate	24413 kbps	1133 kbps
Forward Error Correction Seconds	3051	6
CRC	0	0

System Log

System log shows detailed information about the processes running on the router.



Diagnostics

Your Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "**Re-run 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. Note: Not all tests are supported by all ISPs, so please ensure that your particular failure is actually a problem before investigating further.



Network Tools

Network tools will help you troubleshoot Internet connection problems by verifying your connection. Currently **Ping** and **Traceroute** are supported.



Safety Precautions

- Do not open, service, or change any component.
- Only qualified technical specialists are allowed to service the equipment.
- Observe safety precautions to avoid electric shock
- Check voltage before connecting to the power supply. Connecting to the wrong voltage will damage the equipment.

FCC Notice

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

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

Modifications

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

This device complies with Part 15 of the FCC rules.

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

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

Exposure Information to Radio Frequency Energy

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

15.19:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device does not cause harmful interference.(2)this device must accept any Interference received, including interference that may cause undesired operation.

15.21:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Customer Information

1. This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On bottom of this equipment is a label that contains, among other information, a product identifier of [US:4J2DL01BDSL5085EN]. If requested, this number must be provided to the telephone company.
2. If this equipment [ADSL2+ 4-Ports 300Mbps Wireless-N Modem Router] causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
3. The telephone company may make changes in this facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modification to maintain uninterrupted service.
4. If you experience trouble with this equipment, you disconnect it from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.
5. Please follow instructions for repairing if any (e.g. battery replacement section); otherwise do not alternate or repair any parts of device except specified.
6. Connection to party line service is subject to state tariffs. Contact the state public utility commission public service commission or corporation commission for information.
7. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number that this unit is connected to,
 - b. The ringer equivalence number [0.1B]
 - c. The USOC jack required [RJ11C], and
 - d. The FCC Registration Number [US:4J2DL01BDSL5008EN]

Items (b) and (d) are indicated on the label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five (5.0). If too many devices are attached, they may not ring properly.

Service Requirements

In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents.