Atlantis Land

Web Share 3G 244WN

802.11n Wireless ADSL2+/3G Router

User Manual

www.atlantis-land.com

INDEX

Copyright Statement

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

·On board of airplanes, or

·In an explosive environment, or

·In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user’s authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

Copyright Statement

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user’s authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

CE Mark Warning

In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.
France: except the channel 10 through 13, law prohibits the use of other channels.

CE/EMC Restriction of Liability

The product described in this handbook was designed, produced and approved according to the EMC-regulations and is certified to be within EMC limitations.
If the product is used in an uncertified PC, the manufacturer undertakes no warranty in respect to the EMC limits. The described product in this handbook was constructed, produced and certified so that the measured values are within EMC limitations. In practice and under special circumstances, it may be possible, that the product may be outside of the given limits if it is used in a PC that is not produced under EMC certification. It is also possible in certain cases and under special circumstances, which the given EMC peak values will become out of tolerance. In these cases, the user himself is responsible for compliance with the EMC limits.

Declaration of Conformity

This equipment has been tested and found to comply with Directive 1999/5/CE of the European Parliament and of the Council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. After assessment, the equipment has been found to comply with the following standards: EN 300.328 (radio), EN 301 489-1, EN 301 489-17 (electromagnetic compatibility) and EN 60950 (safety). This equipment may be used in all European Union contries and in all countries applying Directive 1999/5/CE, without restriction, with the exception of the following countries:

France (FR): When this equipment is used outdoors, output power is limited to within the frequency bans listed on the chart. For more info, consult the website *www.art-telecom.fr.*

Location	Frequency Band (MHz)	Power (EIRP)
Indoor (no restriction)	2400-2483,5	100mW(20dBm)

Outdoor	2400-2454
	2454-2483,5
		100mW(20dBm)
		10mW(10dBm)

Italy(IT): For more info, consult the website *www.comunicazioni.it*

Luxembourg: General authorization requie for network and service supply.

Norway (NO): This subsection does not apply for geographical area within a radius of 20 km from the center of Ny Alesund.

Russia (CCP): only for indoor application.

Declaration of Conformity CE

Hereby, Sidin SpA, declares that this product (A02-RAU244-W300N) is in compliance to all relevant essential requirements of R&TTE Directive (99/5/CE). CE Declaration is available on the web site www.atlantis-land.com.

Important information for the correct recycle/treatment procedures of this equipment

The mentioned information are reported herewith in compliance with directive 2002/95/CE, 2002/96/CE and 2003/108/CE which requires a separate collection system and specific treatment and disposal procedures for the waste of electric and electronic equipments.

The crossed-out wheeled bin symbol printed on the unit label or unit packaging indicates that this equipment must not be disposed of as unsorted municipal waste but it should be collected separately.

The waste of electric and electronic equipment must be treated separately, in order to ensure that hazardous materials contained inside the equipment are not buried thereby providing potential future problems for the environment and human health. Moreover, it will be possible to reuse and recycle some parts of the waste of electric and electronic equipment, contributing to reduce the quantities of waste to be disposed of and the depletion of natural resources.

As user of this equipment, you are responsible to contact the producer to know the correct procedure in the separate collection system for the waste of electric and electronic equipments.

Your rôle in participating to the separate collection of waste of electric and electronic equipment is essential to ensure that environmental protection and human health objectives connected to a responsible treatment and recycling activities are achieved.

1. Introduction

1.1 An Overview of WebShare 3G 244WN

Welcome to the WebShare 802.11n 3G/ ADSL2+ (VPN) Firewall Router. The router is an “all-in-one” ADSL router, combining an ADSL modem, ADSL router and Ethernet network switch functionalities, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection. With features such as an ADSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

1.2 Package Contents

Unpack the package and check all the items carefully. If any item contained is damaged or missing, please contact your local dealer as soon as possible. Also, keep the box and packing materials in case you need to ship the unit in the future. The package should contain the following items:

- 1 x WebShare 3G 244WN
- 1 x Power Supply
- 1 x Cat 5 LAN cable (RJ-45 connector)
- 1 x Phone cable (RJ-11 connector)
- 1 x PS2-RS 232 console cable
- 3 x detacheable antennas (2.2 dBi gain)
- 1 x Multilanguage Quick Start Guide (English, Italian and Francais)
- 1 x Cd-Rom with driver, utility and multilanguage manual
- 1 x Warranty Card
- 1 x WEEE Disclaimer

If any item is found missing or damaged, please contact your local reseller for replacement.

1.3 Features

Technical charateristics of WebShare 3G 244WN:

- ***Express Internet Access:*** This router complies with worldwide ADSL standards. It supports downstream rates of up to 12/24 Mbps with ADSL2/2+, 8 Mbps with ADSL, and upstream rates of up to 1 Mbps. With this technology, users enjoy not only high-speed ADSL service but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much more quickly and easily than ever. In particular, by doubling the upstream data rate, the Annex M standard included in the WebShare 3G 244WN supports the latest ADSL2/2+ for higher upload speeds.
- ***802.11n Wireless AP with WPA Support:*** With an integrated 802.11n Wireless Access Point in the router, the device delivers up to 6 times faster speeds and 3 times farther range than an 802.11b/g wireless network. It offers a quick yet easily accessible and mobile to the users among wired network, wireless network, broadband connection (ADSL). In addition to having a 300Mbps. data rate, it is also backward compatible with existing 802.11b/11g equipments. The supported features of Wireless Protected Access (WPA-PSK/ WPA2-PSK) and Wireless Encryption Protocol (WEP) enhance the security level of data protection and access control via Wireless LAN.
- ***Fast Ethernet Switch:*** A 4-port 10/100/1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T, 100Base-TX and 1000Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.
- ***Multi-Protocol to Establish a Connection:*** It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.
- ***Quick Installation Wizard:*** It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.

- ***Universal Plug and Play (UPnP) and UPnP NAT Traversal:*** This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.
- ***Network Address Translation (NAT):*** Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.
- ***SOHO Firewall Security with DoS and SPI:*** Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the private LAN.
- ***Domain Name System (DNS) Relay:*** It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.
- ***Dynamic Domain Name System (DDNS):*** The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.
- ***Quality of Service (QoS) :*** QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router ay lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring

client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

- ***Virtual Server (Port Forwarding):*** Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.
- ***Rich Packet Filtering:*** Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.
- ***Dynamic Host Configuration Protocol (DHCP) Client and Server:*** In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- ***Static and RIP1/2 Routing:*** It has routing capability and supports easy static routing table or RIP1/2 routing protocol.
- ***Simple Network Management Protocol (SNMP):*** It is an easy way to remotely manage the router via SNMP.
- ***Web based GUI:*** It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.
- ***Firmware Upgradeable:*** Device can be upgraded to the latest firmware through the WEB based GUI.
- ***Rich Management Interfaces:*** It supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

2. Using WebShare 3G 244WN

2.1 Cautions for using the WebShare 3G 244WN

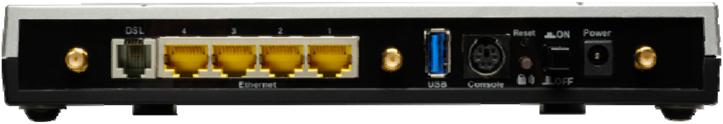
- Do not place the Router under high humidity and high temperature.
- Do not use the same power source for Router with other equipment.
- Do not open or repair the case yourself.
- If the Router is too hot, turn off the power immediately and have a qualified serviceman repair it.
- Place the Router on a stable surface.
- Only use the power adapter that comes with the package.
- Do not upgrade firmware using a wireless connection.

2.2 The Front LEDs

LED	MEANING
Power	• Lit when power turns ON. • Lit in red means POST (Power On Self Test) failure (non-bootable) or device malfunction.
Ethernet (1-4)	• Lit when one of LAN ports are connected to Ethernet devices. If the speed of transmission hits 1000Mbps light will appear Green; If the speed of transmission hits 100Mbps light will appear Orange. If the speed of transmission hits 10Mbps, light will not shine.

	• Blinking when data is Transmitted / Received.
USB	• Lit green when the device is connected to a USB device and ready. • Flashing when the device is sending/receiving data.
Wireless	• Lit green when the wireless connection is established. • Flashing when the device is sending/receiving data. • Flashes steadily when the WPS is active.
DSL	Lit Green when the device is successfully connected to an ADSL DSLAM (“line sync”).
Internet	• Lit red when WAN port fails to get IP address. • Lit green when WAN port gets IP address successfully. • Flashing green when IP traffic flows through the device. • Lit off when the device is in the bridged mode or when ADSL connection is not present.

2.3 The Rear Ports



PORT	MEANING
Antenna (3)	Connect the detachable antenna to this port.

DSL	Connect the supplied RJ-11 (“telephone”) cable on this port when connecting to the ADSL/telephone network.
Ethernet (1-4)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network of 10Mbps, 100Mbps or 1000Mbps.
USB	Connect the USB cable on this port 3G/ HSDPA USB modem backup for Internet access.
Console	Console port.
WPS	Push WPS button to trigger Wi-Fi Protected Setup function.
Reset	To be sure the device is being turned on → press RESET button for: • **1-3 seconds:** quick reset the device. • **6 seconds above, and power off, power on the device:** restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.
Power	Power ON/OFF switch
Power Switch	Connect the supplied power adapter to this jack.

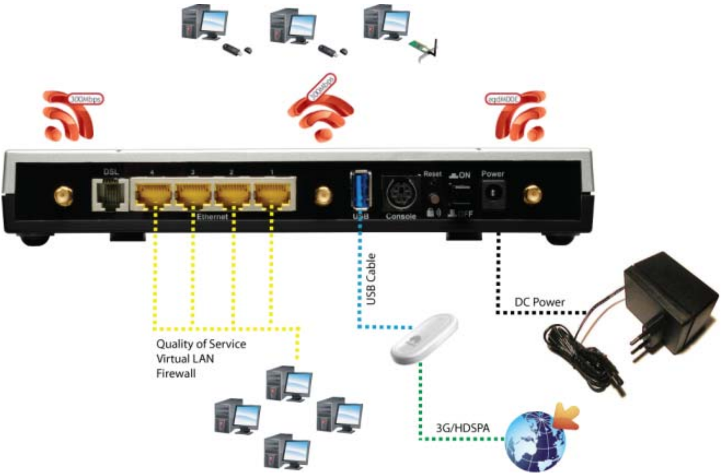
2.4 Cabling and operationa modes

WebShare 3G 244WN can be set in 3 difference mode: ADSL only, 3G only or ADSL main with 3G backup.

2.4.1 Single WAN ADSL

In this mode, WebShare 3G 244WN works as a standard ADSL2+ Router.
Follow the followings steps to cabling the device:

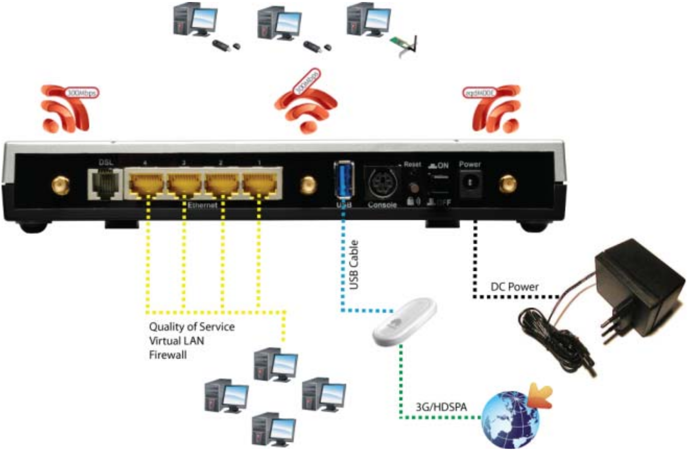
- Connect WAN Port to the telephone line throught RJ-11 cable (contained in package).
- Connect AC-DC Adapter on AC and on device (POWER jack) in the reat r of the product.



2.4.2 Single WAN 3G

In this mode, WebShare 3G 244WN works using an external 3G/HDSPA USB modem to connect the LAN to Internet.
Follow the followings steps to cabling the device:

- Connect the 3G USB modem on the USB 2.0 port on the rear panel of the product.
- Connect AC-DC Adapter on AC and on device (POWER jack) in the reat r of the product.

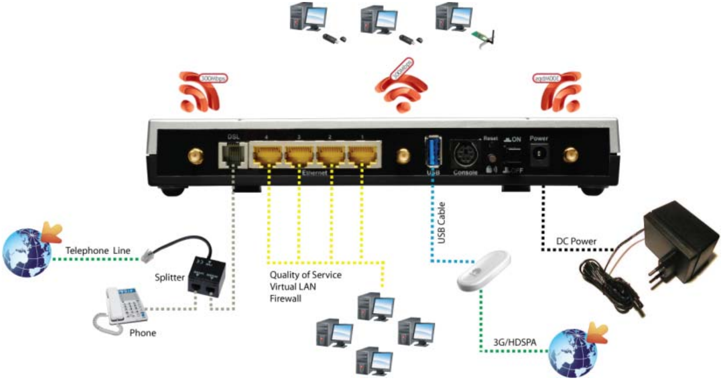


The modem USB 3G/HDSPA is not included to the package contents.
Please check APPENDIX F for a list of compatible devices.

2.4.3 Dual WAN ADSL/3G with backup mode

In this mode, WebShare 3G 244WN works using ADSL as main connection. In case of failover of the main connection, WEbShare 3G 244WN automatically backup it to an external 3G/HDSPA USB modem, in order to provide an always-on connection for the LAN devices.
Follow the followings steps to cabling the device:

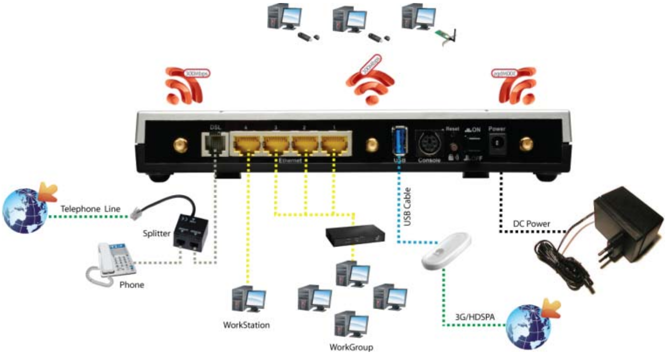
- Connect WAN Port to the telephone line throught RJ-11 cable (contained in package).
- Connect the 3G USB modem on the USB 2.0 port on the rear panel of the product.
- Connect AC-DC Adapter on AC and on device (POWER jack) in the reat r of the product.



The modem USB 3G/HDSPA is not included to the package contents.
Please check APPENDIX F for a list of compatible devices.

2.4.4 Cabling the LAN connection

In this mode, WebShare 3G 244WN can be connected to an existing LAN or can be use to create a new local area network.
Is possible to connect the WebShare 3G 244WN through its embedded Gigabit Ethernet switch or by its embedded Access Point (based on 802.11n specifications), using a wireless client like NetFly 300 series.



Once you've checked all the connections and you've switched on the Router the product will carry on immediately a diagnosis (about 10 seconds). Finished this, the Led **PWR** will be fixed green and **LAN** and **Wireless** will blink green; DSL will blink during sinchonization, and will be fixed when ADSL line is synchronized with WebShare Router. If Led DSL blink continuously, please contact Your ISP in order to check ADSL line state.
Ensure that all other devices connected to the same telephone line as your WebShare (e.g. telephones, fax machines, analog modems) have a line filter (**A01-AF2**) connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around.

3. Basic Installation

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, or IPoA. Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI and VCI VC-based / LLC-based multiplexing Username and Password Service Name
PPPoA	VPI and VCI VC-based / LLC-based multiplexing Username and Password
RFC1483 Bridged	VPI/VCI VC-based / LLC-based multiplexing
RFC1483 Routed	VPI/VCI VC-based / LLC-based multiplexing IP address Subnet mask Default Gateway (IP address) IP address (DNS)

3.1 Factory Default Setting

Before configuring your, you need to know the following default settings:

- Username: **admin**
- Password: **atlantis**
- LAN IP Address: **192.168.1.254**
- Subnet Mask: **255.255.255.0**
- ISP setting in WAN side: **PPPoA, VCMux, Routing, VPI=8, VCI=35**
- SSID: **A02-RAU244-W300N**, Security: **WPA-PSK**
- WPA Passphrase: **WebShare244WN**
- **DHCP Server enabled** with IP pool from 192.168.1.100 to 192.168.1.199

⚠ If you ever forget the password to log in, you may press the RESET button up to 6 seconds to restore the factory default settings.

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

Wireless LAN Interface	
SSID	A02-RAU244-W300N
Security	WPA-PSK
WPA Passphrase	WebShare244WN
Wireless Mode	802.11n (20/40MHz)
LAN Interface	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	Enabled
DHCP Server IP Pool	From 192.168.1.100 to 192.168.1.100
WAN Interface	
Encapsultation	PPPoA
Multiplexing	VC-Mux
Mode	Routing
VPI/VCI	8/35

3.2 TCP/IP Configuration

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to uninstall any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

NOTE: Any TCP/IP capable workstation can be used to communicate with or through the WebShare Router. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring PC (Windows 2000)

1. Go to **Start** -> **Settings** -> **Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connection**s.
2. Double-click **LAN Area Connection**.
3. In the LAN Area Connection Status window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

Configuring PC (Windows XP)

1. Go to **Start** -> **Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**.
3. In the LAN Area Connection Status window, click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration

Configuring PC (Windows Vista)

1. Go to **Start** -> **Control Panel** (in Classic View). In the Control Panel, double-click on **Network and Sharing Center** icon.
2. Click **Manage Network connections** then double-click Local Area Connection. Click **Properties**.
3. Click **Continue** (Windows needs your permission to continue).
4. Select **Internet Protocol Version 4 (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

Configuring for MAC

1. Click on **Apple** Menu and select **Control Panel/TCP/IP**. It will appear the follow screen.
2. Select **Ethernet** on **Connect Via**.
3. Select **Using DHCP Server** on Configure.
4. Leave empty the field **DHCP Client ID**.

Configuration for Linux client (KDE Interface)

1. Activate **System Settings** menu.
2. Select **Network Settings** from **Network and Connectivity** menu.
3. Select **eth0** interface and click on **Configure Interface**.
4. Check **Automatic** option and select the **DHCP** mode from TCP/IP menu.

3.3 Verification of TCP/IP Configuration

To verify your correct configuration (after PC restart, necessary for Windows 98, 98Se, ME and instead enough obtain IP lease for XP, 2000),use ping command. From a DOS Window, type:

```
ping 192.168.1.254
```

If It show you this message:

```
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
Reply from 192.168.1.254: bytes=32 times<10ms TTL=64
```

It i s possibile to continue to follow step. If it show you follow message:

```
Pinging 192.168.1.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Check that LAN LED is lit (change CAT cable if is not). Check PC IP Address typing **winipcfg** for (Win95,98,ME) or **ipconfig** (for Win2000,XP) and eventually re-install TCP/IP stack.

3.4 Browser Configuration

Now open IE, go to **Instruments** menu, select the **Connections** tab and select one of the following options:

- Never use remote connection
- Use remote connection if another network connection isn't available

3.5 Configuring with Web Browser

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**. The default username and password are **admin** and **atlantis**.
WebShare 3G 244Wn includes two different management interfaces, Basic or Advanced. In this manual are explained all features included on **Advanced** interface.

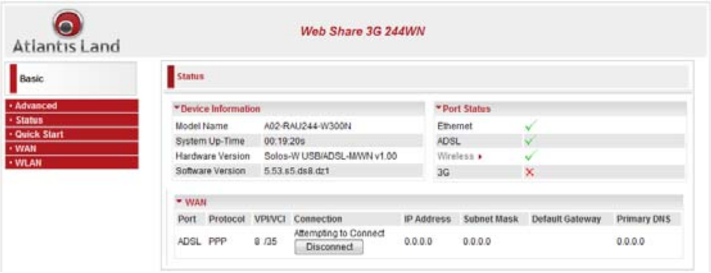
NOTE: Menus contained into Basic interfaces are also included on Advanced.

4. Management Interface

When you login into the management interface, WebShare 3G 244WN will show a simplified interface for configuring standards parameters needed to access on Internet. It is also possible to access to an advanced management interface for deep configurations.
In this user guide will are explains all parameters for **Advanced** interface. All fields shows on **Basic Setup** can be find on **Advanced Setup** as following:

Basic Setup	Advanced Setup
Status	Status
Quick Start	Quick Start
WAN	Configuration - WAN – WAN Profile
WLAN	Configuration – LAN - Wireless

After login, the WebShare 3G 244WN will show this screen:



Device Information

Model Name	A02-RAU244-W300N
System Up-Time	00:19:20s
Hardware Version	Solos-W USB/ADSL-M/WN v1.00
Software Version	5.53.s5.ds8.dz1

Port Status

Ethernet	✓
ADSL	✓
Wireless ▸	✓
3G	✗

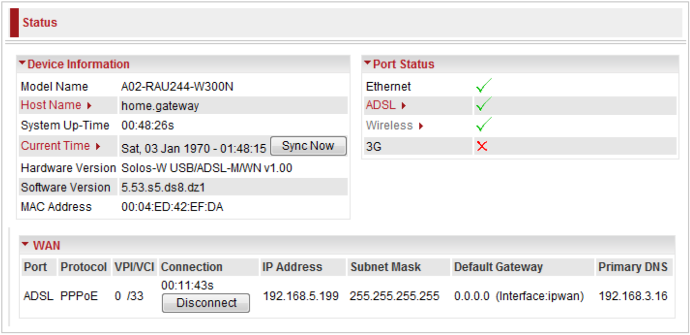
WAN

Port	Protocol	VPI/VCI	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPP	8 /35	Attempting to Connect Disconnect	0.0.0.0	0.0.0.0		0.0.0.0

Click on **Advanced** button to activate the advanced management interface.

5. Status

In this section there are shown all parameters about LAN, WLAN, USB and ADSL interfaces.



Status

Device Information

Model Name	A02-RAU244-W300N
Host Name ▸	home.gateway
System Up-Time	00:48:26s
Current Time ▸	Sat, 03 Jan 1970 - 01:48:15 Sync Now
Hardware Version	Solos-W USB/ADSL-M/WN v1.00
Software Version	5.53.s5.ds8.dz1
MAC Address	00:04:ED:42:EF:DA

Port Status

Ethernet	✓
ADSL ▸	✓
Wireless ▸	✓
3G	✗

WAN

Port	Protocol	VPI/VCI	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPPoE	0 /33	00:11:43s Disconnect	192.168.5.199	255.255.255.255	0.0.0.0 (Interface:ipwan)	192.168.3.16

Device Information

Field	Description
Model Name	Show the model code for WebShare 3G 244WN.
Host Name	Show the name of the device that will be find from others LAN clients.
System Up-Time	Show the up-time of the device from last restart.
Current Time	Show the current time. WebShare 3G 244WN hasn't an internal clock, then is necessary to set the SNTP client embedded to synchronize the Router's date with an external SNTP server.
Hardware Version	Show the hardware version for the device.
Software Version	Show the firmware version. Please check it before make any firmware upgrade.
MAC Address	Show the MAC Address associated to the LAN interface.

Port Status

Field	Description
Ethernet	Show Ethernet interface status.
ADSL	Show ADSL line status.
Wireless	Show Wireless interface status.
3G	Show 3G/HDSPA connection status.

WAN

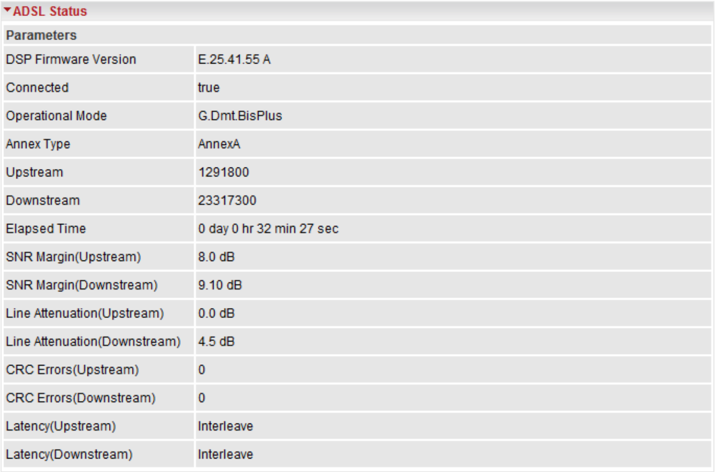
Field	Description
Port	Show the interface using for this connection.
Protocol	Show the encapsulation method.
VPI/VCI	Show VPI/VCI value for each connection profile.
Connection	Show the up-time for each connection.
IP Address	Show IP Address assigned to the WAN interface.
Subnet Mask	Show the subnet mask assigned to the WAN interface.
Default Gateway	Show the default gateway assigned to the WAN interface.
Primary DNS	Show the primary DNS server.

Clicking on **Port Status,** it is possible to configure each interfaces (wireless, ethernet, ADSL and 3G) parameters and see its status.

Click **Sync Now** to synchronize the Router's clock with an external SNTP server (to configure SNTP parameters, please go to **Configuration – System – Time Zone**); using **Connect/Disconnect** button to manage manually the PPP connection.

5.1 ADSL Status

This section displays the ADSL overall status, which shows a number of helpful information such as DSP firmware version.



▾ADSL Status

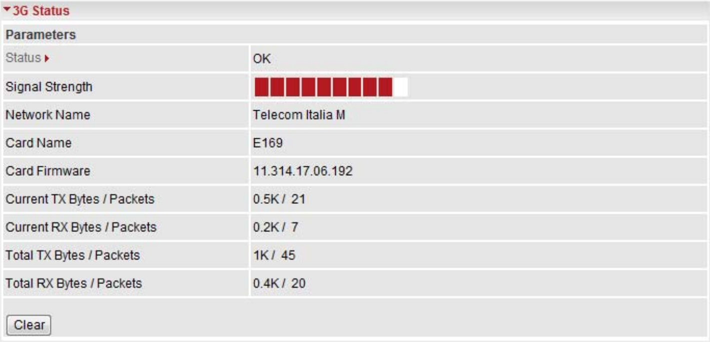
Parameters	
DSP Firmware Version	E.25.41.55 A
Connected	true
Operational Mode	G.Dmt.BisPlus
Annex Type	AnnexA
Upstream	1291800
Downstream	23317300
Elapsed Time	0 day 0 hr 32 min 27 sec
SNR Margin(Upstream)	8.0 dB
SNR Margin(Downstream)	9.10 dB
Line Attenuation(Upstream)	0.0 dB
Line Attenuation(Downstream)	4.5 dB
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	Interleave
Latency(Downstream)	Interleave

5.2 3G Status

This section displays the 3G Card's overall status, which shows you a number of helpful information such as the current signal strength and statistics on current and total bytes transferred and received.

3G USB Modem is not included with WebShare 244WN.
WebShare 3G 244WN can works only with a compatible device.
Please check the modem compatibility on the website www.atlantis-

land.com or with the compatibility list provided with the WebShare 244WN.



3G Status

Parameters	
Status	OK
Signal Strength	█████████░
Network Name	Telecom Italia M
Card Name	E169
Card Firmware	11.314.17.06.192
Current TX Bytes / Packets	0.5K / 21
Current RX Bytes / Packets	0.2K / 7
Total TX Bytes / Packets	1K / 45
Total RX Bytes / Packets	0.4K / 20

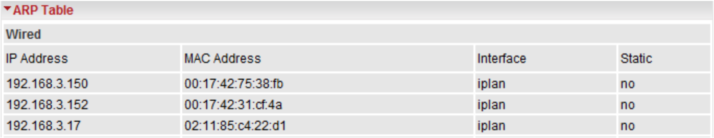
Field	Description
Status	Show the status for 3G interface: • **3G Card ready:** Modem recognized, connection unactive. • **Connect:** Modem recognized, connection active. • **Closed:** Modem recognized and disconnected after ADSL connection failback. • **KO:** Modem not compatible or fault.
Signal Strenght	The signal strength bar indicates current 3G signal strength.
Network Name	The network name that the device is connected to.
Card Name	The name of the 3G card.
Card Firmware	The current firmware for the 3G card.
Current TX/RX Bytes	The statistics of transmission, count for this call.
Total TX/RX Bytes	The statistics of transmission, count from system ready

5.3 iBurst Status

This section show specific parameters for iBurst Wireless client.

5.4 ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



ARP Table

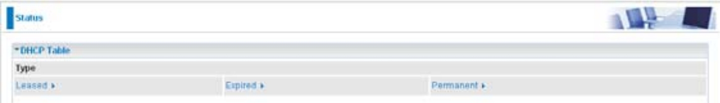
Wired

IP Address	MAC Address	Interface	Static
192.168.3.150	00:17:42:75:38:fb	iplan	no
192.168.3.152	00:17:42:31:cf:4a	iplan	no
192.168.3.17	02:11:85:c4:22:d1	iplan	no

Wired

Field	Description
IP Address	A list of IP addresses of devices on your LAN (Local Area Network).
MAC Address	The MAC (Media Access Control) addresses for each device on your LAN.
Interface	The interface name (on the router) that this IP Address connects to.
Static	Static status of the ARP table entry: • **No:** for dynamically-generated ARP table entries. • **Yes:** for static ARP table entries added by the user.

5.5 DHCP Table



Status

▾DHCP Table

Type		
Leased ▸	Expired ▸	Permanent ▸

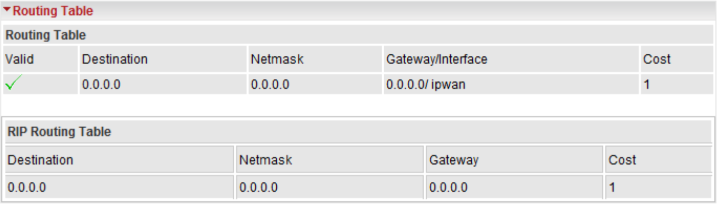
Type

Parametro	Descrizione
Leased	The DHCP assigned IP addresses information.
Expired	The expired IP addresses information.
Permanent	The fixed host mapping information.

Leased Table, Expired Table, Permanent Table

Parametro	Descrizione
IP Address	The IP address that assigned to client.
MAC Address	The MAC address of client.
Client Host Name	The Host Name (Computer Name) of client.
Expiry	The current lease time of client.

5.6 Routing Table



▾Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Table

Destination	Netmask	Gateway	Cost
0.0.0.0	0.0.0.0	0.0.0.0	1

Routing Table

Parametro	Descrizione
Valid	It indicates a successful routing status.
Destination	The IP address of the destination network.

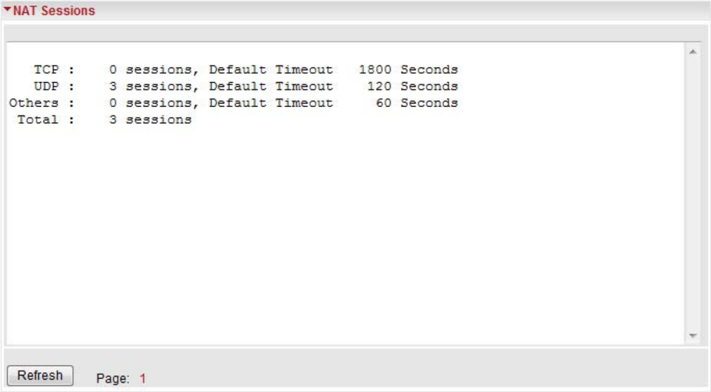
Netmask	The destination Netmask address.
Gateway/Interface	The IP address of the gateway or existing interface that this route will use.
Cost	The number of hops counted as the cost of the route.

RIP Routing Table

Parametro	Descrizione
Destination	The IP address of the destination network.
Netmask	The destination Netmask address.
Gateway/Interface	The IP address of the gateway or existing interface that this route will use.
Cost	The number of hops counted as the cost of the route.

5.7 NAT Sessions

This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).

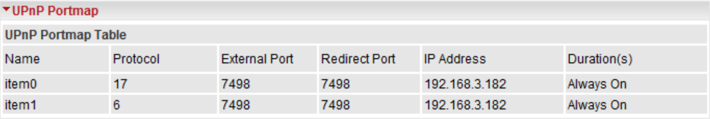


NAT Sessions

```
   TCP :    0 sessions, Default Timeout   1800 Seconds
   UDP :    3 sessions, Default Timeout    120 Seconds
Others :    0 sessions, Default Timeout     60 Seconds
 Total :    3 sessions
```

5.8 UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play. See **Advanced** section of this manual for more details on UPnP and the router's UPnP configuration options.

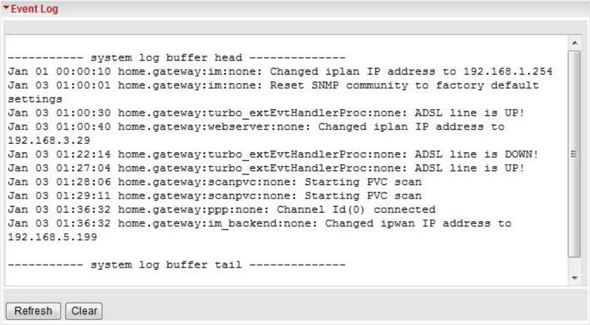


UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address	Duration(s)
item0	17	7498	7498	192.168.3.182	Always On
item1	6	7498	7498	192.168.3.182	Always On

5.9 Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's ADSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.

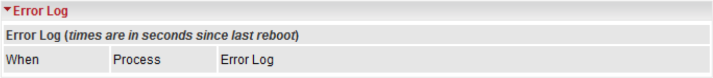


```
----------- system log buffer head --------------
Jan 01 00:00:10 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 01:00:01 home.gateway:im:none: Reset SNMP community to factory default
settings
Jan 03 01:00:30 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is UP!
Jan 03 01:00:40 home.gateway:webserver:none: Changed iplan IP address to
192.168.3.29
Jan 03 01:22:14 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is DOWN!
Jan 03 01:27:04 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is UP!
Jan 03 01:28:06 home.gateway:scanpvc:none: Starting PVC scan
Jan 03 01:29:11 home.gateway:scanpvc:none: Starting PVC scan
Jan 03 01:36:32 home.gateway:ppp:none: Channel Id(0) connected
Jan 03 01:36:32 home.gateway:im_backend:none: Changed ipwan IP address to
192.168.5.199

----------- system log buffer tail --------------
```

5.10 Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.

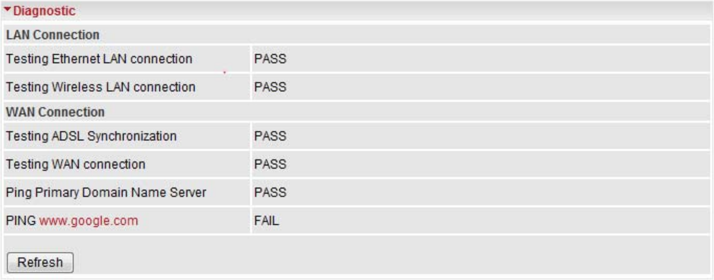


▾Error Log

Error Log (*times are in seconds since last reboot*)		
When	Process	Error Log

5.11 Diagnostic

It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection.



▾Diagnostic

LAN Connection	
Testing Ethernet LAN connection	PASS
Testing Wireless LAN connection	PASS
WAN Connection	
Testing ADSL Synchronization	PASS
Testing WAN connection	PASS
Ping Primary Domain Name Server	PASS
PING www.google.com	FAIL

NOTE: If PING ww.google.com is shown FAIL and the rest is PASS, you ought to check your PC’s DNS settings is set correctly.

6. Quick Start

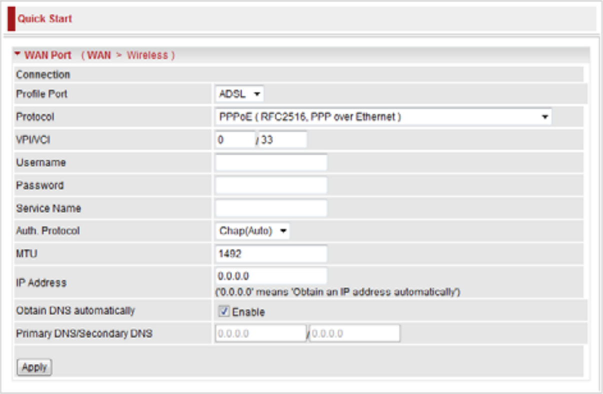
NOTE: ADSL WAN Backup cannot be configured using Quick Start procedure. Please refer **to Advanced – WAN Interface** to set this function.

6.1 Single WAN ADSL Configuration

1. Select **ADSL** from Connect Mode drop-down menu and click **Continue**.

2. If your ADSL line is not ready, you need to check your ADSL line has been set or not.

3. If your ADSL line is ready, the screen appears ADSL Line is Ready. Choose **Auto** radio button and click **Apply**. It will automatically scan the recommended mode for you. Manually mode makes you to set the ADSL line by manual.



Quick Start

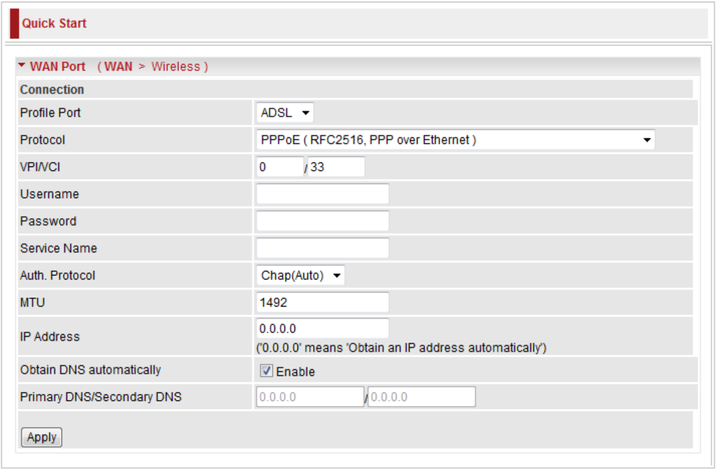
▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL ▾
Protocol	PPPoE (RFC2516, PPP over Ethernet) ▾
VPI/VCI	0 / 33
Username	
Password	
Service Name	
Auth. Protocol	Chap(Auto) ▾
MTU	1492
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

PPPoE / PPPoA

PPPoE (PPP over Ethernet) is an ADSL connection known as dial-up DSL. As the PPPoA it has been created to integrate large band services paying a particular attention to an easy configuration. The user can obtain an high access speed and he can also share the same account with the ISP. No additional software are required. This configuration is valid in case of a subscription with a static IP and active NAT (SUA) (for the managing of the public class turn to the CD handbook). Let's see how to configure correctly this kind of ADSL configuration.

Insert **Username** and **Password** and make sure that the parameters are, in case of **PPPoE**, the ones in the picture, if not specifically shown by the ISP.



Quick Start

▼ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL ▾
Protocol	PPPoE (RFC2516, PPP over Ethernet) ▾
VPI/VCI	0 / 33
Username	
Password	
Service Name	
Auth. Protocol	Chap(Auto) ▾
MTU	1492
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

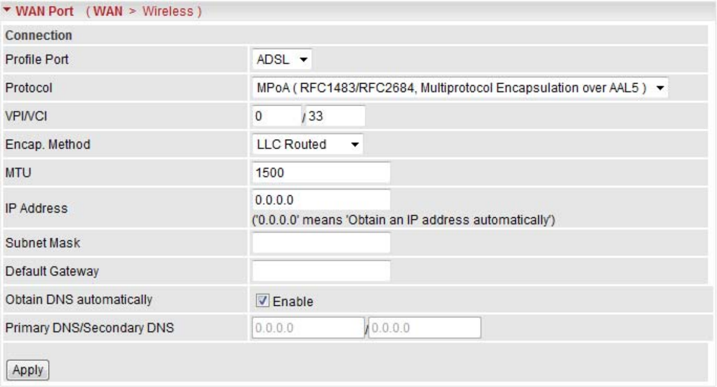
In case of **PPPoA** choose **Protocol=PPPoA(RFC2364, PPP over ALL5**) and insert Username and Password provided by ISP.

Click on **Apply** in order to start **Wireless** configuration.

NOTE: You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

MPOA (Static IP Address)

This configuration is valid in case of a subscription with a static IP with NAT (please check the Manual in order to check different configuration). Make sure that the parameters are, in case of **RFC1483**, the ones in the picture, if not specifically shown by the ISP.



▾ WAN Port (WAN > Wireless)

Connection

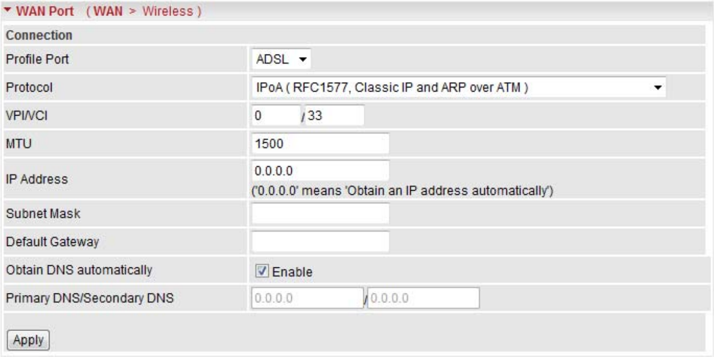
Profile Port	ADSL
Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)
VPI/VCI	0 / 33
Encap. Method	LLC Routed
MTU	1500
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Subnet Mask	
Default Gateway	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Insert then the public static IP address given by the ISP and choose **Protocol=MPOA (1483...)** and **Encapsulation Method=LLC Routed** (if not specifically shown by the ISP).

Make sure that the parameters are, the ones in the picture, if not specifically shown by the ISP.
Click **Apply** in order to start **Wireless** configuration.

IPOA (Classical IP over ATM)

This configuration is valid in case of a subscription with a static IP with NAT (please check the Manual in order to check different configuration). Make sure that the parameters are, in case of **RFC1577**, the ones in the picture, if not specifically shown by the ISP.



▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL ▾
Protocol	IPoA (RFC1577, Classic IP and ARP over ATM) ▾
VPI/VCI	0 / 33
MTU	1500
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Subnet Mask	
Default Gateway	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

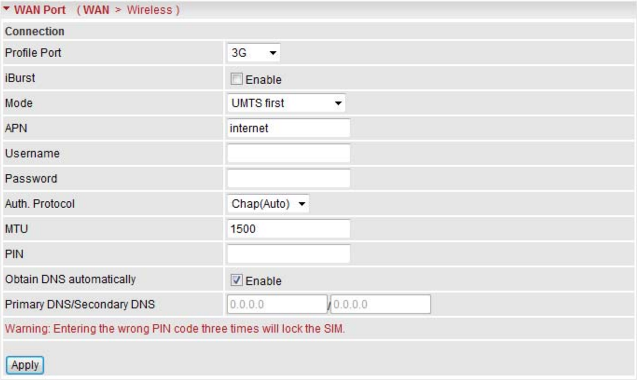
Insert then the public static IP address given by the ISP and choose **Protocol=IPOA (RFC1577…).** Make sure that the parameters are, the ones in the picture, if not specifically shown by the ISP.
Click on **Apply** in order to start **Wireless** configuration.

Pure Bridge

This configuration is valid in case of You would like to use WebShare 3G 244WN as an Ethernet modem (PPPoE stack on PC is necessary in order to establish a connection).

6.2 Single WAN 3G Configuration

1. Select **3G** from Connect Mode drop-down menu and click **Continue**.



▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	3G ▾
iBurst	□ Enable
Mode	UMTS first ▾
APN	internet
Username	
Password	
Auth. Protocol	Chap(Auto) ▾
MTU	1500
PIN	
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Warning: Entering the wrong PIN code three times will lock the SIM.

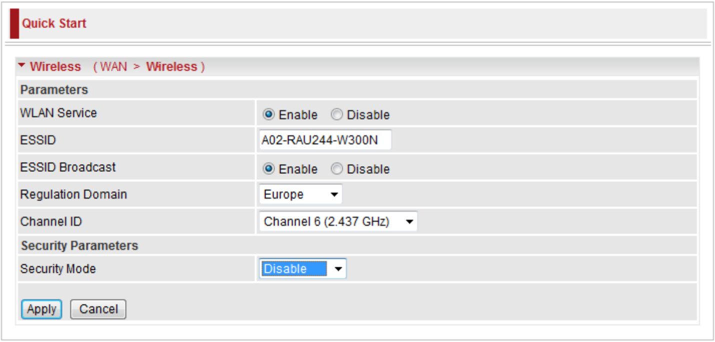
2. Select the connection method using **Mode** combo-box.
3. Insert then the **APN** provided by ISP and the **PIN code** if the SIM is secured.
4. Click on **Apply** in order to start **Wireless** configuration.

NOTE:

You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

6.3 Wireless Configuration

In this section, is possible to set all wireless connection parameters (transmission mode, channel ID, security, etc).



Quick Start

▾ Wireless (WAN > Wireless)

Parameters	
WLAN Service	● Enable ○ Disable
ESSID	A02-RAU244-W300N
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	Europe
Channel ID	Channel 6 (2.437 GHz)
Security Parameters	
Security Mode	Disable

Wireless

Field	Description
WLAN Service	Default setting is set to **Enable**. If you want to use wireless, 802.11n, 802.11g and 802.11b device in your network, you can select **Enable**.
ESSID	The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.
ESSID Broadcast	It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be

	discovered and recognized. Default setting is **Enable**.
Channel ID	Select the ID channel that you would like to use.

Security Parameters

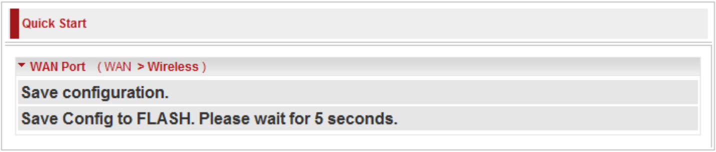
Field	Description
Security Mode	You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

Press **Apply** to continue.

NOTE: A default security profile is configured on the WebShare 3G 244WN using the WPA-PSK encryption.

6.4 Save Settings

Now, the WebShare 3G 244WN is saving configuration on the Flash memory.



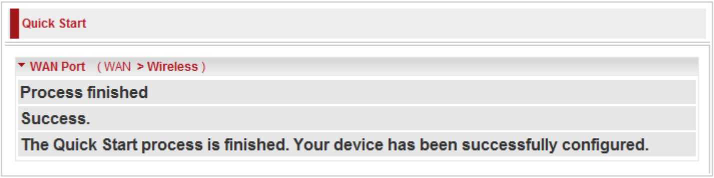
Quick Start

WAN Port (WAN > Wireless)

Save configuration.

Save Config to FLASH. Please wait for 5 seconds.

If connection is successful the following image will be shown.



Quick Start

WAN Port (WAN > Wireless)

Process finished

Success.

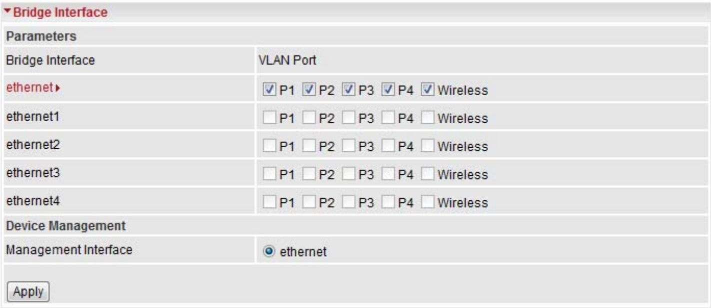
The Quick Start process is finished. Your device has been successfully configured.

7. Configuration

When you click this item, you get following sub-items to configure the ADSL router.

7.1 LAN – Local Area Network

7.1.1 Bridge Interface



▾ Bridge Interface

Parameters

Bridge Interface	VLAN Port
ethernet ▸	☑ P1 ☑ P2 ☑ P3 ☑ P4 ☑ Wireless
ethernet1	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet2	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet3	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet4	□ P1 □ P2 □ P3 □ P4 □ Wireless

Device Management

Management Interface	● ethernet

You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.

Ethernet: P1 and P2 (Port 1, 2).
Ethernet1: P3, P4 and Wireless (Port 3, 4, Wireless).

Uncheck P3, P4 and Wireless from Ethernet VLAN port first.

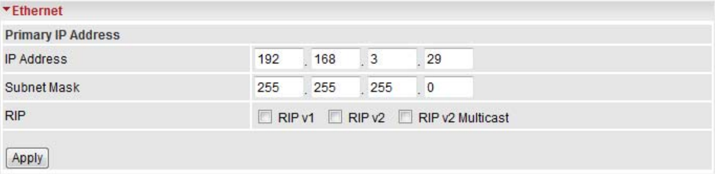
NOTE: You should setup each VLAN group with caution.

Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port
ethernet	P1 / P2 / P3 / P4 / Wireless

ethernet1	P2 / P3 / P4 / Wireless
ethernet2	P3 / P4 / Wireless
ethernet3	P4 / Wireless
ethernet4	Wireless

7.1.2 Ethernet



Ethernet

Primary IP Address

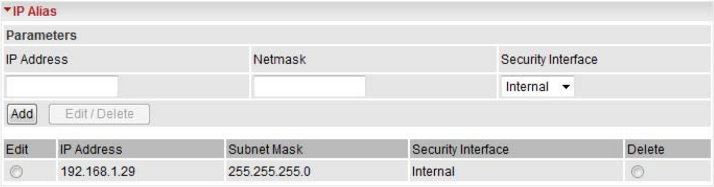
IP Address	192 . 168 . 3 . 29
Subnet Mask	255 . 255 . 255 . 0
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast

Apply

Field	Description
IP Address	The default IP on this router.
Subnet Mask	The default subnet mask on this router.
RIP	RIP v1, RIP v2, and RIP v2 Multicast. Check to **Enable** RIP function.

7.1.3 IP Alias

This function creates multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



IP Alias

Parameters

IP Address	Netmask	Security Interface
		Internal

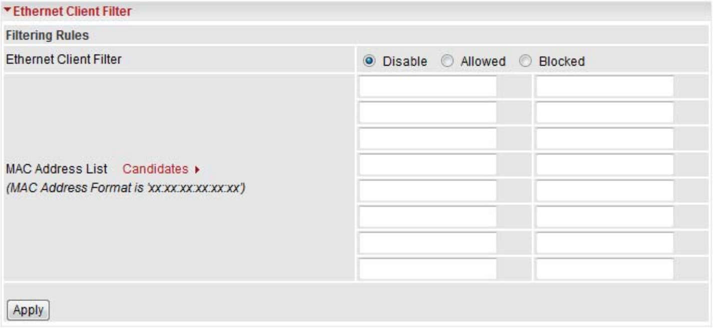
Add Edit / Delete

Edit	IP Address	Subnet Mask	Security Interface	Delete
○	192.168.1.29	255.255.255.0	Internal	○

Field	Description
IP Address	Specify an IP address on this virtual interface
Subnet Mask	Specify a subnet mask on this virtual interface
Security Interface	Choose the interface type between: • **Internal:** The network is behind NAT. All traffic will do network address translation when sending out to Internet if NAT is enabled. • **External:** There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface. • **DMZ:** Specify this network to DMZ area. There is no NAT on this interface.

7.1.4 Ethernet Client Filter

The Ethernet Client Filter supports up to 16 Ethernet network machines that helps you to manage your network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access your LAN.
There are no pre-define Ethernet MAC address filter rules; you can add the filter rules to meet your requirements.



Ethernet Client Filter

Filtering Rules

Ethernet Client Filter ● Disable ○ Allowed ○ Blocked

MAC Address List Candidates ▸
(MAC Address Format is 'xx:xx:xx:xx:xx:xx')

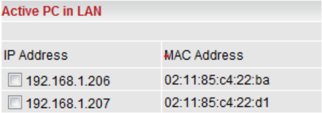
Field	Description
Ethernet Client Filter	Default setting is set **Disable**. • **Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is listed. • **Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is not listed. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number 0 - 9 and letters a - f are

	acceptable.
Mac Address List	Insert MAC Address to filter. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number 0 - 9 and letters a - f are acceptable.

NOTE: Follow the MAC Address Format xx:xx:xx:xx:xx:xx; Semicolon (:) must be included.

Press Candidates ▸ button to show a list of active PC connected to the Router.

Active PC in LAN displays a list of individual Ethernet device's IP Address and MAC Address which connecting to the router.



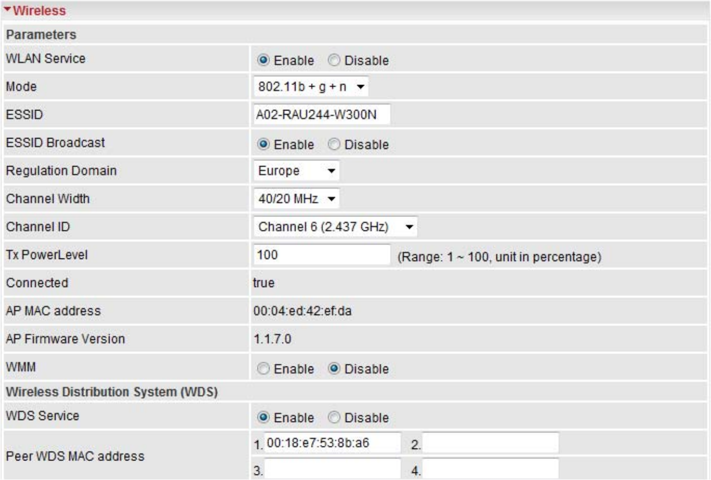
Active PC in LAN

IP Address	MAC Address
□ 192.168.1.206	02:11:85:c4:22:ba
□ 192.168.1.207	02:11:85:c4:22:d1

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table.

NOTE: The maximum Ethernet client is 16.

7.1.5 Wireless



▾Wireless

Parameters	
WLAN Service	● Enable ○ Disable
Mode	802.11b + g + n ▾
ESSID	A02-RAU244-W300N
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	Europe ▾
Channel Width	40/20 MHz ▾
Channel ID	Channel 6 (2.437 GHz) ▾
Tx PowerLevel	100 (Range: 1 ~ 100, unit in percentage)
Connected	true
AP MAC address	00:04:ed:42:ef:da
AP Firmware Version	1.1.7.0
WMM	○ Enable ● Disable
Wireless Distribution System (WDS)	
WDS Service	● Enable ○ Disable
Peer WDS MAC address	1. 00:18:e7:53:8b:a6 2. 3. 4.

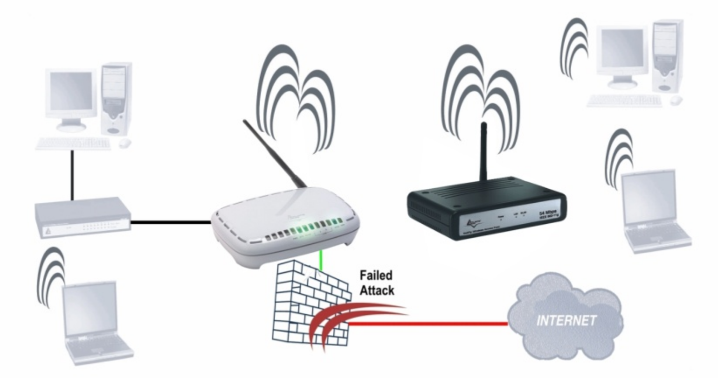
Parameters

Field	Description
WLAN Service	Default setting is set to **Enable**. If you do not have any wireless, 802.11n, 802.11g and 802.11b, device in your network, select **Disable**.
Mode	The default setting is 802.11b+g+n (Mixed mode). If you do not know or have both 11g and 11n devices in your network, then keep the default in mixed mode. From the drop-down manual, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b. If you have only 11n card, then select 802.11n

ESSID	The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default **WebShare244WN** to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.
ESSID Broadcast	It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enabled**. • **Disable:** If you do not want broadcast your ESSID. Any client uses "any" wireless setting cannot discover the Access Point (AP) of your router. • **Enable:** Any client that using the "any" setting can discover the Access Point (AP) in the wireless network.
Regulation Domain	There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting
Channel Widht	Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The higher the bandwidth the better the performance will be.
Channel ID	Select the wireless connection ID channel that you would like to use.
TX Power Level	It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 1 up to maximum 100
Connected	Representing in **true** or **false**. That it is the connection status between the system and the build-in wireless card.
AP Mac Address	It is a unique hardware address of the Access Point
AP Firmware Version	The Access Point firmware version.
WMM	Enable or disable the WMM support.

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply to define peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.



WDS – Wireless Distribution System

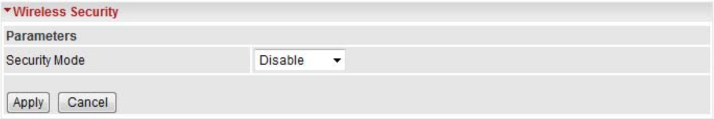
Field	Description
WDS Service	The default setting is **Disabled**. Check **Enable** radio button to activate this function.
Peer WDS MAC Address (1-4)	It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

NOTE:

- ESSID field is case sensitive and it cannot excess 32 characters.
- Wireless performance may degrade if select ID channel is already being occupied by other AP(s).
- The Power Level maybe different in each access network user premises environment and choose the most suitable level for your network
- For MAC Address, Semicolon (:) must be included.

7.1.6 Wireless Security

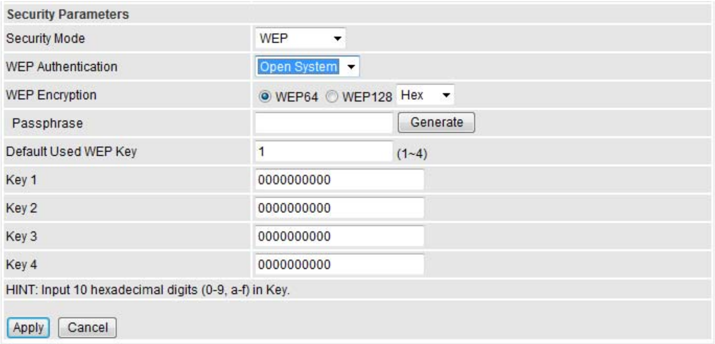
You can disable or enable with WPA or WEP for protecting wireless network.



Wireless Security

Parameters	
Security Mode	Disable ▾

WEP (Wired Equivalent Privacy)



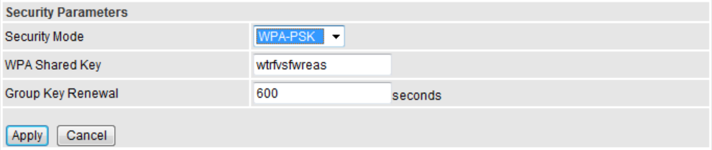
Security Parameters	
Security Mode	WEP ▾
WEP Authentication	Open System ▾
WEP Encryption	● WEP64 ○ WEP128 Hex ▾
Passphrase	Generate
Default Used WEP Key	1 (1~4)
Key 1	0000000000
Key 2	0000000000
Key 3	0000000000
Key 4	0000000000

HINT: Input 10 hexadecimal digits (0-9, a-f) in Key.

Security Parameters

Field	Description
Security Mode	Select **WEP** encryption.
WEP Authentication	To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System** or Shared **key**.
WEP Encryption	To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64. The encryption can either be HEX or ASCII.
Passphrase (attivo solo in caso di selezione della modalità HEX)	This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the Passphrase is enabled. Passphrase will convert an inputted string into the HEX format which will automatically fill the input space for Key 1 to Key 4.
Default Used WEP Key	Select the encryption key ID. There are 4 keys to choose from so that you will not have to re-create a key every time you decide to have it as something different. You can just have 4 sets of keys to rotate instead of jus having 1 key. Please refer to **Key (1~4)** below.
Key 1 – 4	Enter the key to encrypt wireless data this can be in ASCII or HEX depending on the WEP Encryption that you have selected above. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX (10 and 26 HEX codes) or ASCII style (5 and 13 ASCII codes) are required for WEP64 and WEP128 respectively no any separator is included.

WPA-PSK or WPA2-PSK (Wi-Fi Protected Access)



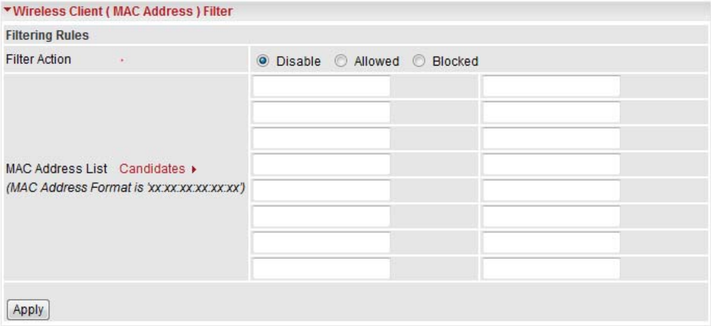
Security Parameters	
Security Mode	WPA-PSK
WPA Shared Key	wtrfvsfwreas
Group Key Renewal	600 seconds

Security Parameters

Field	Description
Security Mode	Select **WPA-PSK** or **WPA2-PSK** security mode.
WPA Shared Key	The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.
Group Key Renewal	The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 600 seconds.

7.1.7 Wireless Client / MAC Address Filter

The MAC Address supports up to 16 wireless network machines and helps you manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) to access your LAN.
There are no pre-define MAC Address filter rules; you can add the filter rules to meet your requirements.



▾Wireless Client (MAC Address) Filter

Filtering Rules

Filter Action	● Disable ○ Allowed ○ Blocked
MAC Address List Candidates ▸ *(MAC Address Format is 'xx:xx:xx:xx:xx:xx')*	16 empty fields

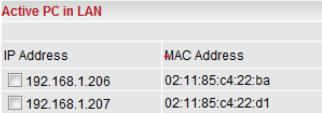
Field	Description
Wireless Client Filter	Default setting is set **Disable**. • **Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is listed. • **Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is not listed. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number 0 - 9 and letters a - f are

	acceptable.
Mac Address List	Insert MAC Address to filter. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number 0 - 9 and letters a - f are acceptable.

NOTE: Follow the MAC Address Format xx:xx:xx:xx:xx:xx; Semicolon (:) must be included.

Press Candidates ▸ button to show a list of active PC connected to the Router.

Associated Wireless Client displays a list of individual Wireless device's IP Address and MAC Address which connecting to the router.



Active PC in LAN

IP Address	MAC Address
□ 192.168.1.206	02:11:85:c4:22:ba
□ 192.168.1.207	02:11:85:c4:22:d1

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table.

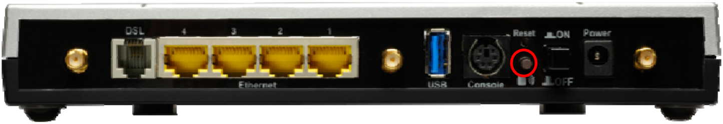
NOTE: The maximum Wireless client is 16.

7.1.8 WPS

WPS feature is follow Wi-Fi Alliance WPS standard and it easily set up security-enabled Wi-Fi networks in the home and small office environment. It reduces half the user steps to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.

WPS Button Setup

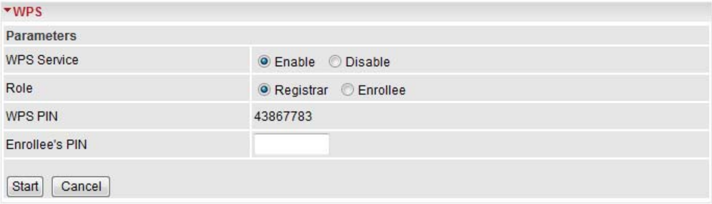
1. Press the WPS button on the rear panel of the WebShare 3G 244WN.



1. Press the WPS button on the wireless clients that would like to associates to the WebShare 3G 244WN within 120 seconds.

WPS PIN Setup

1. Identify WPS PIN on wireless clients to associate to the WebShare 3G 244WN.
2. Click on **Configuration – LAN – WPS** and set Role field as **Registar**.



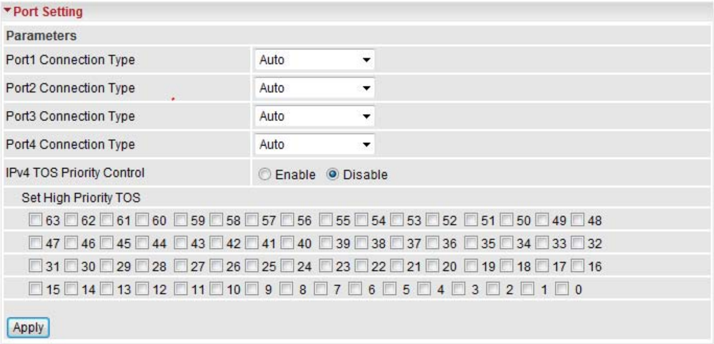
▾WPS

Parameters	
WPS Service	● Enable ○ Disable
Role	● Registrar ○ Enrollee
WPS PIN	43867783
Enrollee's PIN	

3. Now insert the client WPS PIN (one for times) and click Start to synchronize it with the Router.

7.1.9 Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



▾Port Setting

Parameters

Port1 Connection Type	Auto
Port2 Connection Type	Auto
Port3 Connection Type	Auto
Port4 Connection Type	Auto
IPv4 TOS Priority Control	○ Enable ● Disable

Set High Priority TOS

□ 63 □ 62 □ 61 □ 60 □ 59 □ 58 □ 57 □ 56 □ 55 □ 54 □ 53 □ 52 □ 51 □ 50 □ 49 □ 48
□ 47 □ 46 □ 45 □ 44 □ 43 □ 42 □ 41 □ 40 □ 39 □ 38 □ 37 □ 36 □ 35 □ 34 □ 33 □ 32
□ 31 □ 30 □ 29 □ 28 □ 27 □ 26 □ 25 □ 24 □ 23 □ 22 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 □ 14 □ 13 □ 12 □ 11 □ 10 □ 9 □ 8 □ 7 □ 6 □ 5 □ 4 □ 3 □ 2 □ 1 □ 0

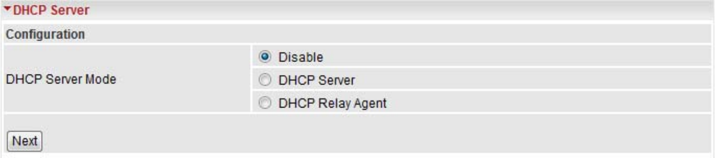
Field	Description
Port # Connection Type	There are Six options to choose from: Auto, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex, 1000M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is Auto, which users should keep unless there are specific problems with PCs not being able to access your LAN.
IPv4 TOS Priority Control	TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority.

If the packet is high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the TOS field matches the checked values in the table (0 to 63), this packet will be treated as high priority.

7.1.10 DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.



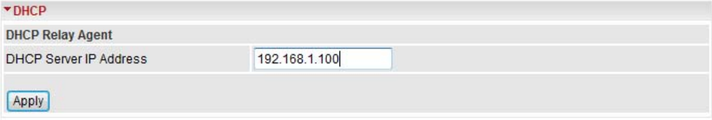
▾DHCP Server

Configuration	
DHCP Server Mode	● Disable ○ DHCP Server ○ DHCP Relay Agent

To disable the router's DHCP Server, check **Disabled** and click **Next**, then click **Apply**. When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PCs on your network, and set the default gateway for each PCs to the IP address of the router (by default this is 192.168.1.254).

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click Apply to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.



DHCP Server IP Address: 192.168.1.100

Click **Apply** to enable this function.

7.2 WAN – Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router’s connection to your ISP and the Internet.

7.2.1 WAN Interface

The factory default settings are configured as following:

WAN Profile	
Encapsultation	PPPoA
Multiplexing	VC-Mux
Mode	Routing
VPI/VCI	8/35

Thorugh this section , is possible to set which interface (ADSL or 3G) use for Internet connection. It is also possible to active some advanced backup features in order to maintain an always-on connection in case of failover of the DSL line.

NOTE: The configuration of 3G interface will be able also without any modem connected to the WebShare 3G 244WN.

NOTE: All backup functionalities are able only if ADSL is set as Main Connection.

NOTE: If the function Failover/Failback is Enable, is necessary to set both interfaces using Wan Profile menu.

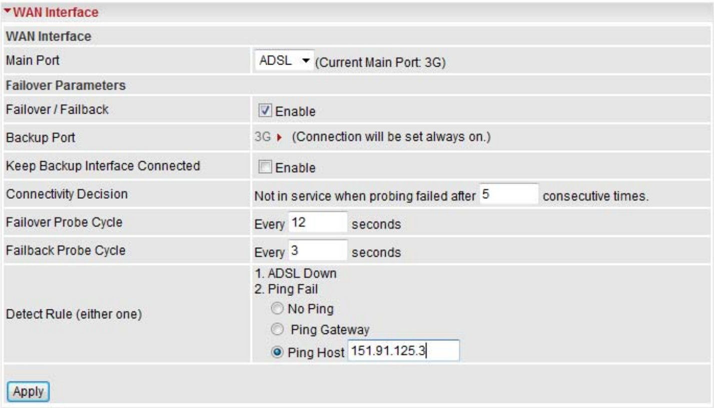
⚠ You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.

Atlantis Land will not be considered responsible in case of wrong or bad configuration.

3G USB Modem is not included with WebShare 244WN.

⚠ WebShare 3G 244WN can works only with a compatible device.
Please check the modem compatibility on the website www.atlantis-land.com or with the compatibility list provided with the WebShare 244WN.

WAN CONNECTION – ADSL MODE



▾WAN Interface

WAN Interface	
Main Port	ADSL ▾ (Current Main Port: 3G)
Failover Parameters	
Failover / Failback	☑ Enable
Backup Port	3G ▸ (Connection will be set always on.)
Keep Backup Interface Connected	□ Enable
Connectivity Decision	Not in service when probing failed after 5 consecutive times.
Failover Probe Cycle	Every 12 seconds
Failback Probe Cycle	Every 3 seconds
Detect Rule (either one)	1. ADSL Down 2. Ping Fail ○ No Ping ○ Ping Gateway ● Ping Host 151.91.125.3

WAN Interface

Field	Description
Main Port	User can select either **ADSL** or **3G** mode.

Failover Parameters

Field	Description
Failover/Failback	Set **Enable** to trigger ADSL / 3G failover / failback function ready.
Backup Port	It links to backup port configuration page. It is necessary to configure it when Failover/Failback be set.
Keep Backup Interface Connected	Select this option to maintain connected the 3G interface also when main connection will be available.
Connectivity Decision	Set how many times of probing failed to switch backup port.

Failover Probe Cycle	Set the time duration for the **Failover Probe Cycle** to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.
Failback Probe Cycle	Set the time duration for the **Failback Probe Cycle** to determine when the router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection is communicating again.
Detect Rule	Select the detection rules for the failover of the main interface. • **Rule 1. ADSL Down** • **Rule 2. Ping Fail** ➢ **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection. ➢ **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every "**Probe Cycle**". ➢ **Ping Host:** It will send ping packet to specific host and wait response in every "**Probe Cycle**". The host must be an IP address.

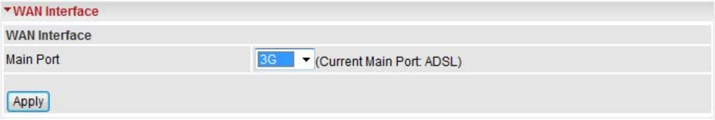
NOTE: If 3G is set for main port, then there can be no option for failover/failback.

NOTE: The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **Connection Decision** amount (e.g. From the image above it will be 12 seconds multiplied by 5 consecutive fails).

NOTE: The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **Connection Decision** amount (e.g. From the image above it will be 3 seconds multiplied by 5 consecutive fails).

WAN CONNECTION – 3G MODE

In the ADSL mode, as the ADSL is not available(failover/failback), it will turn to 3G mode for supporting WAN Connection. However, in the 3G Mode, the ADSL can not support WAN Connection when 3G Mode is unavailable.



▾WAN Interface

WAN Interface	
Main Port	3G ▾ (Current Main Port: ADSL)

You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

3G USB Modem is not included with WebShare 244WN.

WebShare 3G 244WN can works only with a compatible device.
Please check the modem compatibility on the website www.atlantis-land.com or with the compatibility list provided with the WebShare 244WN.

7.2.2 WAN Profile

NOTE: If the function Failover/Failback is Enable, is necessary to set both interfaces using Wan Profile menu.

You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

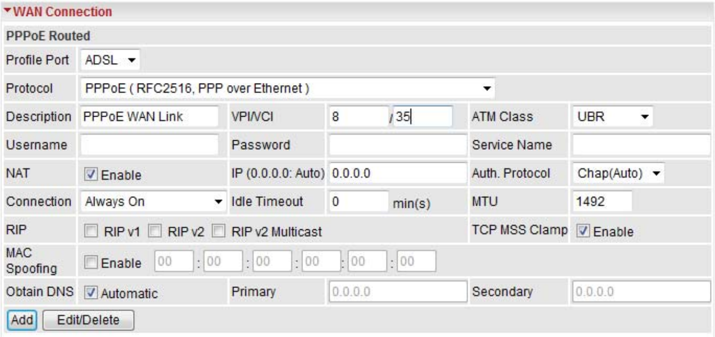
3G USB Modem is not included with WebShare 244WN.

WebShare 3G 244WN can works only with a compatible device.

Please check the modem compatibility on the website www.atlantis-land.com or with the compatibility list provided with the WebShare 244WN.

ADSL - PPPoE Connection

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



WAN Connection

PPPoE Routed

Profile Port	ADSL				
Protocol	PPPoE (RFC2516, PPP over Ethernet)				
Description	PPPoE WAN Link	VPI/VCI	8 / 35	ATM Class	UBR
Username		Password		Service Name	
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Chap(Auto)
Connection	Always On	Idle Timeout	0 min(s)	MTU	1492
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00				
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

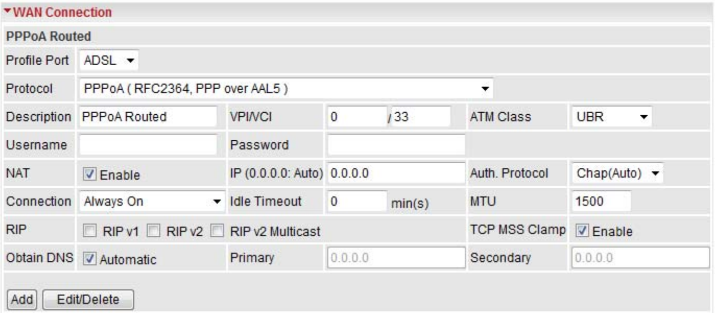
Field	Description
Profile Port	Select the profile port either ADSL or 3G
Protocol	The ATM protocol will be used in the device
Description	A given name for the connection
VPI / VCI	Enter the information provided by your ISP
ATM Class	The Quality of Service for ATM layer
Username	Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
Password	Enter the password provided by your ISP. You can input up to

	128 alphanumeric characters (case sensitive).
Service Name	This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 15 alphanumeric characters.
NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
IP	Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.
Auth. Protocol	Default is Auto. Your ISP should advises you on whether to use Chap or Pap.
Connection	• **Always on:** If you want the router to establish a PPP session when starting up and to automatically re-establish the PPP session when disconnected by the ISP. • **Connect on Demand:** If you want to establish a PPP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).
Idle Timeout	Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. • **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.
MTU	Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.
RIP	RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default is **enabled**.
MAC Spoofing	This option is required by some service providers. You must fill

	in the MAC address that specify by service provider when it is required. Default is disabled.
Obtain DNS	A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

NOTE: You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

ADSL - PPPoA Connection



▾ WAN Connection

PPPoA Routed

Profile Port	ADSL ▾				
Protocol	PPPoA (RFC2364, PPP over AAL5) ▾				
Description	PPPoA Routed	VPI/VCI	0 / 33	ATM Class	UBR ▾
Username		Password			
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Chap(Auto) ▾
Connection	Always On ▾	Idle Timeout	0 min(s)	MTU	1500
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

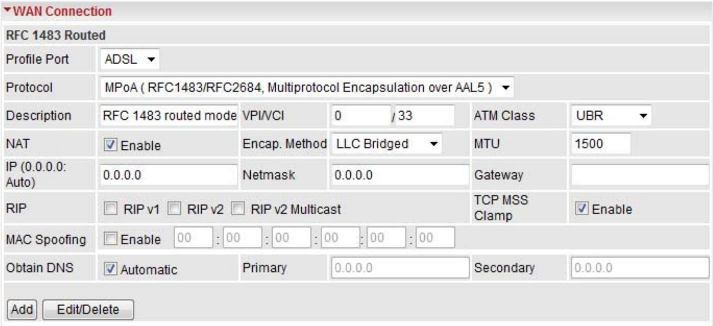
Field	Description
Profile Port	Select the profile port either ADSL or 3G
Protocol	The ATM protocol will be used in the device
Description	A given name for the connection
VPI / VCI	Enter the information provided by your ISP
ATM Class	The Quality of Service for ATM layer
Username	Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
Password	Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).
NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
IP	Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth. Protocol	Default is Auto. Your ISP should advises you on whether to use Chap or Pap.
Connection	• **Always on:** If you want the router to establish a PPP session when starting up and to automatically re-establish the PPP session when disconnected by the ISP. • **Connect on Demand:** If you want to establish a PPP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).
Idle Timeout	Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. • **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.
MTU	Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.
RIP	RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default is **enabled**.
MAC Spoofing	This option is required by some service providers. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.
Obtain DNS	A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

NOTE:

You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance. **Atlantis Land will not be considered responsible in case of wrong or bad configuration.**

ADSL - MPoA Connection (RFC 1483)



▾WAN Connection

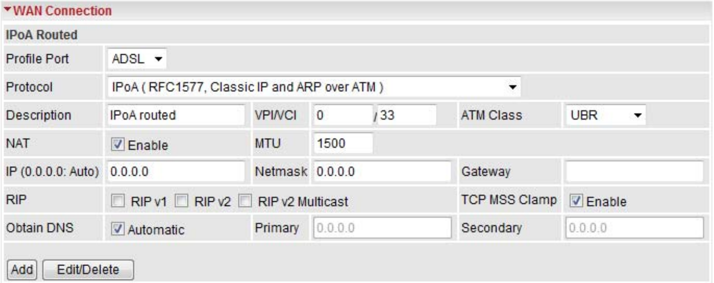
RFC 1483 Routed

Profile Port	ADSL ▾				
Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5) ▾				
Description	RFC 1483 routed mode	VPI/VCI	0 / 33	ATM Class	UBR ▾
NAT	☑ Enable	Encap. Method	LLC Bridged ▾	MTU	1500
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	0.0.0.0	Gateway	
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00				
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Field	Description
Profile Port	Select the profile port either ADSL or 3G
Protocol	The ATM protocol will be used in the device
Description	A given name for the connection
VPI / VCI	Enter the information provided by your ISP
ATM Class	The Quality of Service for ATM layer
NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
Encap. Method	Choose whether you want the packets in WAN interface as bridged packet or routed packet.
MTU	Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.
IP	Your WAN IP address. Leave this at 0.0.0.0 to obtain

	automatically an IP address from your ISP.
Netmask	The default is 0.0.0.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).
Gateway	Enter the IP address of the default gateway (if given).
RIP	RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default is **enabled**.
MAC Spoofing	This option is required by some service providers. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.
Obtain DNS	A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.
Primary/Secondary DNS	Enter DNS server addresses.

ADSL - IPoA Routed Connection (RFC 1577 Routed)



WAN Connection

IPoA Routed

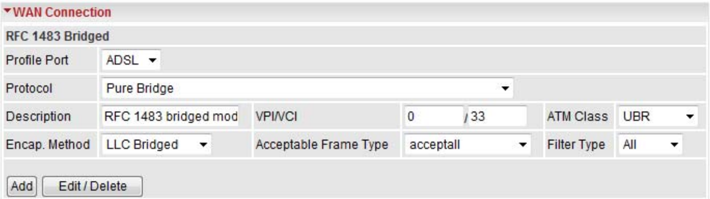
Profile Port	ADSL ▾				
Protocol	IPoA (RFC1577, Classic IP and ARP over ATM) ▾				
Description	IPoA routed	VPI/VCI	0 / 33	ATM Class	UBR ▾
NAT	☑ Enable	MTU	1500		
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	0.0.0.0	Gateway	
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Add Edit/Delete

Field	Description
Profile Port	Select the profile port either ADSL or 3G
Protocol	The ATM protocol will be used in the device
Description	A given name for the connection
VPI / VCI	Enter the information provided by your ISP
ATM Class	The Quality of Service for ATM layer
NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
MTU	Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.
IP	Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.
Netmask	The default is 0.0.0.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway	Enter the IP address of the default gateway (if given).
RIP	RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default is **enabled**.
MAC Spoofing	This option is required by some service providers. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.
Obtain DNS	A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.
Primary/Secondary DNS	Enter DNS server addresses.

ADSL - Pure Bridge



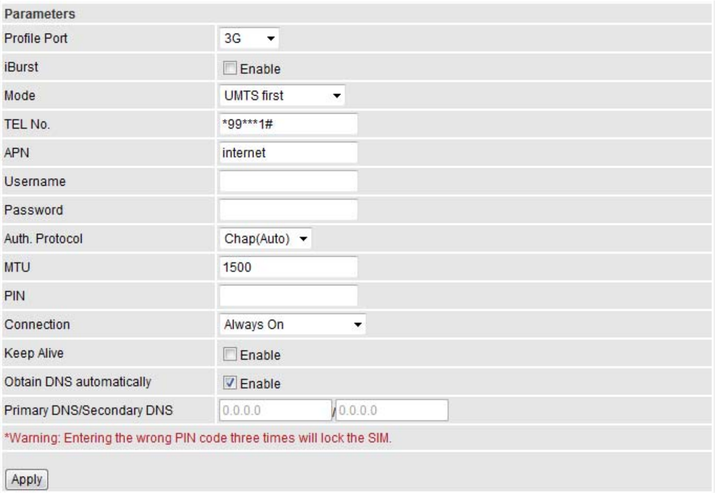
WAN Connection

RFC 1483 Bridged

Profile Port	ADSL				
Protocol	Pure Bridge				
Description	RFC 1483 bridged mod	VPI/VCI	0 / 33	ATM Class	UBR
Encap. Method	LLC Bridged	Acceptable Frame Type	acceptall	Filter Type	All

Field	Description
Profile Port	Select the profile port either ADSL or 3G
Protocol	The ATM protocol will be used in the device
Description	A given name for the connection
VPI / VCI	Enter the information provided by your ISP
ATM Class	The Quality of Service for ATM layer
Encap Method	Choose whether you want the packets in WAN interface as bridged packet or routed packet.
Acceptable Frame Type	Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.
Filter Type	Specify the type of ethernet filtering performed by the named bridge interface: • **All:** Allows all types of ethernet packets through the port. • **IP:** Allows only IP/ARP types of ethernet packets through the port. • **PPPoE:** Allows only PPPoE types of ethernet packets through the port.

3G CONNECTION



Parameters

Profile Port	3G ▾
iBurst	□ Enable
Mode	UMTS first ▾
TEL No.	*99***1#
APN	internet
Username	
Password	
Auth. Protocol	Chap(Auto) ▾
MTU	1500
PIN	
Connection	Always On ▾
Keep Alive	□ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

*Warning: Entering the wrong PIN code three times will lock the SIM.

Connection

Field	Description
Profile Port	Select the profile port either ADSL or 3G
iBurst	Enable a specific parameters set for iBurst client.
Mode	Permit to choose which connection method use as preferred.
Tel No.	Insert telephone number required for a 3G connection.
APN	Specify the APN for 3G connections.
Username	Insert username for authentication (only if required).
Password	Insert password for authentication (only if required).

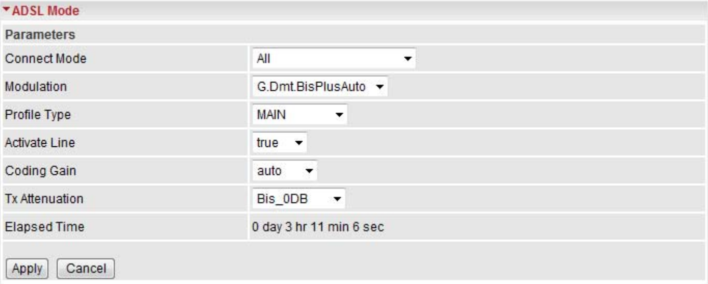
Authentication Protocol	Select authentication protocol for 3G connection.
MTU	Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.
PIN	Insert the PIN code for the SIM (if required).
Connection	Select the connection mode.
Keep Alive	If enable, permit to maintain active 3G connection also if the main connection is active after failback.
Obtain DNS automatically	A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.
Primary DNS / Secondary DNS	Enter DNS server addresses.

⚠ You have to pay particular attention to the WAN-ADSL connection. If you have any doubt turn to qualified personnel or contact Atlantis-Land technical assistance.
Atlantis Land will not be considered responsible in case of wrong or bad configuration.

3G USB Modem is not included with WebShare 244WN.

⚠ WebShare 3G 244WN can works only with a compatible device.
Please check the modem compatibility on the website www.atlantis-land.com or with the compatibility list provided with the WebShare 244WN.

7.2.3 ADSL Mode



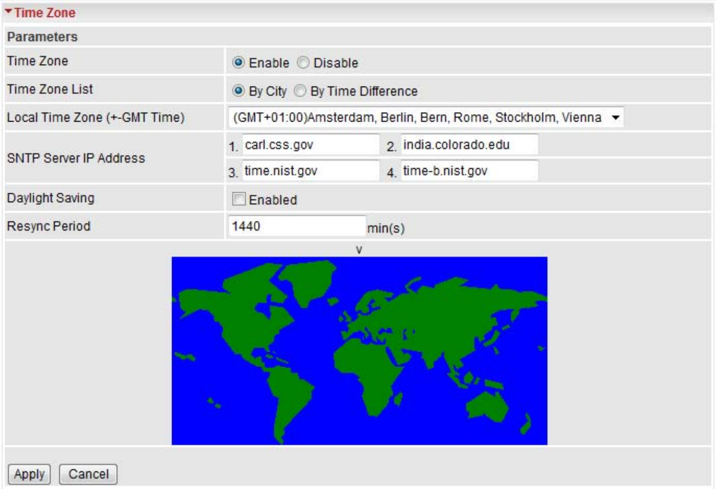
Connect Mode	All
Modulation	G.Dmt.BisPlusAuto
Profile Type	MAIN
Activate Line	true
Coding Gain	auto
Tx Attenuation	Bis_0DB
Elapsed Time	0 day 3 hr 11 min 6 sec

Field	Description
Connect Mode	This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL, All. Please keep the factory setting unless ADSL is detected as the symptom of synchronization problem
Modulation	It will automatically detect capability of your ADSL line mode. Please keep the factory setting unless A: This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL, All. Please keep the factory setting unless ADSL is detected as the symptom of synchronization problem DSL is detected as the symptom of synchronization problem.
Profile Type	Please keep the factory settings unless ADSL is detected as the symptom of low link rate or unstable problems. You may need to change the profile setting to reach the best ADSL line rate, it depends on the different DSLAM and location.
Active Line	Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of Connect Mode.
Coding Gain	It reduces router's transmit power which will effect to router's

	downstream performance. Higher the gain will increase the downstream rate but it sometimes causes unstable ADSL line. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic

7.3 System

7.3.1 Time Zone



▾Time Zone

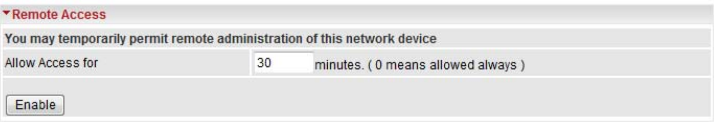
Parameters	
Time Zone	● Enable ○ Disable
Time Zone List	● By City ○ By Time Difference
Local Time Zone (+-GMT Time)	(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▾
SNTP Server IP Address	1. carl.css.gov 2. india.colorado.edu 3. time.nist.gov 4. time-b.nist.gov
Daylight Saving	□ Enabled
Resync Period	1440 min(s)

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Daylight Saving is also known as Summer Time Period. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check Automatic box to auto set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

7.3.2 Remote Access



Remote Access

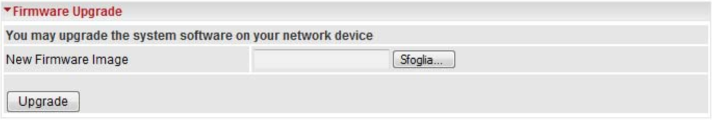
You may temporarily permit remote administration of this network device

Allow Access for: 30 minutes. (0 means allowed always)

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable**. You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of **0** minute.

7.3.3 Firmware Upgrade



Firmware Upgrade

You may upgrade the system software on your network device

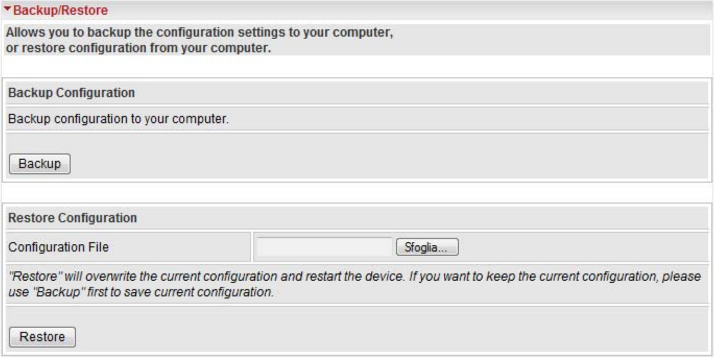
New Firmware Image:

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes. Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.

- Do NOT upgrade firmware on any Atlantis Land product over a wireless connection.
- Failure of the device may result. Use only hard-wired network connections.
- Restore a saved configuration file generated with another firmware version may render your Router unstable and prevent some functions from working properly. After upgrading you must reset the router to factory default settings, then manually re-enter your settings.
- Detach ADSL Line and connect to the Router using only 1 Ethernet port.
- Please pay attention. In case electrical shutdown, during this procedure, this product could be not usable.
- When uploading software to the Router, it is important not to interrupt the Web browser by closing the window or loading a new page. If the browser is interrupted, it may corrupt the software

7.3.4 Backup / Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.



Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Restore Configuration

Configuration File

"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

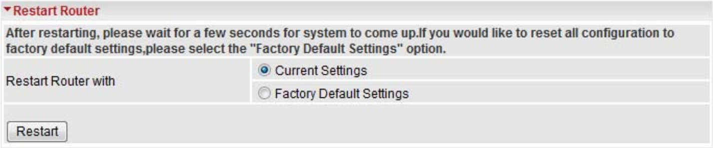
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the current version of the router's firmware. Settings files saved to your PC should not be manually edited in any way.

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

7.3.5 Restart Router

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



▾Restart Router

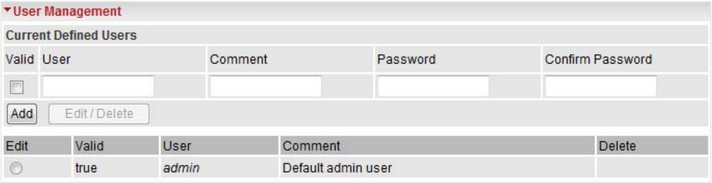
After restarting, please wait for a few seconds for system to come up.If you would like to reset all configuration to factory default settings,please select the "Factory Default Settings" option.

Restart Router with	● Current Settings ○ Factory Default Settings

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

You may also reset your router to factory settings by holding the small Reset pinhole button more than 6 seconds on the back of your router.

7.3.6 User Management



▾User Management

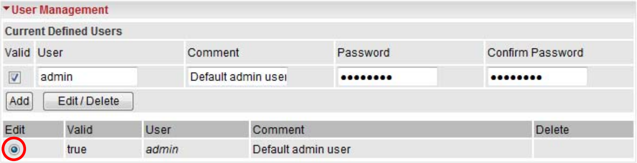
Current Defined Users

Valid	User	Comment	Password	Confirm Password
□				

Edit	Valid	User	Comment	Delete
○	true	*admin*	Default admin user	

In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked on **Edit**, you are shown the following options:



User Management

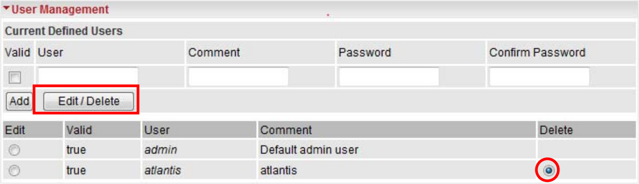
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☑	admin	Default admin usei	•••••••••	•••••••••

Add Edit / Delete

Edit	Valid	User	Comment	Delete
●	true	*admin*	Default admin user	

You can change the user's **password**, whether their account is active and **valid**, as well as add a comment to each user account. Click Edit/Delete button to save your revise. You cannot delete the default admin account, if you do you will be log out. However, you can delete any other created accounts by clicking **Delete** when editing the user. You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.



User Management

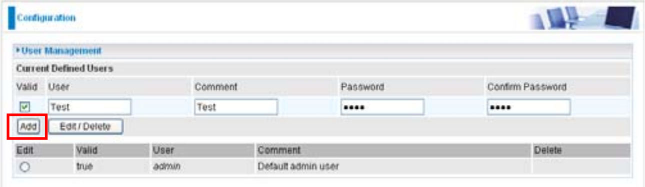
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☐				

Add Edit / Delete

Edit	Valid	User	Comment	Delete
○	true	*admin*	Default admin user	
○	true	*atlantis*	atlantis	●

When you create a user account, you check Valid to fill in the blank with User, Comment, Password and Confirm Password. Later, click **Add** button to add your new user account.



Configuration

User Management

Current Defined Users

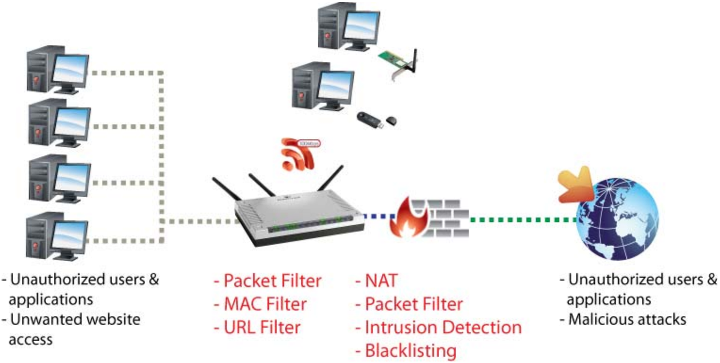
Valid	User	Comment	Password	Confirm Password
☑	Test	Test	••••	••••

Add Edit / Delete

Edit	Valid	User	Comment	Delete
○	true	*admin*	Default admin user	

7.4 Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. Besides, when using NAT, the router acts as a “natural” Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



1. **Firewall:** Prevents access from outside your network. The router provides three levels of security support:
   - **NAT natural firewall:** This masks LAN users’ IP addresses which is invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when NAT function is enabled.
   - **Firewall Security and Policy (General Settings):** Inbound direction of Packet Filter rules to prevent unauthorized

computers or applications accessing your local network from the Internet.

- **Intrusion Detection:** Enable Intrusion Detection to detect, prevent and log malicious attacks.

2. **Access Control:** Prevents access from PCs on your local network:
   - **Firewall Security and Policy (General Settings):** Outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.
   - **URL Filter:** To block PCs on your local network from unwanted websites.

7.4.1 General Settings

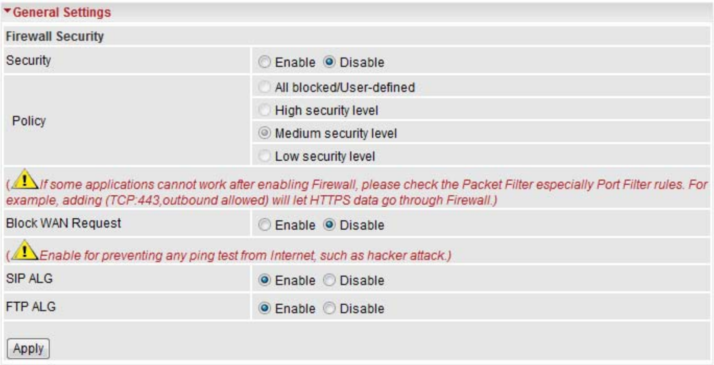
You can choose not to enable Firewall and still able to access to URL Filter and IM/P2P Blocking or enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.
There are four options when you enable the Firewall, they are:

- **All blocked/User-defined:** no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- **High/Medium/Low security level:** the predefined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either High, Medium or Low security level to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detailed on level of preset port filter information, refer to Table 1: Predefined Port Filter.

If you choose of the preset security levels and add custom filters, this level of filter rules will be saved even and do not need to re-configure the rules again if you disable or switch to other firewall level.

The **Block WAN Request** is a stand-alone function and not relate to whether security enable or disable. Mostly it is for preventing any scan tools from WAN site by hacker.



General Settings

Firewall Security

Security ○ Enable ● Disable

Policy
○ All blocked/User-defined
○ High security level
● Medium security level
○ Low security level

(⚠ *If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)*

Block WAN Request ○ Enable ● Disable

(⚠ *Enable for preventing any ping test from Internet, such as hacker attack.)*

SIP ALG ● Enable ○ Disable

FTP ALG ● Enable ○ Disable

Table 1: Predefined Port Filter

Application	Protocol	Port Number		Low Level		Medium Level		High Level	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES

DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO

SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP /SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

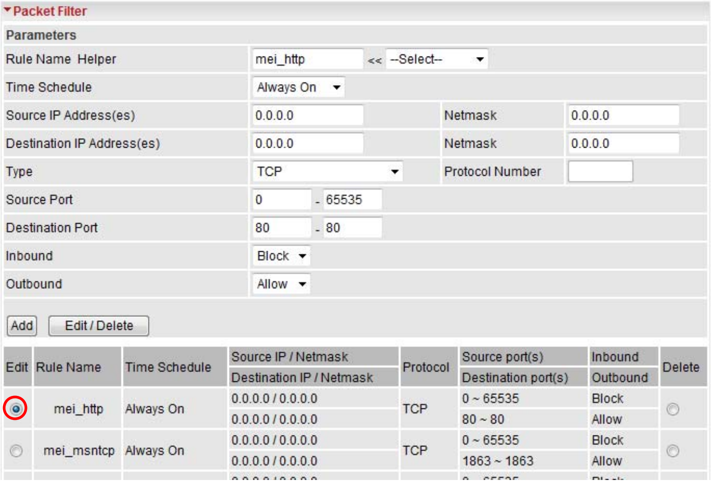
Inbound: Internet to LAN ; **Outbound:** LAN to Internet; **YES:** Allowed ; **NO:** Blocked ; **N/A:** Not Applicable

Premere **Apply** per confermare le eventuali modifiche.

7.4.2 Packet Filter

This function is only available when the Firewall is enabled and one of these four security levels is chosen (All blocked, High, Medium and Low). The preset port filter rules in the Packet Filter must modify accordingly to the level of Firewall, which is selected.

See Table1: Predefined Port Filter for more detail information.



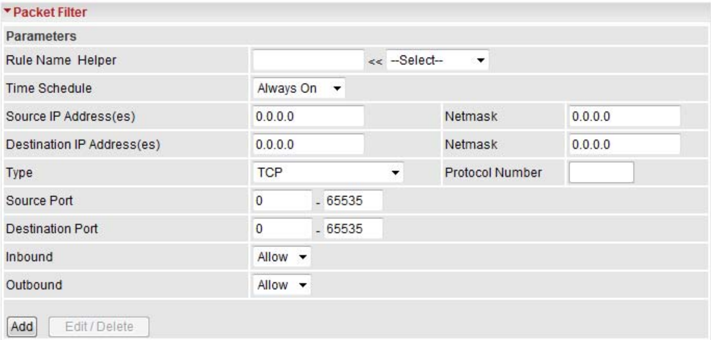
Packet Filter

Parameters

Rule Name Helper	mei_http << --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	80 - 80		
Inbound	Block		
Outbound	Allow		

Edit	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	Delete
●	mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	○
○	mei_msntcp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 1863 ~ 1863	Block Allow	○

Add TCP/UDP Filter



▾ Packet Filter

Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Field	Description
Rule name	Users-define description to identify this entry or click “Select” drop-down menu to select existing predefined rules. The maximum name length is 32 characters.
Time Schedule	It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section
Source/Destination IP Address(es)	This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Selecting the Subnet Mask of the IP address range you wish to allow/block the traffic to or form; set IP address and Subnet Mask to 0.0.0.0 to inactive the Address-Filter rule.
Type	It is the packet protocol type used by the application, select TCP, UDP or both TCP/UDP.
Protocol Number	Insert the port number
Source Port	This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set

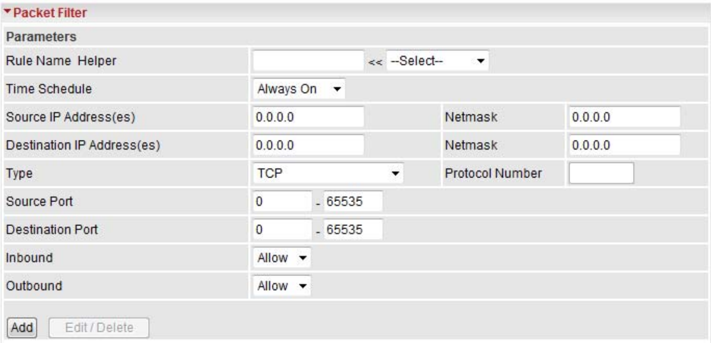
	from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.
Destination Port	This is the Port or Port Ranges that defines the application
Inbound/Outbound	Select Allow or Block the access to the Internet (“Outbound”) or from the Internet (“Inbound”).

NOTE: To block access, to/from a single IP address, enter that IP address as the Host IP Address and use a Host Subnet Mask of “255.255.255.255”.

Click **Add** button to apply your changes.

Add Raw IP Filter

Go to “**Type**” drop-down menu, select “**Use Protocol Number**”.



Packet Filter

Parameters

Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

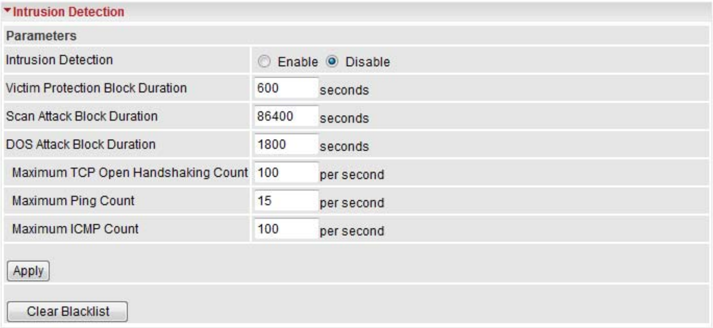
Field	Description
Rule name	Users-define description to identify this entry or choosing “Select” drop-down menu to select existing predefined rules.

Time Schedule	It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section
Protocol Number	Insert the port number, i.e. GRE 47
Inbound/Outbound	Select Allow or Block the access to the Internet ("Outbound") or from the Internet ("Inbound").

Click **Add** button to apply your changes.

7.4.3 Intrusion Detection

The router's Intrusion Detection System (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.



Intrusion Detection

Parameters

Intrusion Detection	○ Enable ● Disable
Victim Protection Block Duration	600 seconds
Scan Attack Block Duration	86400 seconds
DOS Attack Block Duration	1800 seconds
Maximum TCP Open Handshaking Count	100 per second
Maximum Ping Count	15 per second
Maximum ICMP Count	100 per second

Field	Description
Intrusion Detection	If enabled, IDS will block Smurf attack attempts. Default is false.

Victim Protection Block Duration	This is the duration for blocking Smurf attacks. Default value is 600 seconds.
Scan Attach Block Duration	This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include X'mas scan, IMAP SYN/FIN scan and similar attempts. Default value is 86400 seconds.
DOS Attack Block Duration	This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include Ascend Kill and WinNuke. Default value is 1800 seconds.
Maximum TCP Open Handshaking Count	This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds
Maximum Ping Count	This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.
Maximum ICMP Count	This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes

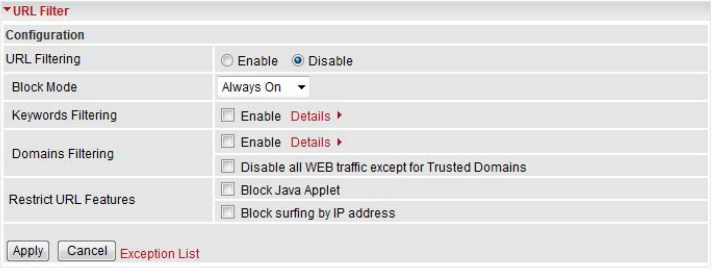
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes

Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP**, Src Port:** Source Port**, Dst Port:** Destination Port**, Dst IP:** Destination IP

7.4.4 URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



URL Filter

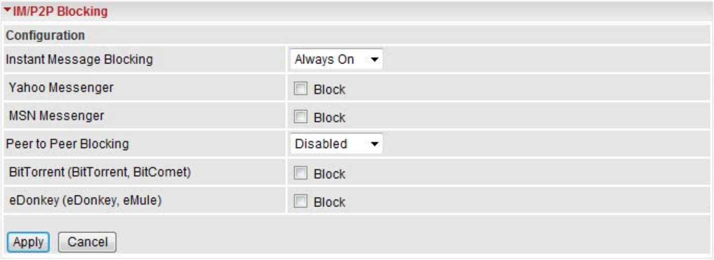
Configuration	
URL Filtering	○ Enable ● Disable
Block Mode	Always On
Keywords Filtering	□ Enable Details
Domains Filtering	□ Enable Details □ Disable all WEB traffic except for Trusted Domains
Restrict URL Features	□ Block Java Applet □ Block surfing by IP address

Field	Description
URL Filtering	To enable or disable URL Filter feature
Block Mode	A list of the modes that you can choose to check the URL filter rules. The default is set to Always On. • **Disabled:** No action will be performed by the Block Mode. • **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day. • **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to Time Schedule section.
Keywords Filtering	Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords

	are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.
Domains Filtering	This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure: 1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server. 2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped. 3. If the packet does not match either of the above two items, it is sent to the remote web server. 4. Please be note that the completed URL, "www" + domain name shall be specified. For example to block traffic to www.google.com.au, enter "www.google" or "www.google.com"
Restricted URL Features	This function enhances the restriction to your URL rules. • **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage your system via standard HTTP protocol. • **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping Domains Filtering function. Activates only and if Domain Filtering enabled.
Exception List	E' possibile indicare una lista di indirizzi IP che non verranno sottoposti alle policy di filtraggio URL configurate.

7.4.5 IM/P2P Blocking

IM, short for Instant Message, is required to use client program software that allows users to communicate, in exchanging text message, with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of computer users who share file to specific groups of people across the Internet. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Billion's IM and P2P blocking helps users to restrict LAN PCs to access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



IM/P2P Blocking

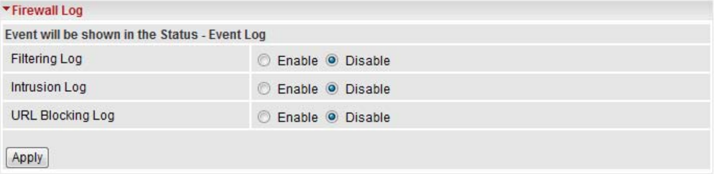
Configuration

Instant Message Blocking	Always On
Yahoo Messenger	□ Block
MSN Messenger	□ Block
Peer to Peer Blocking	Disabled
BitTorrent (BitTorrent, BitComet)	□ Block
eDonkey (eDonkey, eMule)	□ Block

Field	Description
Instant Message Blocking	The default is set to Disabled. • **Disabled:** Instant Message blocking is not triggered. No action will be performed. • **Always On:** Action is enabled. • **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to Time Schedule section.
Yahoo/MSN Messenger	Check the box to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the Instant Message

	Blocking first.
Peer to Peer Blocking	The default is set to Disabled. **Disabled:** Instant Message blocking is not triggered. No action will be performed. **Always On:** Action is enabled. **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to Time Schedule section.
BitTorrent / eDonkey	Check the box to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the Peer to Peer Blocking first

7.4.6 Firewall Log


▾Firewall Log

Event will be shown in the Status - Event Log

Filtering Log	○ Enable ● Disable
Intrusion Log	○ Enable ● Disable
URL Blocking Log	○ Enable ● Disable

Firewall Log display log information of any unexpected action with your firewall settings. Check the **Enable** box to activate the logs.

Log information can be seen in the **Status – Event Log** after enabling.

7.5 Qos (Quality of Service)

QoS function helps you to control your network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream.

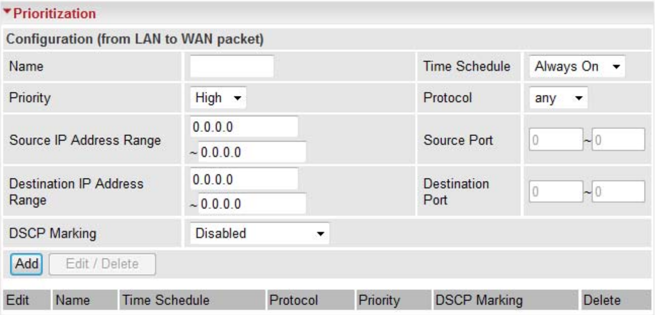
7.5.1 Prioritization

There are three priority settings to be provided in the Router:

- **High**
- **Normal**
- **Low**
-

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%).

To delete the application, you can choose **Delete** option and then click **Edit/Delete**.



Prioritization

Configuration (from LAN to WAN packet)

Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete

Field	Description
Name	User-define description to identify this new policy/application
Time Schedule	Scheduling your prioritization policy
Priority	The priority given to each policy/application. Its default setting is set to High; you may adjust this setting to fit your policy/application.
Source IP Address Range	The source IP address or range of packets to be monitored

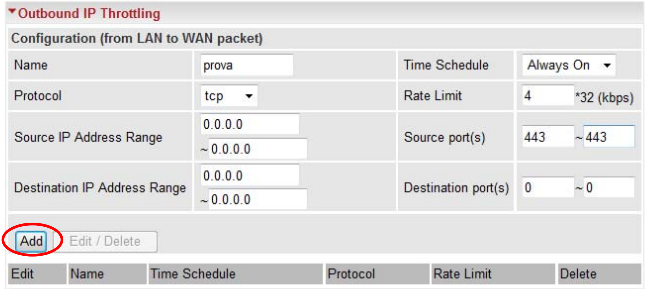
Source Port	The source port of packets to be monitored
Destination IP Address Range	The destination IP address or range of packets to be monitored
Destination Port	The destination port of packets to be monitored.
DSCP Marking	Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value.

DSCP Mapping Table

WebShare 3G 244WN	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

7.5.2 IP Throttling (Outbound e Inbound)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.



Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name	prova	Time Schedule	Always On
Protocol	tcp	Rate Limit	4 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	443 ~ 443
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete

Field	Description
Name	User-define description to identify this new policy/name
Time Schedule	Scheduling your prioritization policy. Refer to Time Schedule for more information
Protocol	The name of supported protocol.
Rate Limit	To limit the speed of outbound traffic
Source IP Address Range	The source IP address or range of packets to be monitored
Source Port	The source port of packets to be monitored
Destination IP Address Range	The destination IP address or range of packets to be monitored
Destination Port	The destination port of packets to be monitored.

7.6 Virtual Server

In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

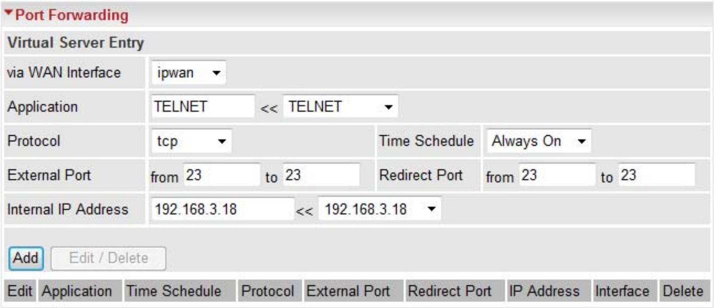
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the WAN configuration section of this manual for more information on NAT. The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

7.6.1 Port Forwarding

Because NAT can act as a "natural" Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.



Port Forwarding

Virtual Server Entry

via WAN Interface	ipwan		
Application	TELNET << TELNET		
Protocol	tcp	Time Schedule	Always On
External Port	from 23 to 23	Redirect Port	from 23 to 23
Internal IP Address	192.168.3.18 << 192.168.3.18		

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete

Field	Description
Application	Users-define description to identify this entry or click --Select-- drop-down menu to select existing predefined rules.
Protocol	It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.
Time Schedule	User-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to Time Schedule section
External Port	The Port number on the Remote/WAN side used when accessing the virtual server.
Redirect Port	The Port number used by the Local server in the LAN network.
Internal IP Address	The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

NOTE: Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

⚠ If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

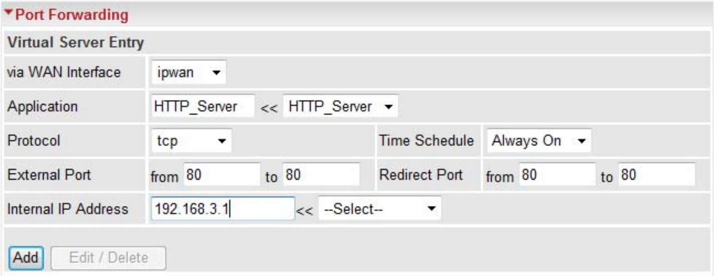
Application	Incoming Connection	Outcoming Connection
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
mIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey/Emule	Nessuno	principalmente 4660-4662 TCP , 4665-4672 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863 UDP 6901 UDP 5190
VNC	Nessuno	TCP 5900

Service	Port Number / Protocol
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

If you like to remote accessing your Router through the Web/HTTP at all time, you would need to enable port number 80 (Web/HTTP) and map to Router's IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the

Router with IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the Application click Helper. A list of predefined rules window will pop and select HTTP_Sever.

Application: HTTP_Sever
Time Schedule: Always On
Protocol: tcp
External Port: 80-80
Redirect Port: 80-80
IP Address: 192.168.3.1



Port Forwarding

Virtual Server Entry

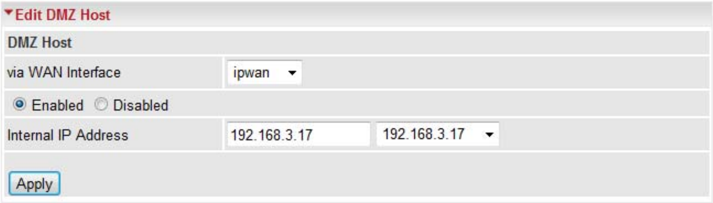
via WAN Interface	ipwan		
Application	HTTP_Server << HTTP_Server		
Protocol	tcp	Time Schedule	Always On
External Port	from 80 to 80	Redirect Port	from 80 to 80
Internal IP Address	192.168.3.1 << --Select--		

Click **Add** to apply your settings.

7.6.2 Edit DMZ Host

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

⚠ This Local computer exposing to the Internet may face varies of security risks.



Edit DMZ Host

DMZ Host

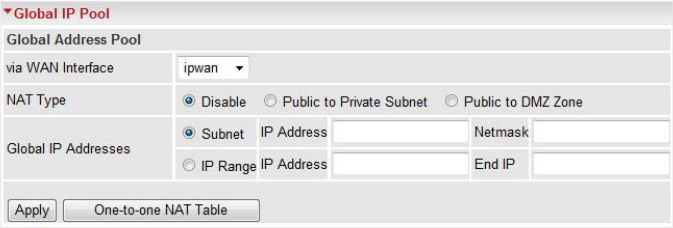
via WAN Interface	ipwan	
● Enabled ○ Disabled		
Internal IP Address	192.168.3.17	192.168.3.17

Field	Description
Enabled/Disabled	• **Enabled:** It activates your DMZ function. • **Disabled:** As set in default setting, it disables the DMZ function.
Internal IP Address	Give a static IP address to the DMZ Host when Enabled radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **Apply** button to apply your changes.

7.6.3 Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private/local IP address to a global/public IP address. If you have multiple public/WAN IP addresses from you ISP, you are eligible for One-to-One NAT to utilize these IP addresses.



Global IP Pool

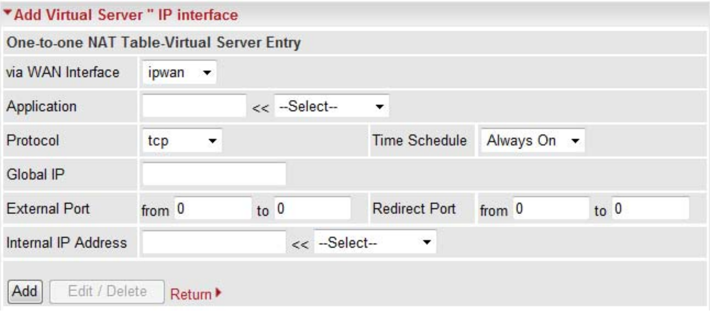
Global Address Pool

via WAN Interface	ipwan			
NAT Type	● Disable ○ Public to Private Subnet ○ Public to DMZ Zone			
Global IP Addresses	● Subnet	IP Address	Netmask	
	○ IP Range	IP Address	End IP	

Field	Description
NAT Type	Select desired NAT type. As set in default setting, it disables the One-to-One NAT function.
Global IP Address	• **Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method. • **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

Select the **Apply** button to apply your changes.

Check One-to-one NAT Table to create a new One-to-One NAT rule:



▾Add Virtual Server " IP interface

One-to-one NAT Table-Virtual Server Entry

via WAN Interface	ipwan		
Application	<< --Select--		
Protocol	tcp	Time Schedule	Always On
Global IP			
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select--		

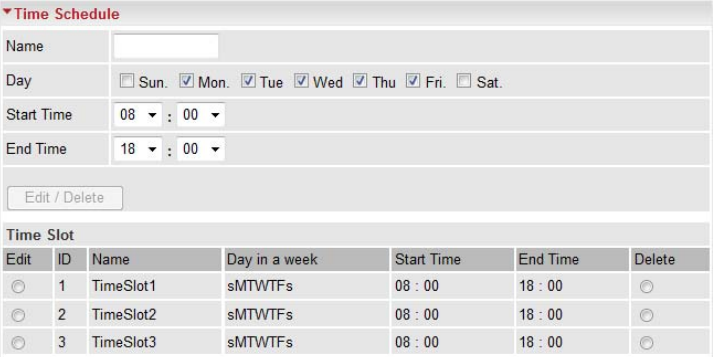
Field	Description
Application	Users-defined description to identify this entry or click --Select-- drop-down menu to select existing predefined rules.
Protocol	It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to

	specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP
Time Schedule	User-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to Time Schedule section
Global IP	Define a public/ WAN IP address for this Application to use. This Global IP address must be defined in the Global IP Address.
External Port	The Port number on the Remote/WAN side used when accessing the virtual server.
Redirect Port	The Port number used by the Local server in the LAN network.
Internal IP Address	The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

Select the **Add** button to apply your changes.

7.7 Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications. This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



▾Time Schedule

Name	
Day	□ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. □ Sat.
Start Time	08 : 00
End Time	18 : 00

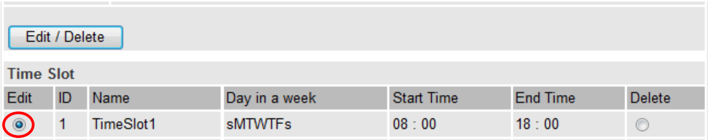
Edit / Delete

Time Slot

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
○	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○
○	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	○
○	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	○

To edit a Time Slot:

1. Choose any Time Slot (ID 1 to ID 16) to edit, click **Edit** radio button.



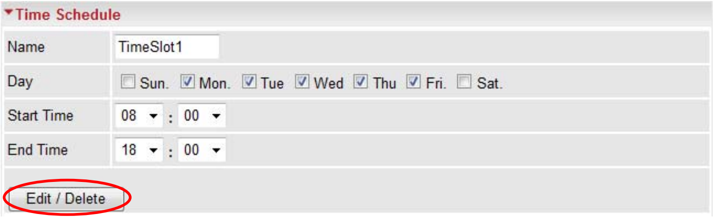
Edit / Delete

Time Slot

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
●	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○

NOTE: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the day(s) is not selected, and no rule will apply on this day(s).

2. A detailed setting of this Time Slot will be shown.



Time Schedule

Name	TimeSlot1
Day	□ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. □ Sat.
Start Time	08 : 00
End Time	18 : 00

Edit / Delete

Field	Description
Name	A user-define description to identify this time portfolio.
Day	The default is set from Monday through Friday. You may specify the days for the schedule to be applied.
Start Time	The default is set at 8:00 AM. You may specify the start time of the schedule.
End Time	The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

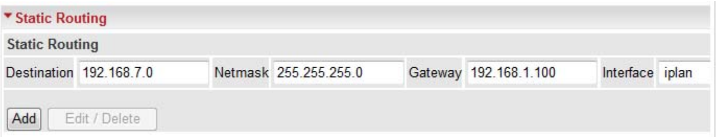
Choose Edit radio button and click **Edit/Delete** button to apply your changes.

To delete a Time Slot rule, choose **Delete** radio button, and click **Delete** button to delete the existing Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

7.8 Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

7.8.1 Static Route



▾ Static Routing

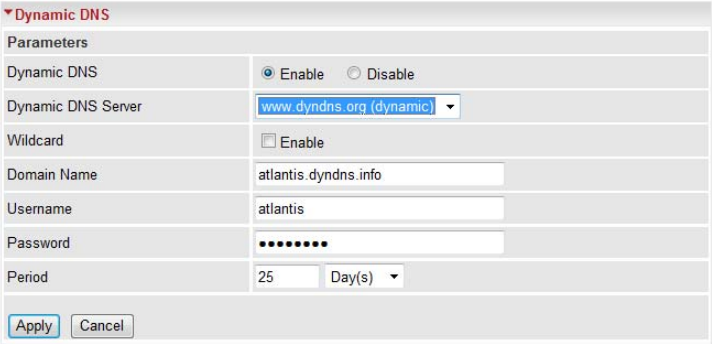
Static Routing

Destination	192.168.7.0	Netmask	255.255.255.0	Gateway	192.168.1.100	Interface	iplan

Field	Description
Destination	This is the destination subnet IP address.
Netmask	Subnet mask of the destination IP addresses based on above destination subnet IP.
Gateway	This is the gateway IP address to which packets are to be forwarded.
Interface	Select the interface through which packets are to be forwarded.
Cost	This is the same meaning as Hop. This should usually be left at 1.

7.8.2 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



▾Dynamic DNS

Parameters	
Dynamic DNS	● Enable ○ Disable
Dynamic DNS Server	www.dyndns.org (dynamic) ▾
Wildcard	□ Enable
Domain Name	atlantis.dyndns.info
Username	atlantis
Password	●●●●●●●●●
Period	25 Day(s) ▾

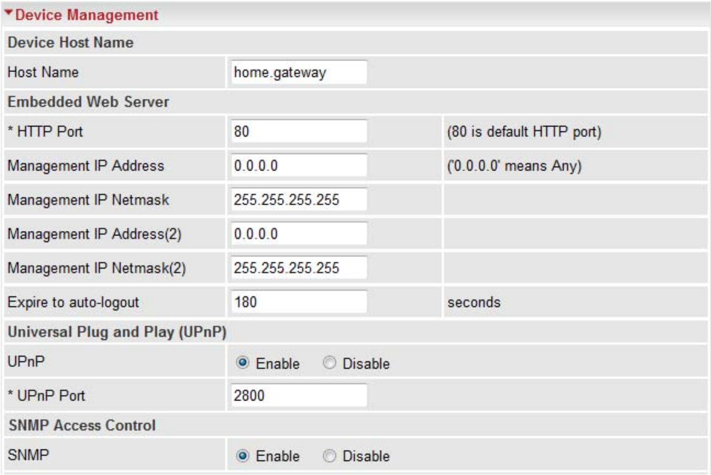
You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/ (there are more than 5 DDNS services supported).

Field	Description
Dynamic DNS	• **Disable:** Check to disable the Dynamic DNS function. • **Enable:** Check to enable the Dynamic DNS function.
Dynamic DNS Server	Select the DDNS service you have established an account with.
Domain Name	Insert the domain name associated to the DDNS account.
Username/Password	Insert username and password for DDNS account login.
Period	Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Select the **Apply** button to apply your changes.

7.8.3 Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



▾Device Management

Device Host Name		
Host Name	home.gateway	
Embedded Web Server		
* HTTP Port	80	(80 is default HTTP port)
Management IP Address	0.0.0.0	('0.0.0.0' means Any)
Management IP Netmask	255.255.255.255	
Management IP Address(2)	0.0.0.0	
Management IP Netmask(2)	255.255.255.255	
Expire to auto-logout	180	seconds
Universal Plug and Play (UPnP)		
UPnP	● Enable ○ Disable	
* UPnP Port	2800	
SNMP Access Control		
SNMP	● Enable ○ Disable	

Device Host Name

Field	Description
Host Name	Give a name for it

Embedded Web Server

Field	Description
HTTP Port	This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for

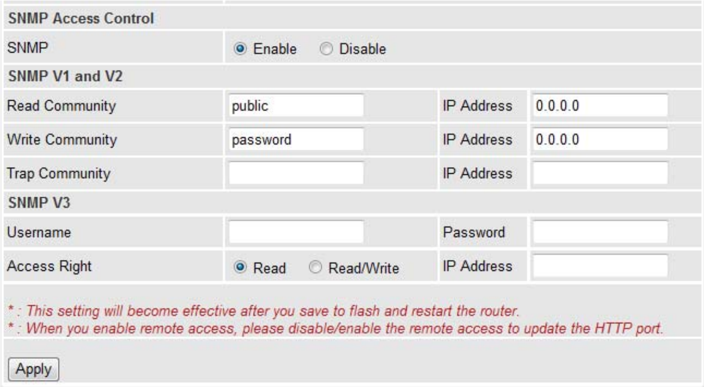
	example, they are running a web server on a PC within their LAN.
Management IP Address / Netmask	You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.
Expire to Auto-logout	Specify a time frame for the system to auto-logout the user's configuration session.

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Universal Plug'n'Play (UP'n'P)

Field	Description
UPnP	• **Disable:** Check to disable the router's UPnP functionality. • **Enable:** Check to enable the router's UPnP functionality.
UPnP Port	Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.



SNMP Access Control			
SNMP	● Enable ○ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	● Read ○ Read/Write	IP Address	

** : This setting will become effective after you save to flash and restart the router.*
** : When you enable remote access, please disable/enable the remote access to update the HTTP port.*

SNMP Access Control

Field	Description
SNMP	Enable or disable SNMP control.

SNMP V1 and V2

Field	Description
Read Community	Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.
Write Community	Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.
Trap Community	Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the

	string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

NOTE:

The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least. Example:
Host Name: homegateway ==> **Incorrect**
Host Name: home.gateway or my.home.gateway ==> **Correct**

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard. SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

RFC 1213 (MIB-II):
System group
Interfaces group
Address Translation group
IP group
ICMP group
TCP group
UDP group
EGP (not applicable)
Transmission
SNMP group

RFC1650 (EtherLike-MIB):
dot3Stats

RFC 1493 (Bridge MIB):
dot1dBase group
dot1dTp group
dot1dStp group (if configured as spanning tree)

RFC 1471 (PPP/LCP MIB):
pppLink group
pppLqr group (not applicable)

RFC 1472 (PPP/Security MIB):
PPP Security Group)

RFC 1473 (PPP/IP MIB):
PPP IP Group

RFC 1474 (PPP/Bridge MIB):
PPP Bridge Group

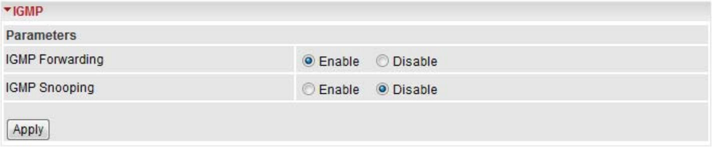
RFC1573 (IfMIB):
ifMIBObjects Group

RFC1695 (atmMIB):
atmMIBObjects

RFC 1907 (SNMPv2):
only snmpSetSerialNo OID

7.8.4 IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.



IGMP

Parameters

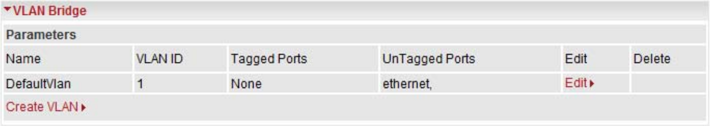
IGMP Forwarding ● Enable ○ Disable

IGMP Snooping ○ Enable ● Disable

Field	Description
IGMP Forwarding	Accepting multicast packet. Default is set to **Enable**.
IGMP Snooping	Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to **Disable**.

7.8.5 VLAN Bridge

This section allows you to create VLAN group and specify the member.



VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	UnTagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,	Edit ▸	

Field	Description
Edit	Edit your member ports in selected VLAN group.
Create VLAN	To create another VLAN group.

8. Logout

To exit the router’s web interface, choose Logout. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the Advanced section of this manual for more information.

APPENDIX A: Troubleshooting

This chapter covers potential problems and the corresponding remedies.

A.1 Using LEDs to diagnose problems

The LEDs are useful aides for finding possible problem causes.

A.1.1 Power LED

The PWR LED on the front panel does not light up.

Steps	Corrective Action
1	Make sure that the ADSL Router's power adaptor is connected to the ADSL Router and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the ADSL Router and the power source are both turned on and the ADSL Router is receiving sufficient power.
3	Turn the ADSL Router off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

A.1.2 LAN LED

The LAN LED on the front panel does not light up.

Steps	Corrective Action
1	Check the Ethernet cable connections between the ADSL Router and the computer or hub.
2	Check for faulty Ethernet cables.
3	Make sure your computer's Ethernet card is working properly.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.1.3 ADSL LED

The DSL LED on the front panel does not light up.

Steps	Corrective Action
1	Check the telephone wire and connections between the ADSL Router DSL port and the wall jack.
2	Make sure that the telephone company has checked your phone line and set it up for DSL service.
3	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the Maintenance chapter (web configurator) or the System Information and Diagnosis chapter.
4	If these steps fail to correct the problem, contact your local distributor for assistance.

A.2 Telnet

I cannot telnet into the ADSL Router.

Steps	Corrective Action
1	Check the LAN port and the other Ethernet connections.
2	Make sure you are using the correct IP address of the ADSL Router. Check the IP address of the ADSL Router.
3	Ping the ADSL Router from your computer. If you cannot ping the ADSL Router, check the IP addresses of the ADSL Router and your computer. Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the ADSL Router.
4	Make sure you entered the correct password. The default password is “admin”. If you have forgot your username or password, refer to Section A.5.
5	If these steps fail to correct the problem, contact the distributor.

A.3 WEB Configurator

I cannot access the web configurator.

Steps	Corrective Action
1	Make sure you are using the correct IP address of the ADSL Router. Check the IP address of the ADSL Router.

2	Make sure that there is not an console session running.
3	Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.
4	For WAN access, you must configure remote management to allow server access from the Wan (or all).
5	Your computer's and the ADSL Router's IP addresses must be on the same subnet for LAN access.
6	If you changed the ADSL Router's LAN IP address, then enter the new one as the URL.
7	Remove any filters in LAN or WAN that block web service.
8	See also Section A.9.

The web configurator does not display properly.

Steps	Corrective Action
1	Make sure you are using Internet Explorer 5.0 and later versions.
2	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files … button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

A.4 Login Username e Password

I forgot my login username and/or password.

Steps	Corrective Action
1	If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This will erase all custom configurations and restore all of the factory defaults including the password.
2	Press the RESET button for 10 seconds, and then release it. When the PWR LED begins red, the defaults have been restored and the ADSL Router restarts. Or refer to the Resetting the ADSL Router

	section for uploading a configuration file via console port.
3	The default username is “admin”. The default password is “atlantis”. The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.
4	It is highly recommended to change the default username and password. Make sure you store the username and password in a save place.

A.5 LAN Interface

I cannot access the ADSL Router from the LAN or ping any computer on the LAN.

Steps	Corrective Action
1	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If the 10M/100M LEDs on the front panel are both off, refer to Section A.1.2.
2	Make sure that the IP address and the subnet mask of the ADSL Router and your computer(s) are on the same subnet.

A.6 WAN Interface

Initialization of the ADSL connection failed.

Steps	Corrective Action
1	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the ADSL Router should be on.
2	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
3	Restart the ADSL Router. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

I cannot get a WAN IP address from the ISP.

Steps	Corrective Action
1	The ISP provides the WAN IP address after authenticating you.

	Authentication may be through the user name and password, the MAC address or the host name.
2	The username and password apply to PPPoE and PPoA encapsulation only. Make sure that you have entered the correct Service Type, User Name and Password (be sure to use the correct casing).

A.7 Internet Access

I cannot access the Internet.

Steps	Corrective Action
1	Make sure the ADSL Router is turned on and connected to the network.
2	If the DSL LED is off, refer to Section A.1.3.
3	Verify your WAN settings.
4	Make sure you entered the correct user name and password.

Internet connection disconnects.

Steps	Corrective Action
1	Check the schedule rules.
2	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting.
3	Contact your ISP.

A.8 Remote Management

I cannot remotely manage the ADSL Router from the LAN or WAN.

Steps	Corrective Action
1	Refer to the Remote Management Limitations section in the Firmware and Configuration File Management chapter for scenarios when remote management may not be possible.
2	Use the ADSL Router's WAN IP address when configuring from the WAN. Use the ADSL Router's LAN IP address when configuring from the LAN.
3	Refer to Section A.6 for instructions on checking your LAN

	connection. Refer to Section A.7 for instructions on checking your WAN connection.
4	See also the Section A.4.

A.9 Remote Node Connection

I cannot connect to a remote node or ISP.

Steps	Corrective Action
1	Check WAN screen to verify that the username and password are entered properly.
2	Verify your login name and password for the remote node.
3	If these steps fail, you may need to verify your login and password with your ISP.

A.10 Frequently Asked Question

Question	Can I run an application from a remote computer over the wireless network?
Answer	This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Question	Can I play computer games with other members of the wireless network?
Answer	Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's user guide for more information.

Question	What is Spread Spectrum?
Answer	Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that

	is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Question	What is DSSS? What is FHSS? And what are their differences?
Answer	Frequency-Hopping Spread-Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-Sequence Spread-Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Question	Would the information be intercepted while transmitting on air?
Answer	WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN offers the encryption function (WEP) to enhance security and access control.

Question	What is WEP?
Answer	WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm, as described in the IEEE 802.11 standard.

Question	What is infrastructure mode?
Answer	When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a wired network through a wireless access point.

Question	What is roaming?
Answer	Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the workstation must make sure that it is the same channel number with the access point of dedicated coverage area.

Question	What is ISM band?
Answer	The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

Question	What is the IEEE 802.11g standard?
Answer	Approved in June, 2003 as an IEEE standard for wireless local area networks (WLANs), 802.11g offers wireless transmission over relatively short distances at up to 54 megabits per second (Mbps) compared with the 11 megabits per second of the 802.11b (Wi-Fi) standard. Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it.

APPENDIX B: Modem 3G Compatibility List

Following a listo of compatible devices (HSDPA/GPRS/UMTS) tested and fully compliant with WebShare 3G 244WN:

Brand	Model
Sierra	Aircard 880U
Sierra	Aircard 875U
Sierra	Aircard 885U
Huawei	E180
Huawei	E170
Huawei	E160G
Huawei	E169G
Huawei	E169
Huawei	E220
Huawei	E270
Huawei	E172
Huawei	E272
ZTE	MF626 NEW
ZTE	MF638
ZTE	MF628
ZTE	MF622

NOVATEL	MC950D
NOVATEL	MC930D NEW
NOVATEL	MC990D NEW
BandRich	Bandluxe C100
Alcatel	OT-X020
C-Motech	D50
Telstra	USB3-8521
Option	GlobeSurfer iCON 7.2 NEW
Option	iCON 225 NEW
Option	GlobeSurfer iCON HSUPA NEW
Option	GlobeTrotter HSUPA NEW

Only models in this list can work with WebShare 3G 244WN.

For updated compatibility list, refer to www.atlantis-land.com

APPENDIX C: Support

If you have any problems with the WebShare Wireless Router ADSL2+, please consult this manual. If you continue to have problems you should contact the dealer where you bought this ADSL Router. If you have any other questions you can contact the Atlantis Land company directly at the following address:

Atlantis Land
Via Pelizza da Volpedo, 59
20092 Cinisello Balsamo (MI) - Italy
Tel: +39. 02.00.632.300
Fax: +39. 02.66.016.666
Website: http://www.atlantis-land.com
Email: info@atlantis-land.com

Atlantis Land

Via Pelizza da Volpedo, 59
Cinisello Balsamo – MI – Italy
info@atlantis-land.com