# WebShare 242W
# Wireless ADSL2+ Router
## A02-RA242-W54

# USER'S MANUAL
A02-RA242-W54_ME01

**Where solutions begin**

**Copyright**

The Atlantis Land logo is a registered trademark of Atlantis Land SpA. All other names mentioned mat be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors and/or omissions.

**CE Mark Warning**

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

**FCC Warning**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

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

# TABLE OF CONTENTS

# Chapter 1
# Introduction

## 1.1 An Overview of the WebShare 242W

**Broadband Sharing and IP sharing**
The Wireless ADSL2+ Router supports 4 x 10/100 Mbps auto-negotiating Fast Ethernet ports for connection to your PC or LAN and downstream (with built-in ADSL2+ modem) rate up to 24Mbps. Power by NAT technology, dozens of network users can surf on the Internet and share the ADSL connection simultaneously by using one ISP account and one single IP address.

**Wireless**
With integrated IEEE802.11g Wireless Access Point (up to 54Mbps), the device offers quick and easy access among wired network and wireless network. The Wireless Router also supports WPA/WPA2 security, it increases the level of data protection and access control for Wireless LAN. Reverse-SMA 5 dBi Antenna provides extended coverage.

**Security: Firewall (SPI, DoS) & VLAN**
This product also serves as an Internet firewall, protecting your network from being accessed by outside users. Not only provide the natural firewall function (Network Address Translation, NAT), it also provides rich firewall features to secure user's network. The VLANs allow to segment the traffic of net and, in this way, they improve management and performance of entire network.

**Quality of Service and IP Throttling**
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 move through the router at lightning speed, even under heavy load. Using IP Throttling, bandwidth limits can be enforced on any system within your LAN, or even on a particular application.

**Easy Configuration and Management**
Support web based GUI and Telnet for configuration and management. Also supports remote management (Web and telnet) capability for remote user to configure and manage this product. It incorporates besides a client Dynamic DNS.

## 1.2 Package Contents

- WebShare 242W Wireless ADSL2+ Router
- Vera (Multilanguage Interactive Tutorial)

- One CD-Rom containing the online manual
- One Quick Start Guide
- One 5 dBi Antenna (R-SMA)
- One RJ-11 ADSL/telephone cable
- One CAT-5 LAN cable
- One AC-DC power adapter (12VDC, 1A)

**If any of the above items are missing, please contact your reseller.**

# 1.3 WebShare 242W Features

ADSL Router2+ provides the following features:

- **ADSL Multi-Mode Standard:** Supports downstream transmission rates of up to 8Mbps, the router is capable of up to 12/24 Mbps with ADSL2/2+, and upstream transmission rates of up to 1024Kbps. It also supports rate management that allows ADSL subscribers to select an Internet access speed suiting their needs and budgets. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2); G.hs(G994.1); G.dmt.bis(ITU G.992.3); Gdmt.bisplus(ITU G.992.5)].

- **Fast Ethernet Switch:** A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or cross-over cable can be used directly, this fast Ethernet switch will detect it automatically.

- **Wireless Ethernet 802.11g:** With built-in 802.11g access point for extending the communication media to WLAN while providing the WEP and WPA/WPA2 for securing your wireless networks.

- **Multi-Protocol to Establish A Connection:** 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:** Supports a WEB GUI page to install this device quickly. With this wizard, an end user can enter the information easily which they from the 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.

- **Network Address Translation (NAT):** Allows multi-users to access outside resource such as Internet simultaneously with one IP address/one Internet access account. Besides, many application layer gateway (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting and others.

- **Firewall:** Supports SOHO firewall with NAT technology. Automatically detects and blocks the Denial of Service (DoS) attack. The URL-blocking, packet filtering are also

supported. The hacker's attack will be recorded associated with timestamp in the security logging area. More firewall features will be added continually, please visit our web site to download latest firmware.

- **VLAN:** A VLAN is a group of end-stations that are not constrained by their physical location and can communicate as if a common broadcast domain, a LAN. The primary utility of using VLAN is to reduce latency and need for routers, using faster switching instead. Other VLAN utility includes:

    - Security, Security is increased with the reduction of opportunity in eavesdropping on a broadcast network because data will be switched to only those confidential users within the VLAN.

    - Cost Reduction, VLANs can be used to create multiple broadcast domains, thus eliminating the need of expensive routers.

    - Port-based (or port-group) VLAN is the common method of implementing a VLAN, and is the one supplied in the Switch.

- **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 move through the Router at 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.

- **Domain Name System (DNS) relay:** 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, then every DNS conversion requests packet from the PC to this router will be forwarded to the real DNS in the outside network. After the router gets the reply, then forwards it back to the PC.

- **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 an account from this free Web server http://www.dyndns.org/. There are more than 5 DDNS servers supported.

- **PPP over Ethernet (PPPoE):** Provide embedded PPPoE client function to establish a connection. Users can get greater access speed without changing the operation concept, sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. The Always ON, Dial On Demand and auto disconnection (Idle Timer) functions are provided too.

- **Virtual Server:** Users can specify some services to be visible from outside users. The router can detect incoming service request and forward it to the specific local computer to handle it. For example, users can assign a PC in a LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse an inside web server 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 also provides a higher-level security control.

- **Dynamic Host Control Protocol (DHCP) client and server:** In the WAN site, the DHCP client can get an IP address from the Internet Server Provider (ISP) automatically. In the LAN site, the DHCP server can allocate up to 253 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:** Supports an easy static table or RIP1/2 routing protocol to support routing capability.

- **SNTP:** An easy way to get the network real time information from an SNTP server.

- **SNMP:** SNMP is an application layer protocol that is used for managing networks (V1,V2 and V3)

- **Web based GUI:** supports web based GUI for configuration and management. It is user-friendly with an on-line help, providing necessary information and assist user timing. It also supports remote management capability for remote users to configure and manage this product.

- **Firmware Upgradeable:** the device can be upgraded to the latest firmware through the WEB based GUI.

- **Rich management interfaces:** Supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal application through console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage a device.

# 1.4 WebShare 242W Wireless  Application



Internet
Internet after Firewall
4 porte Fast Ethernet
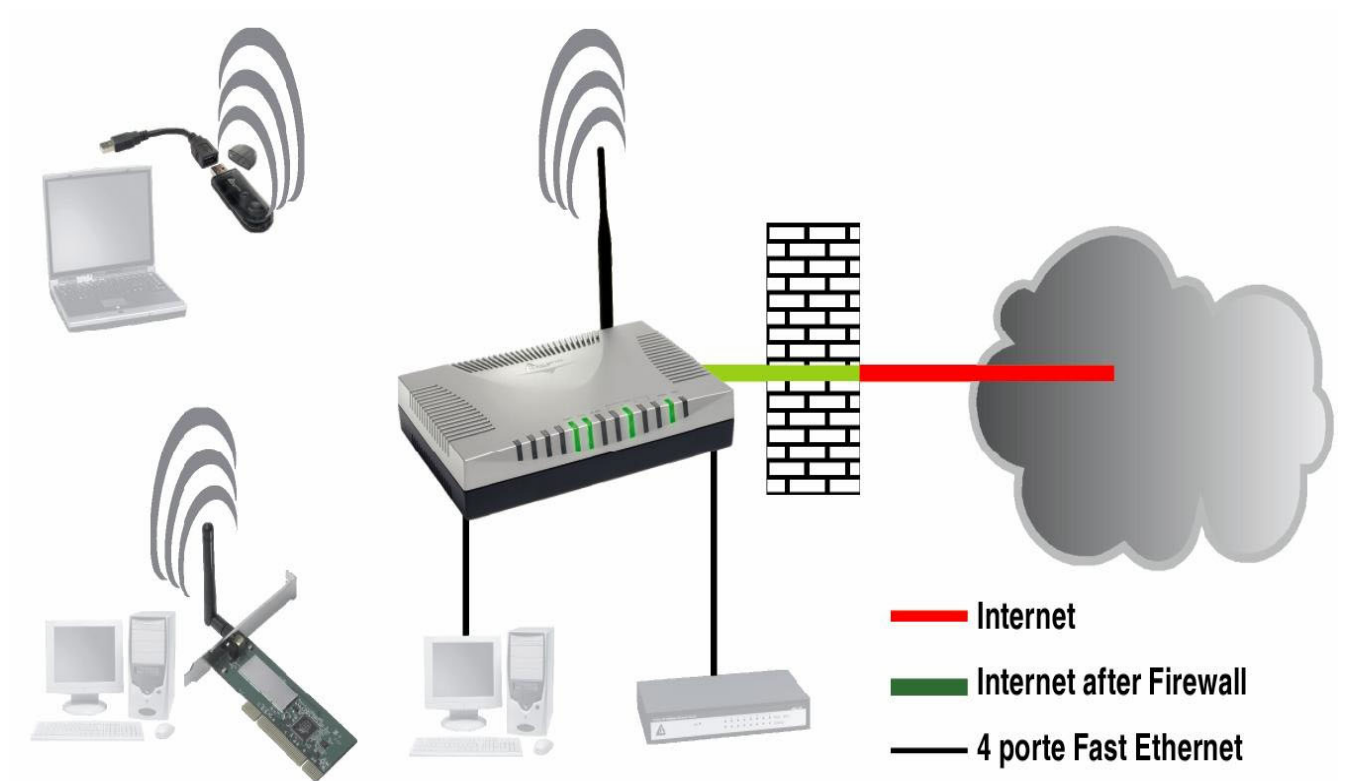
# Chapter 2
## Using WebShare 242W Wireless

## 2.1 Cautions for using the WebShare 242W Wireless

Do not place the WebShare 242W Wireless under high humidity and high temperature.

Do not use the same power source for WebShare 242W Wireless with other equipment.

Do not open or repair the case yourself. If the WebShare 242W Wireless is too hot, turn off the power immediately and have a qualified serviceman repair it.

Avoid using this product and all accessories outdoors.

Place the WebShare 242W Wireless on a stable surface.

Only use the power adapter that comes with the package.

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.

## 2.2 The Front LEDs
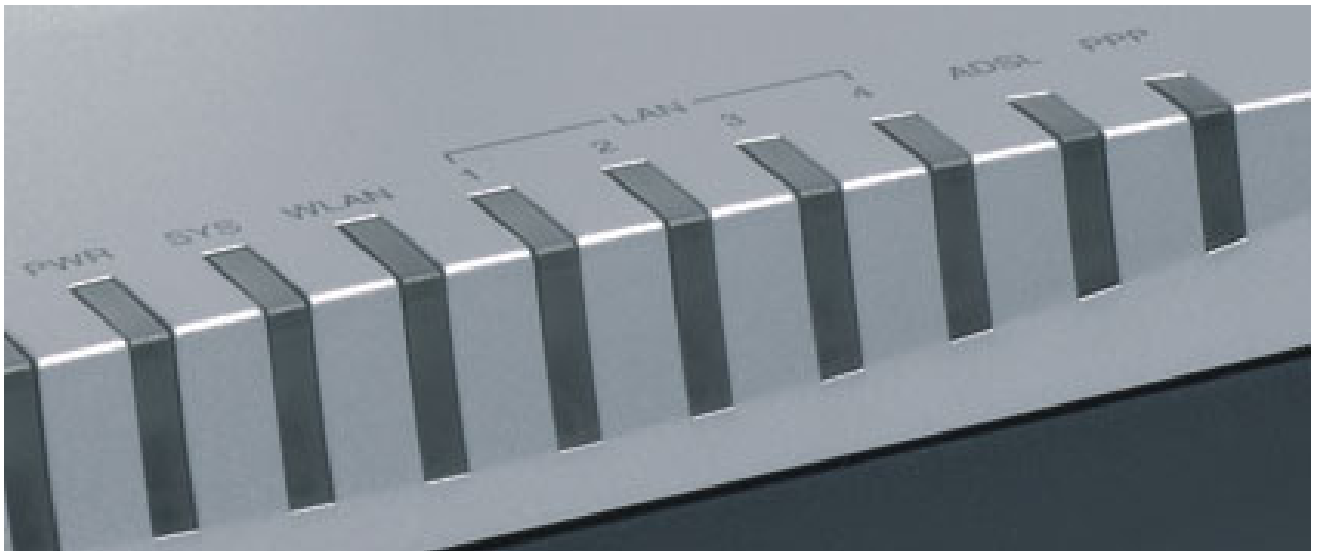


| LED | Meaning |
|---|---|
| **PWR** | Lights when power ON. |
| **SYS** | Lights when system is ready. |
| **WLAN** | Flashes when sending/receiving data. |
| **LAN** | Lights when connected to Ethernet device: |

| | • Green for 100Mbps; Orange for 10Mbps<br>• Blinking when data transmit/received. |
|---|---|
| **ADSL** | Lights when successfully connected to an ADSL DSLAM. |
| **PPP** | Steady glow when there is a PPPoA / PPPoE connection. |

# 2.3 The Rear Ports



| PORT | Meaning |
|---|---|
| **LINE** | Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network. |
| **LAN** | Connect an UTP Ethernet cable to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. |
| **RESET** | Recovery procedures for a lost web interface password:<br>After turning the router on press the *Emergency/Failure Recovery Button* on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. The login will be reset to *admin* and the password will be reset to *atlantis*, and the modem will be accessible via its default IP address at http://192.168.1.254/<br>This is used when you can not login to the router, e.g. forgot the password) |
| **PWR** | Connect the supplied power adapter to this jack. |
| **POWER (Switch)** | A Power ON/OFF switch. |

# 2.4 Cabling

The most common problem is bad cabling or ADSL line. Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. As a first check, verify that the LAN Link, ADSL , PWR, SYS LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (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.

Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including frequent disconnections.

## Application Scheme

Phone Line

Phone

Modem/Router ADSL
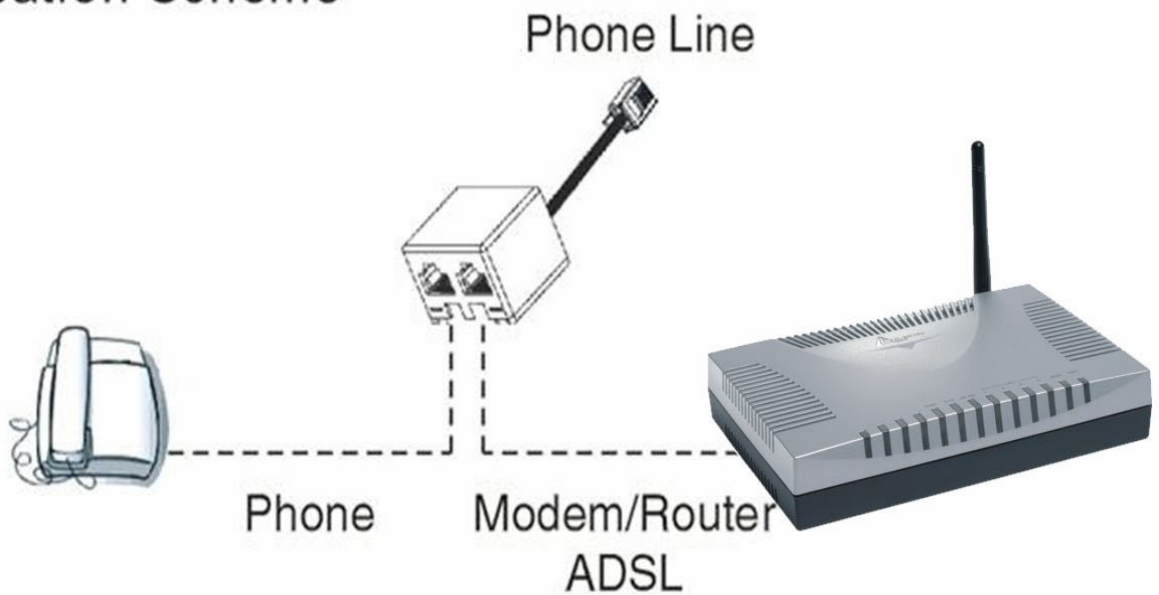
# Chapter 3

# Configuration

The WebShare 242W Wireless  can be configured with your Web browser.  The web browser is included as a standard application in the following operation systems, UNIX, Linux, Mac OS, Windows 95/98/NT/2000/Me, and etc. The product provides a very easy and user-friendly interface for configuration.

## 3.1 Before Configuration

This section describes the configuration required by LAN-attached PCs that communicate with the WebShare 242W Wireless , either to configure the device or for network access. These PCs must have an Ethernet interface installed properly, 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 of the ADSL Firewall Router. The default IP address of the WebShare 242W Wireless  is 192.168.1.254 and subnet mask is 255.255.255.0. The best and easy way is to configure the PC to get an IP address from the WebShare 242W Wireless . Also make sure you have UNINSTALLED any kind of software firewall that can cause problems while accessing the 192.168.1.254 IP address of the router.

Please follow the steps below for 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 MS Windows related manuals.

**NOTE:** Any TCP/IP capable workstation can be used to communicate with or through the WebShare 242W Wireless . To configure other types of workstations, please consult the manufacturer's documentation.

## 3.2 Connecting the WebShare 242W Wireless

- Connect the WebShare 242W Wireless  to a LAN (Local Area Network) and the ADSL/telephone network.
- Power on the device
- Make sure the PWR  is lit steady & LAN/ADSL LED is lit.
- Before taking the next step, make sure you have uninstalled any software firewall.
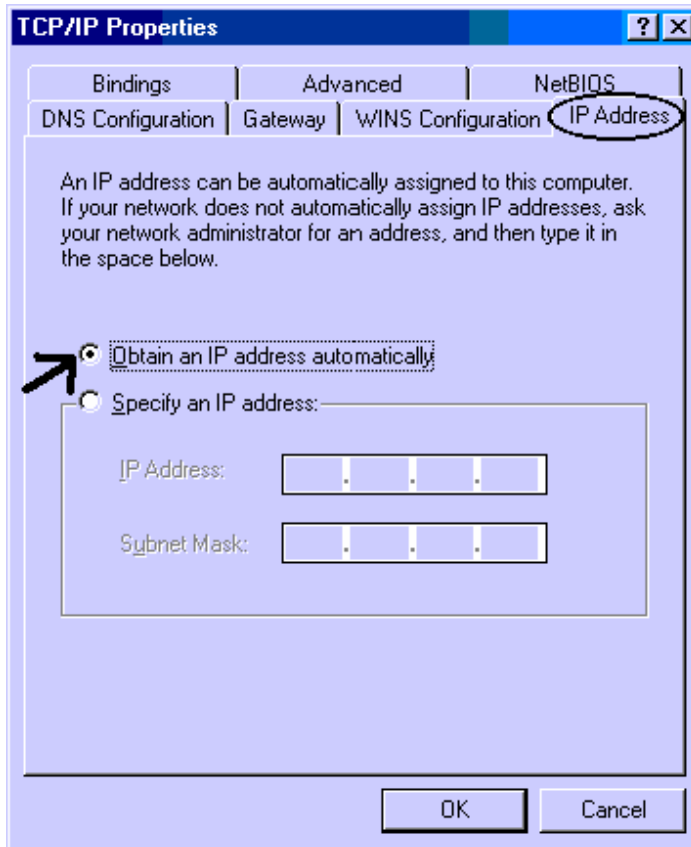
# 3.3 Configuring PC in Windows

## For Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.

2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC.
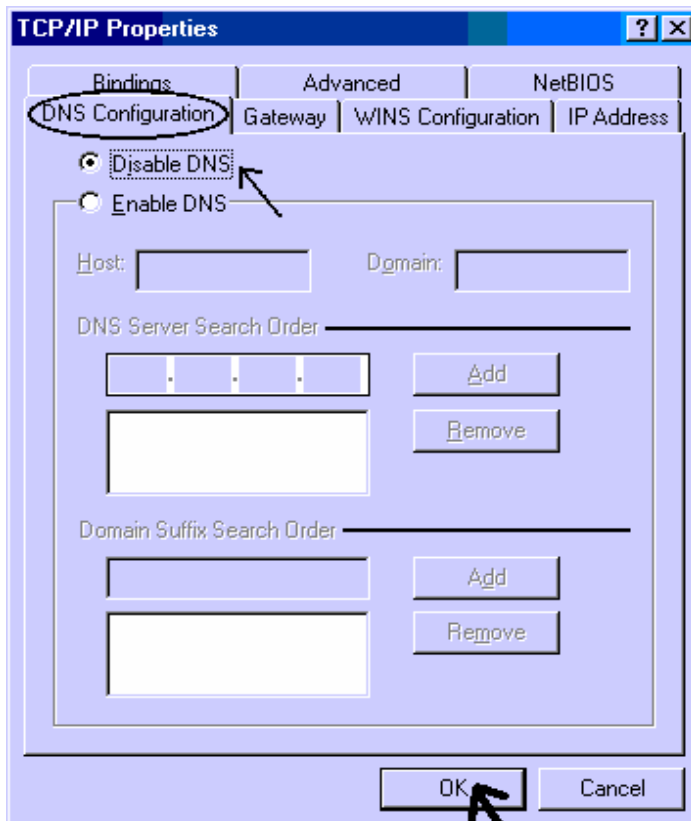
3.    Click Properties.
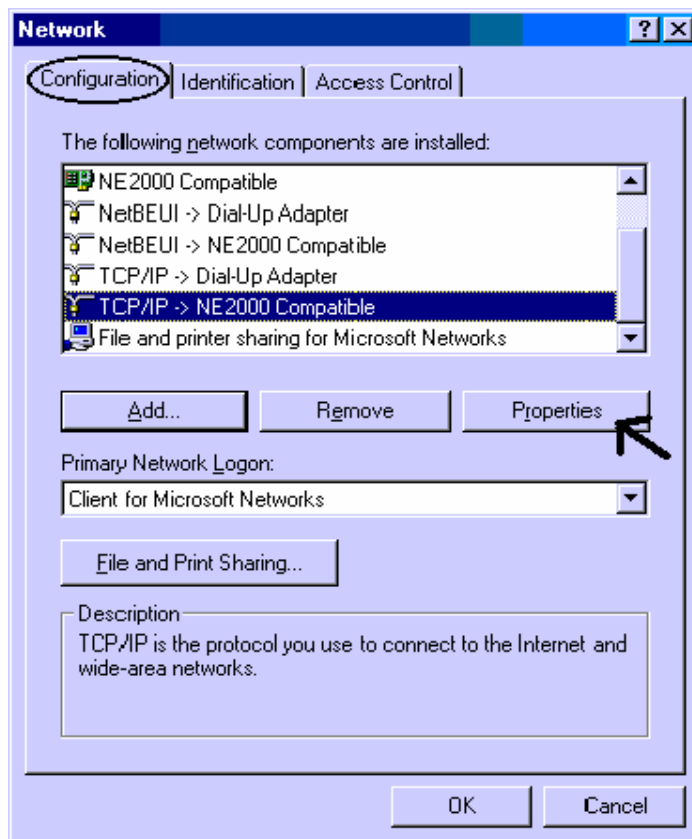


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.

**5.** Then select the **DNS Configuration** tab.

**6.** Select the **Disable DNS** radio button and click **"OK"** to finish the configuration.
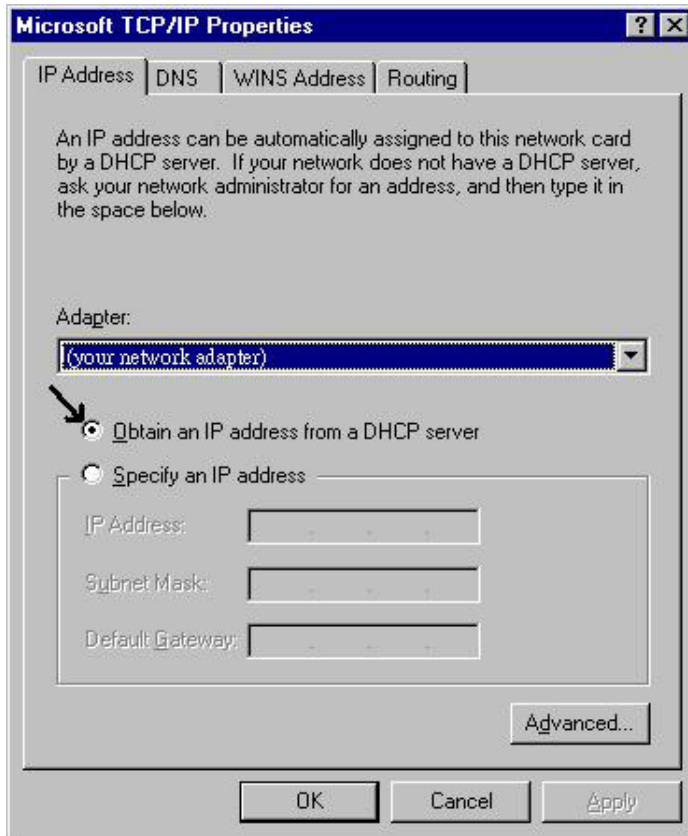
# For Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

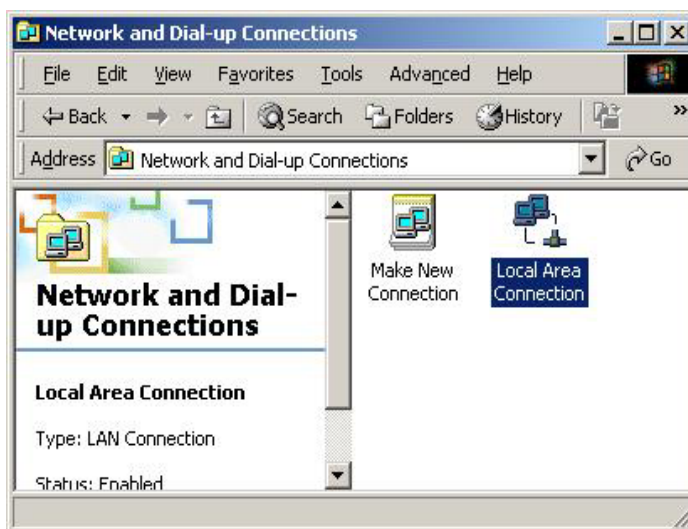2. Select **TCP/IP Protocol** and click **Properties**.
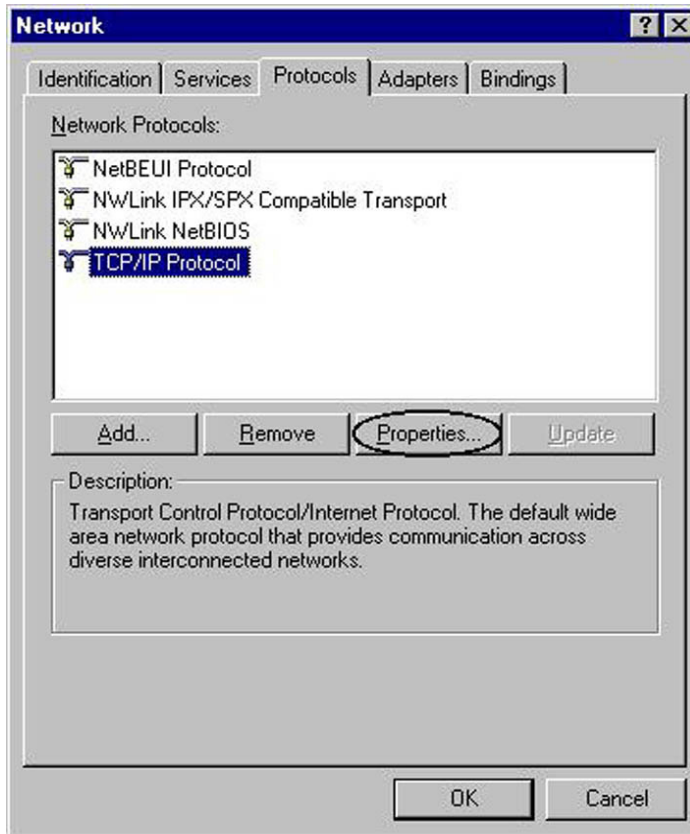


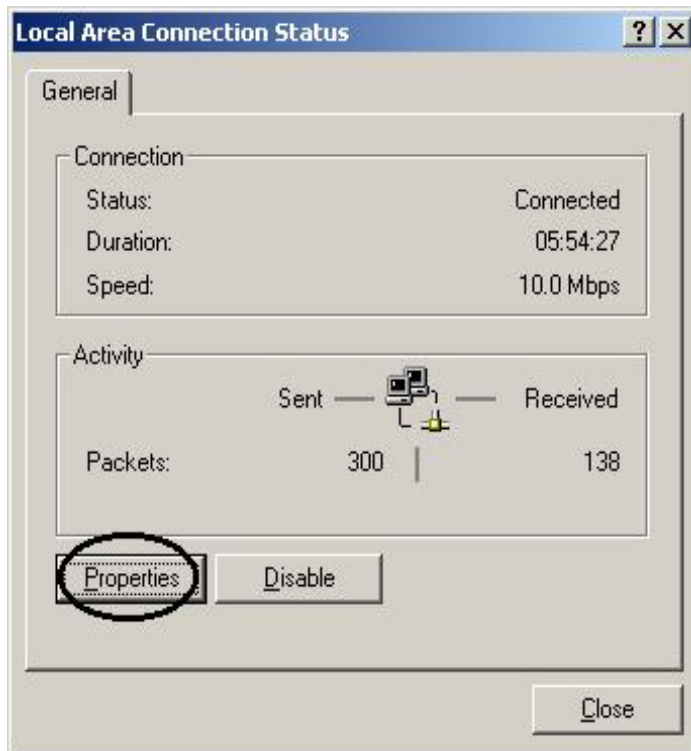3. Select the **Obtain an IP address from a DHCP server** radio button and click **"OK"**.
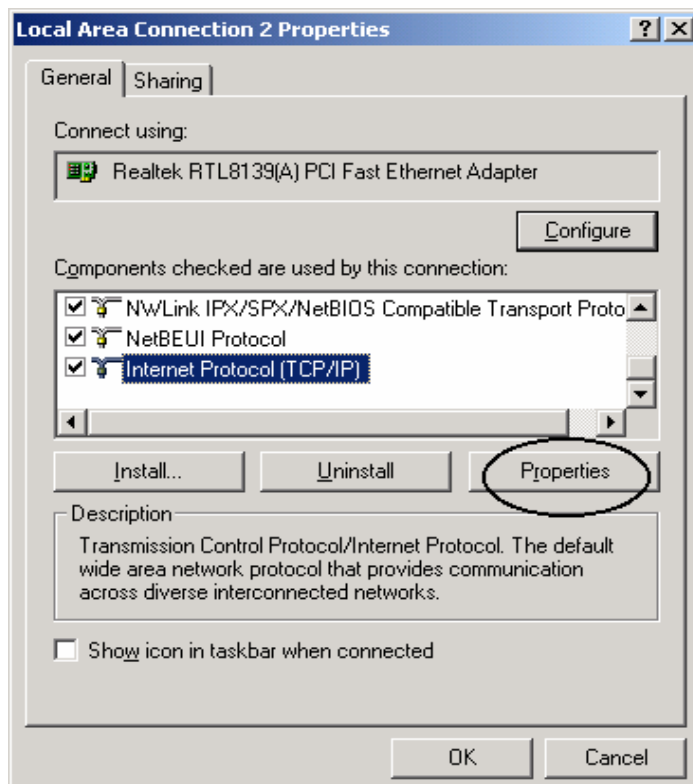
# For Windows 2000

1.  Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

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.

# For Windows XP

1.  Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections.**

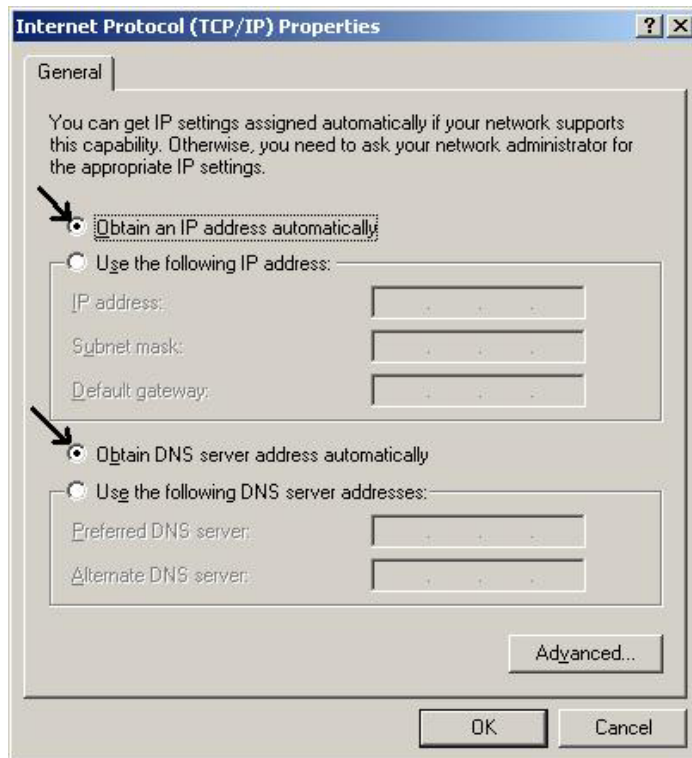2.  Double-click **Local Area Connection**



3.  In the **LAN Area Connection Status** window, click **Properties**.

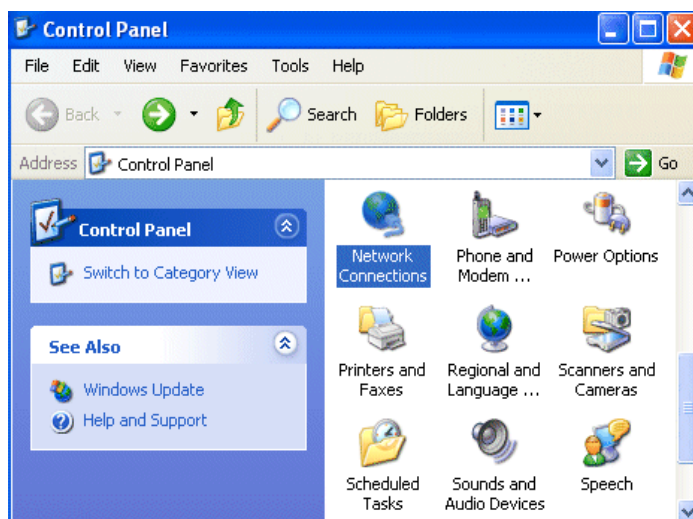**4.** Select **Internet Protocol (TCP/IP)** and click **Properties**.



**5.** Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons

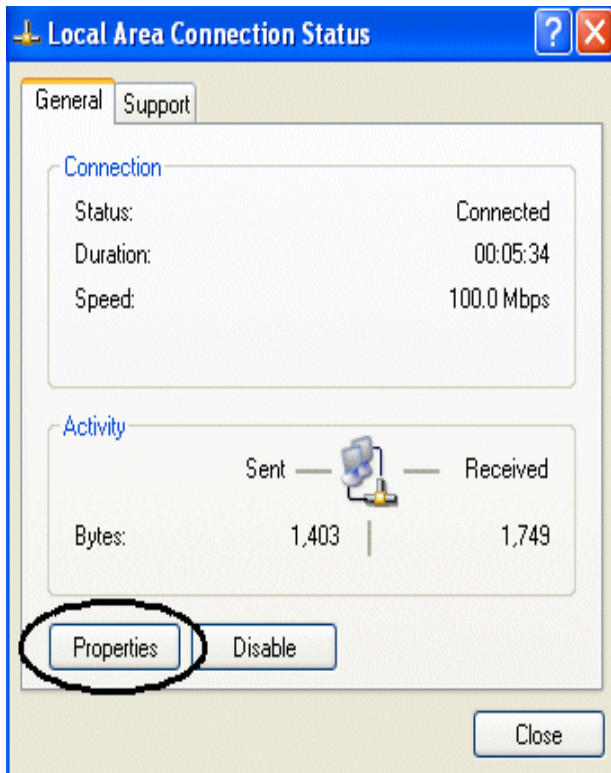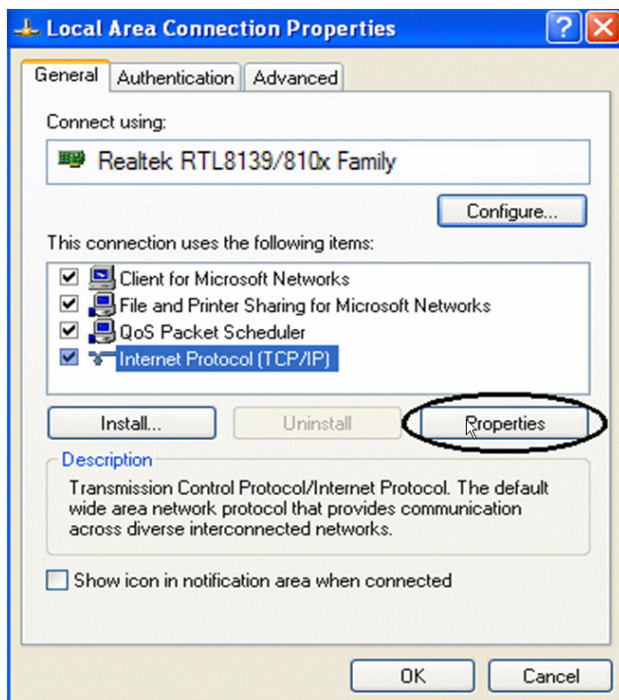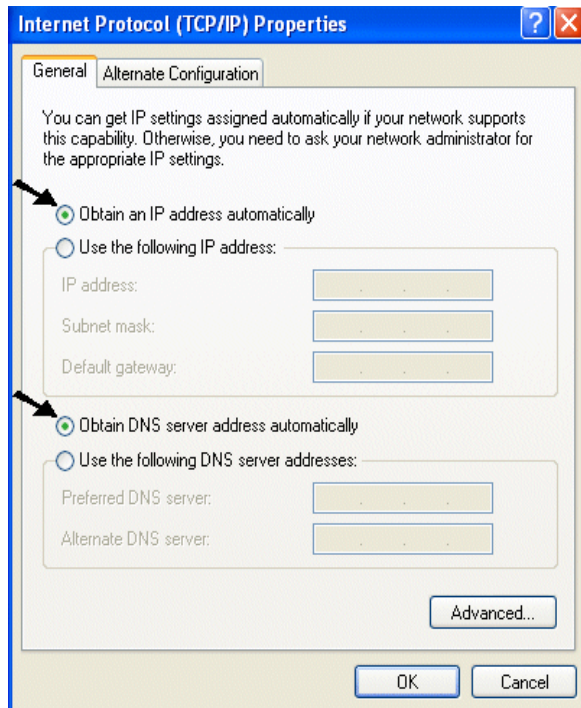**6.** Click **"OK"** to finish the configuration.

# 3.4 Factory Default Settings

Before configurating this WebShare 242W Wireless , you need to know the following default settings.

- Username: **admin**
- Password : **atlantis**
- IP Address : **192.168.1.254**
- Subnet Mask : **255.255.255.0**
- DHCP server is enabled.

## 3.4.1 Username and Password

The default username and password are **admin** and **atlantis** respectively.

If you ever forget the password to log in, you may press the RESET button to restore the factory default settings. After turning the router on press the Emergency/Failure Recovery Button on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings (approximately 10 seconds). The login will be reset to admin and the password will be reset to admin, and the modem will be accessible via its default IP address at http://192.168.1.254/

## 3.4.2 LAN and WAN Port Addresses

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

| LAN Port | | WAN Port |
|---|---|---|
| **IP address** | 192.168.1.254 | N/A |
| **Subnet Mask** | 255.255.255.0 | |
| **DHCP server function** | Enabled | |

# 3.5 Information from the ISP

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, IpoA.

Gather the information as illustrated in the following table and keep it for reference.

| | |
|---|---|
| **PPPoE** | VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed). |
| **PPPoA** | VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed). |
| **RFC1483 Bridged** | VPI/VCI, VC-based/LLC-based multiplexing and configure this product into BRIDGE Mode. |
| **RFC1483 Routed** | VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address). |
| **IPoA** | VPI/VCI, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address). |

# 3.6 Configuring with the Web Browser

Open the web browser, enter the local port IP address of this WebShare 242W Wireless , which defaults at **http://192.168.1.254**, and click "**Go**", a username and password window will appear.  The default **username** & **password** are **admin** & **atlantis**, in respectively
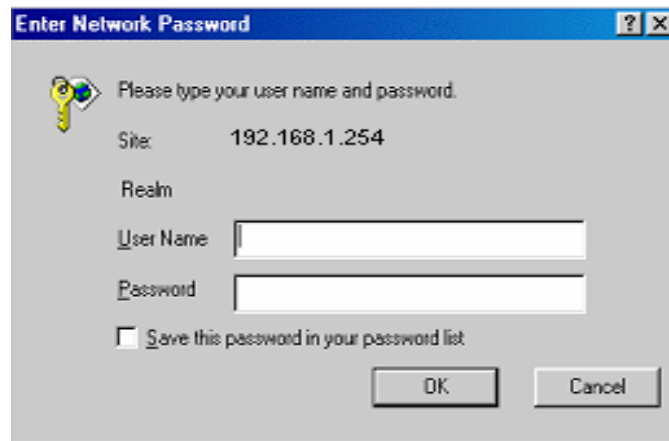
You will get a status report web page when login successfully.

At the configuration homepage, the left navigation page where bookmarks are provided links you directly to the desired setup page, including:

- **Status (ARP Table, Routing Table, DHCP Table, System Log, Security Log)**
- **Quick Start**
- **Configuration (LAN, WAN, System, Firewall, QoS, Virtual Server, Advanced)**
- **Save Config to Flash**
- **Language**

Click on the desired item to expand the page in the main navigation page.

# 3.6.1 STATUS

The Status section provides and contains many items including device H/W and S/W information, LAN, WAN, Port status and all defined interfaces. It also provides useful information for users to review the status of device.

Click on **Status** will open all the following subsections:
- **ARP Table**
- **Wireless Table**
- **Routing Table**
- **DHCP Table**
- **System Log**
- **Security Log**

## 3.6.1.1 ARP Table/ Wireless Table

The router's ARP (Address Resolution Protocol) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine 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.

### ARP Table

**IP <> MAC List**

| IP Address | MAC Address | Interface | Static |
|---|---|---|---|
| 192.168.1.187 | 00:E0:18:DF:7B:64 | br0 | no |

- **IP Address:** A list of IP addresses of devices on your LAN (Local Area Network).
- **MAC Address:** MAC (Media Access Control) address 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

## 3.6.1.2 Routing Table
Display the current routing paths of A02-RA242-W54.

### Routing Table

**Routing Table**

| # | Destination | Netmask | Gateway/Interface | Cost | | |
|---|-------------|---------|-------------------|------|------|--------|
| 1 | 151.6.134.65 | 255.255.255.255 | 0.0.0.0/ppp0 | 0 | Edit ▶ | Delete ▶ |
| 2 | 192.168.1.0 | 255.255.255.0 | 0.0.0.0/br0 | 0 | Edit ▶ | Delete ▶ |
| 3 | 0.0.0.0 | 0.0.0.0 | 151.6.134.65/ppp0 | 0 | Edit ▶ | Delete ▶ |

Create ▶

### Static Route

**Add Rule4**

| Destination | | | |
|-------------|--|--|--|
| Netmask | | | |
| Gateway | | Interface | Please Select ▼ |
| Cost | 0 | | |

Apply   Cancel

- #:  **Item number**
- **Destination:** IP address of the destination network.
- **Netmask:** The destination netmask address.
- **Gateway/Interface**: IP address of the gateway or existing interface that this route uses.
- **Cost:** The cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.
- **Interface:** Select the interface through which packets are forwarded.

## 3.6.1.3 DHCP Table

### DHCP Table

**Leased Table**

| IP Address | MAC Address | Client Host Name | Register Time |
|------------|-------------|------------------|---------------|
| 192.168.1.100 | 00:e0:18:df:7b:64 | Tolomeo | 2005/06/16 10:32:31 - 2005/06/16 22:32:31 |

- **Leased:** DHCP assigned IP addresses information.
- **IP Address:** IP addresses of devices on your LAN (Local Area Network).
- **MAC Address:** The MAC Address that you want to assign the fixed IP address
- **Client Host Name:** Expired IP addresses information
- **Register Time:** Register time information

## 3.6.1.4 System Log

Display the system logs cumulated till the present time. You can trace the historical information through this function.

**System Log**

**Current Time:Wed Jun 8 16:08:14 2005**

If you would like to save the log to a text file, right click here and select "Save Target As ..."

```
1502,AAL 5)
Jan  1 00:01:07 syslog: atm init aal5
Jan  1 00:01:11 syslog: get mac 00 04 ED FF F6 2F
Jun  8 15:23:54 NTP current time is Wed Jun  8 15:23:54 2005
Jun  8 15:45:36 DNS RELAY: reading /etc/resolv.conf
Jun  8 15:45:36 DNS RELAY: using nameserver 193.70.152.25#53
Jun  8 15:45:36 DNS RELAY: using nameserver 193.70.152.15#53
Jun  8 16:02:48 syslog: TC3162 nor-flash: waiting for chip to read, state = 4
Jun  8 16:06:03 syslog: TC3162 nor-flash: waiting for chip to read, state = 4
```

Refresh    Clear

## 3.6.1.5 Security Log

Display the information of security logs. If hacker attacks your sever, he will be isolated by the firewall function and the router will record related information. Hence, you know where the hacker comes from.

**Security Log**

**Current Time:Wed Jun 8 16:09:05 2005**

If you would like to save the log to a text file, right click here and select "Save Target As ..."

```
Jun  8 15:48:20 Block Wan: DROP ICMP packet from [ppp0] 219.151.40.36 to
151.38.129.212
Jun  8 16:03:10 Packet Filter: DROP ICMP packet from [br0] 192.168.1.187 to
192.168.7.1
Jun  8 16:03:15 Packet Filter: DROP ICMP packet from [br0] 192.168.1.187 to
192.168.7.1
Jun  8 16:03:20 Packet Filter: DROP ICMP packet from [br0] 192.168.1.187 to
192.168.7.1
Jun  8 16:03:25 Packet Filter: DROP ICMP packet from [br0] 192.168.1.187 to
```

Refresh    Clear

# 3.6.2 Quick Start Guide

For detailed instructions on configuring WAN settings, see the WAN section of this manual. The information you need for the Quick Start wizard to get you online are your login (often in the form of username@ispname), your password, and the encapsulation type.
**Your ISP can supply all the details you need.** Alternatively, if you have deleted the current WAN Connection in the WAN – ISP section of the interface, you can use the router's PVC Scan feature to determine the Encapsulation types offered by your ISP.



**Connection**
**Encapsulation:** Select the encapsulation type your ISP uses or choose "**Auto Scan**".



Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful, you are presented with a list of supported options.
- **VCI:** Enter the VCI assigned to you. This field may already be configured.
- **VPI:** Enter the VPI assigned to you. This field may already be configured.

- **NAT:** Select "**Enabled**".

**Optional Setting**
- **IP Address:** Type your ISP assigned IP address in the IP Address text box.
- **Subnet Mask:** Enter a subnet mask in dotted decimal notation.
- **Default Gateway:** You must specify a gateway IP address (supplied by your ISP)

**DNS**
- **Obtain DNS automatically:** Select this check box to use DNS.
- **Primary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
- **Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

**PPP**
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is usually 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).

Press **Apply** and then click on **Save Config.**

# 3.6.3 CONFIGURATION

When you click this item, you get following sub-items to configure WebShare 242W Wireless :

- **LAN**
- **WAN**
- **System**
- **Firewall**
- **QoS**
- **Virtual Server**
- **Advanced**

# 3.6.3.1 LAN

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

There are 2 items within the LAN section: **Ethernet** and **DHCP Server.**

## 3.6.3.1.1 Ethernet



The router supports two Ethernet IP addresses in the LAN, and two different LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN, so there is no need to configure a Secondary IP address. The default IP address for the router is 192.168.1.254.

**RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

The Subnet mask of the Secondary IP Address depends on the setting of the Primary IP Address.

## 3.6.3.1.2 Wireless

**Wireless**

**Parameters**

| | |
|---|---|
| WLAN service | ⦿ Enable   ○ Disable |
| Mode | 802.11b+g ▾ |
| ESSID | wlan_ap |
| Regulation Domain | N.America ▾ |
| Channel ID | Channel 1 (2.412 GHz) ▾ |
| MAC Address | 00:11:09:0d:96:2d |
| AP Version | IPN2220AP Ver:1.45.10.2004 |

**Wireless Distribution System (WDS)**

| | |
|---|---|
| WDS Service | ○ Enable  ⦿ Disable |
| Peer WDS MAC Address | |

[Apply]  [Cancel]

- **Mode:** 802.11b + g (Mixed mode), 802.11b and 802.11g. The factory default is 802.11b + g.
- **ESSID:** Enter the unique ID given to the Access Point (AP), which is already built-in to the router's wireless interface. To connect to this device, your wireless clients must have the same ESSID as the device.
- **Regulation Domain:** There are five 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 ID:** Select the ID channel that you would like to use.
- **MAC Address**: The AP's MAC Address
- **AP Version:** The Access Point firmware version.
- **WDS Service:**

  WDS (Wireless Distribution System) uses wireless media to communicate with other APs. It is able to extend the effective range and coverage of the wireless network. Please make sure the SSID is the same as that AP you want to extend. Wireless LAN is Half Duplex, so one transaction pass-through 2 wireless its real data-rate will be half of normal one. In figure an example of configuration.
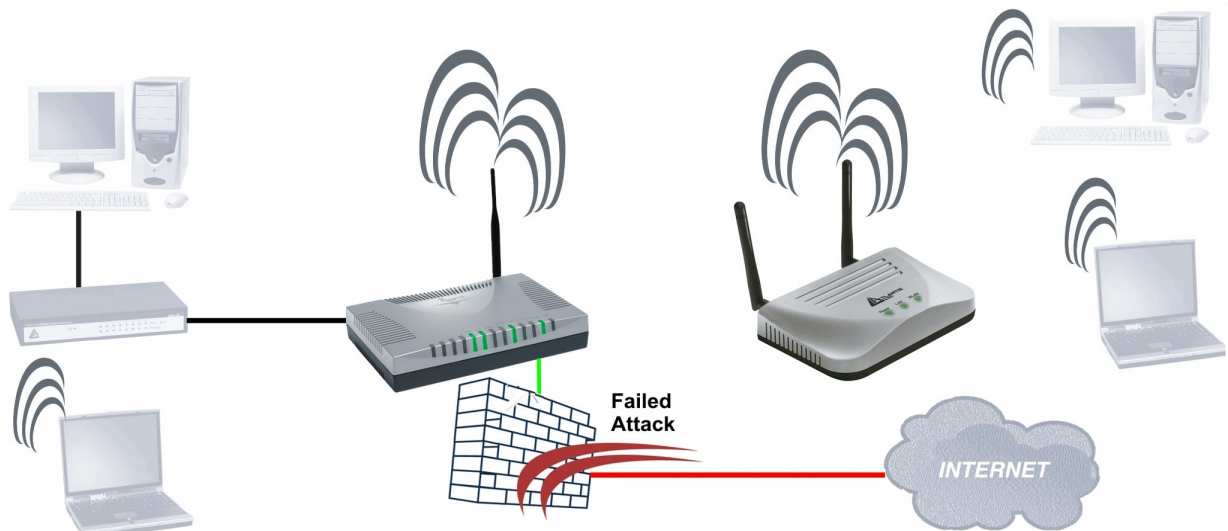
You must make sure that the SSID, Encryption and Channel is set the same as that AP you wish to connect. When WDS is enable only WEP ecryption is supported.

The range of radio frequencies used by IEEE 802.11b wireless devices is called a "channel". Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

Please use A02-AP-W54 toextende wireless coverage.

### 3.6.3.1.3 Wireless Security
You can disable or enable with WPA or WEP for protecting wireless network.
The default mode of wireless security is **disabled**.

**WPA Pre-Shared Key:**



- **WPA Algorithms:** TKIP (Temporal Key Integrity Protocol) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.
- **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).
- **Hide ESSID:** User can select Enable or Disable to hide ESSID.

**WEP:**
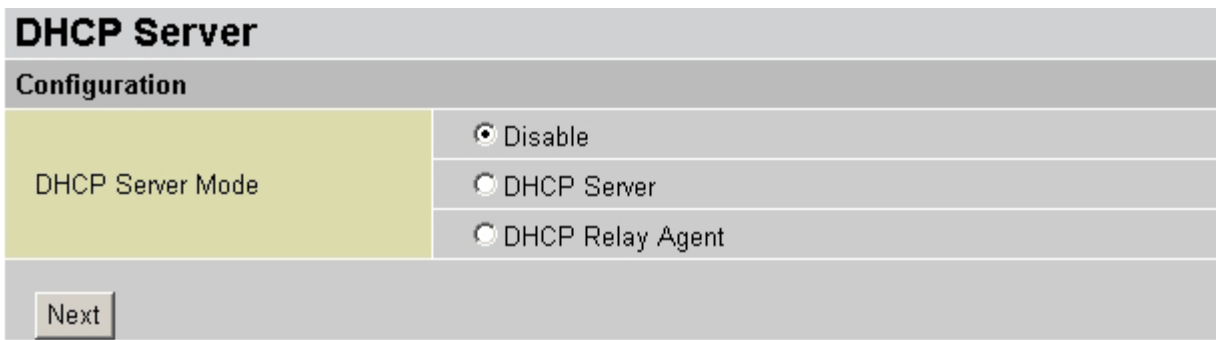


- **WEP Encryption:** To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.
- **Passphrase:** 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..

- **Key (1-4):** Enter the key to encrypt wireless data. 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 style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

- **Hide ESSID:** User can select Enable or Disable to hide ESSID.

## 3.6.3.1.4 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 |

[Next]

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

**DHCP**

**Disable server and relay agent**

The DHCP server and relay agent will be disabled.

[Apply] [Cancel]

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 performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).

## DHCP SERVER

### Parameters

| | |
|---|---|
| Domain Name | home.gateway |
| Use Router as DNS Server | ☑ |
| Primary DNS Server Address | 192.168.1.251 |
| Secondary DNS Server Address | |
| Default Lease Time | 43200    seconds |
| Maximum Lease Time | 86400    seconds |
| Range Start | 192.168.1.100 |
| Range End | 192.168.1.199 |

If you check **DHCP Relay Agent** and click **Next** then you must enter the IP address of the DHCP server which assigns 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. Click **Apply** to enable this function.

## DHCP Relay

### Parameters

| | |
|---|---|
| DHCP Relay Server | |

Apply   Cancel

# 3.6.3.2 WAN

Before you start installing this device, you have to check with your ISP what kind of service (connection method) is provided such as PPPoE, PPPoA, RFC1483 bridged or routed, IPoA. Gather the information as illustrated in the following table and keep it for reference.

| PPPoE | VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed). |
|---|---|
| PPPoA | VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned from ISP or be set fixed). |
| RFC1483 Bridged | VPI/VCI, VC-based/LLC-based multiplexing |
| RFC1483 Routed | VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address). |
| IPoA | VPI/VCI, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address). |

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are three items within the **WAN** section: **ISP**, **DNS** and **ADSL.**

## 3.6.3.2.1 ISP

The factory default is PPPoE. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

A simpler alternative is to select **Quick Start** from the main menu on the left. See the Quick Start section of the manual for more information.

**ISP**

Please select the type of service you wish to create

| ATM | RFC 1483 Routed | RFC 1483 Bridged |
|---|---|---|
| | PPPoA Routed | |
| | PPPoE Routed | Quick Start ▶ |

Next

Click **Next** in order to finish the configuration.

## PPPoE(RFC 2516) or PPPoA(RFC 2364)

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

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the information provided by your ISP.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **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 **20** alphanumeric characters.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Authentication Protocol:** Default is **Chap.** Your ISP advises on using **Chap** or **Pap.**
- **Connection:**
    - **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

- **Connect to Demand(PPPoE only):** If you want to establish a PPPoE 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.
- **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface. Please use: 1492(PPPoE), 1500(PPPoA).

## RFC 1483 Routing

**WAN Connection**

**RFC 1483 Routed**

| | |
|---|---|
| Description | 1483_Routed_mode |
| VPI | 8 |
| VCI | 35 |
| NAT | ⦿ Enable ○ Disable |
| Encapsulation Method | LLC Routed ▼ |
| IP Assignment | ○ Obtain an IP address automatically via DHCP client |
| | ⦿ Use the following IP address |
| | IP Address |
| | Netmask |
| | Gateway |
| RIP | No RIP ▼ |

[ Apply ] [ Cancel ]

- **Description:** Your description of this connection.
- **VPI and VCI:** Enter the information provided by your ISP.
- **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.
- **Encapsulation method:** Select the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.
- **DHCP client:** Enable or disable the DHCP client, specify if the router can get an IP address from the Internet Service Provider (ISP) automatically or not.
- **Obtain an IP address automatically via DHCP client** to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.
- **RIP:** RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

## BRIDGE (PPPoE)

**WAN Connection**

**RFC 1483 Bridged**

| | |
|---|---|
| Description | 1483_Bridged_mode |
| VPI | 8 |
| VCI | 35 |
| Encapsulation Method | LLC Bridged ▼ |

Apply   Cancel

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the information provided by your ISP.
- **Encapsulation method:** Select the encapsulation format, this is provided by your ISP.

### 3.6.3.2.2 DNS

**DNS**

**Parameters**

| | |
|---|---|
| Obtain DNS Automatically | ☑ Enable |
| Primary DNS | |
| Secondary DNS | |

Apply   Cancel

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.yahoo.com and an IP address. An IP address is a 32-bit number in the form of *xxx.xxx.xxx.xxx*, for example 192.168.1.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS allows you to find the telephone number for any particular domain name. Since an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP provides the DNS IP address automatically. You may leave the configuration field blank. Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address.

⚠ If you choose one of the other protocols, RFC1483 Routed or Bridged, check with your ISP, as it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS Server address on your PC to the LAN IP address of this router.

## 3.6.3.2.3 ADSL

**ADSL**

**Parameters**

| | |
|---|---|
| Connect Mode | ADSL ▼ |
| DSP FirmwareVersion | DMT FwVer: 3.1.0.0_A_TC, HwVer:T14F7_0.0 |
| DMT Status | Up |
| Operational Mode | ADSL G.Dmt |
| Annex Type | AnnexA |
| Upstream | 320 kbps |
| Downstream | 1504 kbps |

Apply    Cancel

- **ADSL Mode:** There are four modes "**Annex A**","**Annex L**","**Annex M**","**Annex J**", that user can select for this connection.
- **Modulator:** There are four modes "**AUTO**","**ADSL multimode**","**ADSL2**"and"**ADSL2+**" that user can select for this connection.
- **DSP Firmware Version:** DSP code version
- **DMT Status:** DMT Status
- **Operational Mode:** To show the state when user select "AUTO" on connect mode.
- **Annex Type:** To show the router's type, e.g. Annex A, Annex B
- **Upstream:** Upstream rate
- **Downstream:** Downstream rate

## 3.6.3.3 System

There are six items within the **System** section: **Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart** and **User Management.**

### 3.6.3.3.1 Time Zone



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 retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

**Resync Period** (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. 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.

### 3.6.3.3.2 Remote Access

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router permits 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.
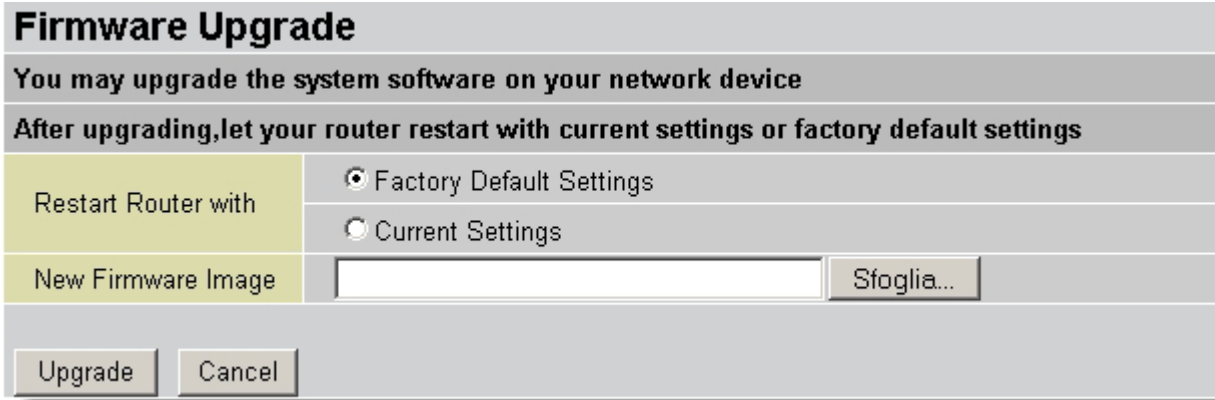
### 3.6.3.3.3 Firmware

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 modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows 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.

**Firmware Upgrade**

You may upgrade the system software on your network device

After upgrading,let your router restart with current settings or factory default settings

| Restart Router with | ⊙ Factory Default Settings |
| | ○ Current Settings |
| New Firmware Image | [                    ] Sfoglia... |

Upgrade | Cancel

**New Firmware Image:** Type in the location of the file you wish to upload in this field or click **Browse ...** to find it.

**Browse...:** Click **Browse...** to find the .ras file you wish to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

**Upgrade**: Click **upgrade** to begin the upload process. This process may take up to two minutes.

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

### 3.6.3.3.4 Backup/Restore

**Backup/Restore**

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

**Backup Configuration**

Backup configuration to your computer.

[ Backup ]

**Restore Configuration**

Configuration File [                    ] [ Sfoglia... ]

*"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.*

[ 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.

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.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

**Config Restore Progress**

Do NOT switch off modem during flash update

| Restore Progress | Status: | |
|---|---|---|
| | Total: [ ] | - 11% |

### 3.6.3.3.5 Restart

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

**Restart**

| After restarting. Please wait for several seconds to let the system | |
|---|---|
| Restart Router with | ○ Save Config to Flash<br>⊙ Current Settings<br>○ Factory Default Settings |

[Restart] [Cancel]

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 pressing in the small Reset pinhole button on the back of your router for 10-12 seconds while the router is turned on. You have to Switch Off and Switch On the device that boot with factory default settings.

### 3.6.3.3.6 User Management

**User Management**

| Current Defined Users | | | |
|---|---|---|---|
| Valid | User | | |
| true | *admin* | Edit ▶ | |

Create ▶

To prevent unauthorized access to your router's configuration interface, all users are required 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 **Create** 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**

| Edit | |
|---|---|
| Username | **admin** |
| Password | ••••• |
| Valid | true |

[Apply] [Cancel]

You can change the user's **password**, whether their account is active and **Valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking **Cancel** 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.

# 3.6.3.4 Firewall

Your router includes a full DoS firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation. Please see the **WAN** configuration section for more details on 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.

**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 are 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.

**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.

**MAC Filter rules**: To prevent unauthorized computers accessing the Internet.

**URL Filter:** To block PCs on your local network from unwanted websites.

You can find 10 items under the Firewall section: General Settings, Packet Filter, Intrusion Detection, MAC Address Filter, URL Filter (up to 30 rules)  and Firewall Log.

You can choose not to enable Firewall, to add all filter rules by yourself, or enable the Firewall using preset filter rules and modify the port filter rules as required.

## 3.6.3.4.1 Packet Filering

User can decide to enable this firewall function including Packet Filter, Block Hacker Attack, and Block WAN request features for better security control or not. But be noted, it wastes network processor computation power. The performance will be lower about 10% to 15%. More firewall features will be added continually, please visit our web site to download latest firmware.

Packet filtering function enables you to configure your router to check specified internal/external user (IP address) from Internet access, or you can disable specific service request (Port number) to /from Internet. This configuration program allows you to set up different filter rules up to 10 for different users based on their IP addresses or their network Port number. The relationship among all filters is "or" operation, which means the device checks these different filter rules one by one, stating from the first rule.

As long as one of the rules is satisfied, the specified action will be taken. remote server using the port number.

## Packet Filter

**Default Rules** Forward ▼

**Parameters**

| Rule No. | Active | Flow | Packet Type | Action | Source IP | | Source Port | | Destination IP | | Dest. Port | | Log | Schedule Time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | from | to | from | to | from | to | from | to | | |

Add  Edit  Delete

Apply  Cancel

## Packet Filter

**Application List**

| Application | User Defined ▼ | ☐ Reverse Direction |
|---|---|---|

**Parameters**

| Rule number | 1 | Packet Flow | ● Outgoing  ○ Incoming |
|---|---|---|---|
| Active | Yes ▼ | Packet Type | Any ▼ |
| Log | Yes ▼ | Action When Matched | Drop ▼ |

**Source IP Address** / **Destination IP Address**

| from | | from | |
|---|---|---|---|
| to | | to | |

**Source Port** / **Destination Port**

| from | | from | |
|---|---|---|---|
| to | | to | |

| Schedule Time | ● Always |
|---|---|
| | ○ Schedule from   08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ |
| | ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat |

Return  Cancel

Packet filtering function enables you to configure your router to check specified internal/external user (IP address) from Internet access, or you can disable specific service request (Port number) to /from Internet. This configuration program allows you to set up different filter rules up to 10 for different users based on their IP addresses or their network Port number. The relationship among all filters is "or" operation, which means the device checks these different filter rules one by one, stating from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

- **Add:** Click this button to add a new packet filter rule. After click, next figure will appear.
- **Edit:** Check the Rule No. you want to edit. Then, click the "Edit" button.
- **Delete:** Check the Rule No. you want to delete. Then, click the "Delete" button.
- **Outgoing / Incoming:** Determine whether the rule is for outgoing packets or for incoming packets.
- **Active:** Choose "Yes" to enable the rule, or choose "No" to disable the rule.

- **Packet Type:** Specify the packet type (TCP, UDP, ICMP or any) that the rule will be applied to.Select TCP if you want to scope for the connection-based application service on the remote server using the port number. Or select UDP if you want to scope for the connectionless application service on the remote server using the port number.
- **Log:** Choose "Yes" if you want to generate logs when the filer rule is applied to a packet.
- **Action When Matched:** If any packet matches this filter rule, Forward or Drop this packet.
- **Source IP Address:** Enter the incoming or outgoing packet's source IP address(es).
- **Source Port:** Check the TCP or UDP packet's source port number(s).
- **Destination IP Address**: Enter the incoming or outgoing packet's destination IP address(es).
- **Destination Port:** Check the TCP or UDP packet's destination port number(s).

**E.G.**

## Packet Filter

Default Rules [Drop ▼]

Parameters

| Rule No. | Active | Flow | Packet Type | Action | Source IP | | Source Port | | Destination IP | | Dest. Port | | Log | Schedule Time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | from | to | from | to | from | to | from | to | | |

[Add] [Edit] [Delete]

[Apply] [Cancel]

**http(OutGoing/Ingoing):**

## Packet Filter

### Application List

| Application | HTTP Client (port 80) ▾ | ☑ Reverse Direction |
|---|---|---|

### Parameters

| Rule number | 8 | Packet Flow | ⦿ Outgoing ○ Incoming |
|---|---|---|---|
| Active | Yes ▾ | Packet Type | Tcp ▾ |
| Log | Yes ▾ | Action When Matched | Forward ▾ |

### Source IP Address | | ### Destination IP Address

| Source IP Address | | Destination IP Address | |
|---|---|---|---|
| from | | from | |
| to | | to | |

### Source Port | | ### Destination Port

| Source Port | | Destination Port | |
|---|---|---|---|
| from | | from | 80 |
| to | | to | 80 |

| Schedule Time | ⦿ Always |
|---|---|
| | ○ Schedule from 08 ▾ : 00 ▾ to 18 ▾ : 00 ▾ |
| | ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat |

Return  Cancel

**POP3 (OutGoing/Ingoing):**

## Packet Filter

### Application List

| Application | POP3 Client (port 110) ▼ | ☑ Reverse Direction |
|---|---|---|

### Parameters

| Rule number | 8 | Packet Flow | ◉ Outgoing    ○ Incoming |
|---|---|---|---|
| Active | Yes ▼ | Packet Type | Tcp ▼ |
| Log | Yes ▼ | Action When Matched | Forward ▼ |

| Source IP Address | | Destination IP Address | |
|---|---|---|---|
| from | | from | |
| to | | to | |

| Source Port | | Destination Port | |
|---|---|---|---|
| from | | from | 110 |
| to | | to | 110 |

| Schedule Time | ◉ Always | | |
|---|---|---|---|
| | ○ Schedule from | 08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ | |
| | ☐ Sun  ☐ Mon  ☐ Tue  ☐ Wed  ☐ Thu  ☐ Fri  ☐ Sat | | |

| Return | Cancel |
|---|---|

## SMTP (OutGoing/Ingoing):

### Packet Filter

**Application List**

| Application | SMTP Client (port 25) ▼ | ☑ Reverse Direction |
|---|---|---|

**Parameters**

| Rule number | 8 | Packet Flow | ⦿ Outgoing ○ Incoming |
|---|---|---|---|
| Active | Yes ▼ | Packet Type | Tcp ▼ |
| Log | Yes ▼ | Action When Matched | Forward ▼ |

**Source IP Address** | | **Destination IP Address** |
| from | | from | |
| to | | to | |

**Source Port** | | **Destination Port** |
| from | | from | 25 |
| to | | to | 25 |

| Schedule Time | ⦿ Always |
|---|---|
| | ○ Schedule from   08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ |
| | ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat |

[Return] [Cancel]

45

## FTP (OutGoing/Ingoing)::

### Packet Filter

**Application List**

| Application | FTP Client (port 21) ▼ | ☑ Reverse Direction |
|---|---|---|

**Parameters**

| Rule number | 8 | Packet Flow | ⦿ Outgoing  ○ Incoming |
|---|---|---|---|
| Active | Yes ▼ | Packet Type | Tcp ▼ |
| Log | Yes ▼ | Action When Matched | Forward ▼ |

| **Source IP Address** | | **Destination IP Address** | |
|---|---|---|---|
| from | | from | |
| to | | to | |

| **Source Port** | | **Destination Port** | |
|---|---|---|---|
| from | | from | 20 |
| to | | to | 21 |

| Schedule Time | ⦿ Always |
|---|---|
| | ○ Schedule from  08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ |
| | ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat |

Return   Cancel

**DNS (OutGoing/Ingoing):**

## Packet Filter

**Application List**

| Application | DNS Client (port 53) ▼ | ☑ Reverse Direction |
|---|---|---|

**Parameters**

| Rule number | 8 | Packet Flow | ⦿ Outgoing ○ Incoming |
|---|---|---|---|
| Active | Yes ▼ | Packet Type | Udp ▼ |
| Log | Yes ▼ | Action When Matched | Forward ▼ |

| **Source IP Address** | | **Destination IP Address** | |
|---|---|---|---|
| from | | from | |
| to | | to | |

| **Source Port** | | **Destination Port** | |
|---|---|---|---|
| from | | from | 53 |
| to | | to | 53 |

| Schedule Time | ⦿ Always |
|---|---|
| | ○ Schedule from  08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ |
| | ☐ Sun  ☐ Mon  ☐ Tue  ☐ Wed  ☐ Thu  ☐ Fri  ☐ Sat |

Return   Cancel

## 3.6.3.4.2 MAC address Filtering

MAC filtering function enables you to configure your ADSL Firewall Router to block internal user (**MAC address**) from Internet access.

## MAC Address Filter

**Default Rules** Forward ▼

**Parameters**

| | Rule No. | Active | Action | Log | MAC Address |
|---|---|---|---|---|---|
| Add  Edit  Delete | | | | | |

Apply   Cancel

If you check **Enable,** remember to choosea defaulkt rules policy between **Forward** or **Drop**. If you select **Forward** , the packet with the MAC address in the table(**Drop**) will be dropped and others will be forwarded. If you select **Drop**, the packet with the MAC address in the table (**Forward**) will be forwarded and others will be dropped. Then select **Apply** button to save the setting.

## MAC Filter

**Parameters**

| Rule 2 | |
|---|---|
| Active | Yes ▾ |
| Action When Matched | Drop ▾ |
| Log | Yes ▾ |
| Mac Address | |

Return   Cancel

- **Active:** Select **Yes** from the drop down list box to enable MAC address filtering.
- **Action When Matched:** Select "Drop" or "Forward".
- **Log:** Choose "Yes" if you wish to generate logs when the filer rule is applied to a packet.
- **MAC Address:** Enter the MAC addresses you wish to manage.

### 3.6.3.4.3 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.

Hacker attack types recognized by the IDS:

- IP Spoofing
- Ping of Death (Length > 65535)
- Land Attack (Same source / destination IP address)
- IP with zero length
- Sync flooding
- Smurf Attack (ICMP Echo with x.x.x.0 or x.x.x.255)
- Snork Attack
- UDP port loop-back
- TCP NULL scan

## Intrusion Detection

**Parameters**

| Intrusion Detection | ⦿ Enable ○ Disable |
|---|---|
| Alert Mail | ☐ |
| Alert Mail Time | 30                          minutes |
| Your E-mail(Must be xxx@yyy.zzz) | |
| Recipient's E-mail(Must be xxx@yyy.zzz) | |
| SMTP server | |

Apply   Cancel

- **Intrusion Detection:** Check "Enable" if you wish to detect intruders accessing your computer without permission.
- **Alert Mail:** Select this check box to use Alert Mail.

- **Alert Mail Time:** Set the time for receiving Alert mail.
- **Your E-Mail:** Set your email address.
- **Recipient's E-mail:** Set the Recipient's email address to which the E-<mail notification is sent.
- **SMTP server:** Set the SMTP (mail) server address.

## 3.6.3.4.4 Block Wan Request

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.

**Block WAN Request**

| Parameters | |
|---|---|
| Block WAN Request | ○ Enable ◉ Disable |

Submit | Cancel

## 3.6.3.4.5 URL Blocking

URL filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no predefined URL filter rules; you can add filter rules to meet your requirements.

**URL Filter**

| Rule No. | Active | PC IPs from | to | Block Mode | Keywords Filtering | Domains Filtering | Restrict URL Features |
|---|---|---|---|---|---|---|---|

Add | Edit | Delete

Apply | Cancel

## URL Filter

**Parameters**

| Rule 1 | Active | Yes ▼ |
|---|---|---|

**PC IP Address Range**

| From | | | To | |
|---|---|---|---|---|

| Block Mode | ● Always Block | |
|---|---|---|
| | ○ Block from | 08 ▼ : 00 ▼ to 18 ▼ : 00 ▼ |
| | ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat | |

| Keywords Filtering | ☐ Enable [Details] |
|---|---|
| Domains Filtering | ☐ Enable [Details] |

| Restrict URL Features | ☐ Block Java Applet |
|---|---|
| | ☐ Block ActiveX |
| | ☐ Block Cookies |
| | ☐ Block Proxy |

[Return] [Cancel]

**From/To:** IP Address

**Block Mode:** You can select when Router have yo use thess settings

**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.

For example, if the URL is http://www.atlantis-land.com/start.html, it will be dropped as the keyword "start" occurs in the URL.

**Domains Filtering:**

This function checks the domain name 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). The checking procedure is:

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, and if present then the connection attempt is 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 domain only should be specified, not the full URL. For example to block traffic to www.sex.com, enter "sex" or "sex.com" instead of "www.sex.com". In the example below, the URL request for www.helloworld.com.tw will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.sex or www.sex.com will be dropped, because helloworld.com is in the forbidden list.

**Restrict URL Features**

- Block Java Applet: Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- Block ActiveX: Blocks ActiveX
- Block Cookies: Blocks Cookies
- Block Proxy: Blocks Proxy

# 3.6.3.5 QoS
## Quality of Service Introduction

If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in routers is such a breakthrough for home users and office users.

### QOS: Keeping Your Net Connection Fast and Responsive

Configurable by source IP address, destination IP address, protocol, and port, the Quality of Service (QOS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

## QOS Setup

Please choose the **QOS** in the **Configuration** item of the left window as depicted below.



After clicking the QOS item, you can Add/Edit/Delete a QOS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

## QoS

**Maximum ISP Bandwidth**

Type: Manual Input

Upstream(LAN->WAN): 256 Kbps

Downstream(WAN->LAN): 1024 Kbps

**QoS Rule List**

| | Application | Time Schedule | Direction | Assigned Bandwidth Ratio |
|---|---|---|---|---|
| ○ | VoIP | Always On | LAN to WAN | 20% (46kbps) Minimum Guaranteed Rate with High priority |
| ○ | FTP_Server_Out | Day Time | LAN to WAN | 30% (69kbps) Minimum Guaranteed Rate with Low priority |
| ○ | FTP_Server_IN | Day Time | WAN to LAN | 30% (261kbps) Minimum Guaranteed Rate with Low priority |
| ○ | HTTP_Out | Always On | LAN to WAN | 20% (46kbps) Fixed Rate |
| ◉ | HTTP_IN | Always On | WAN to LAN | 30% (261kbps) Fixed Rate |

**Non-Assigned Bandwidth Ratio**

| LAN to WAN : **30%** | WAN to LAN : **40%** |
|---|---|

Add | Edit | Delete

Apply | Cancel

● **Application**: A name that identifies an existing policy.

● **Time Schedule**: Scheduling your QOS policy to be applied.

● **Direction**: The traffic flow direction to be controlled by the QOS policy.

There are two settings to be provided in the Router:

⊙ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. E.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QOS policy. So, you need to add a policy with LAN to WAN direction setting.

⊙ **LAN to WAN**: Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

● **Assigned Bandwidth Ratio**: This field shows the assigned bandwidth ratio in percentage for a QOS policy. If WAN connection to internet is established, the estimated transfer rate will be shown in kbps. You may specify a fixed transfer rate or Minimum Guaranteed Rate with priority for non-used bandwidth.

**Non-Assigned Bandwidth Ratio**: This field shows the available bandwidth ratio, for LAN to WAN and WAN to LAN, that has not yet assigned.

Add : Press this button to add a new QOS policy.

Edit Delete : Before using these buttons to edit or delete a policy, please select one policy you want to edit/delete from the radio option ⭕ VoIP .

Apply : After you have configured the policies, you can press this button to apply the configuration. If you want to make the change persistent in flash, choose Save Config to Flash in the left windows to save it into flash.

When you press Add or Edit buttons described above, the following page will show up in your browser. You can use it to define a QOS policy.

## QoS

### Parameters

| | |
|---|---|
| Controlled Traffic Flow | ◉ LAN to WAN ◯ WAN to LAN |
| Application | APPL1 |
| Packet Type | ANY ▾ |
| Assigned Data Rate | Rate Type: Fixed (Maximum) ▾    Data Ratio: [ ] %    Priority for Non-used Bandwidth: Normal ▾ |
| DSCP Marking (LAN to WAN only) | Disabled ▾ |
| Local Machine IPs | From [ ] To [ ] |
| Remote Machine IPs | From [ ] To [ ] |
| Local Application Ports | From [ ] To [ ] |
| Remote Application Ports | From [ ] To [ ] |
| Schedule Time | ◉ Always<br>◯ Schedule from   08 ▾ : 00 ▾ to 18 ▾ : 00 ▾<br>☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat |

Return Cancel

🔘 **Controlled Traffic Flow:** Specify the traffic flow you want to control. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

🔘 **Packet type**: The packet type will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

◉ **ANY:** No specified protocol type is specified.

◉ **TCP**

◉ **UDP**

◉ **ICMP**

⊙ **GRE:** For PPTP VPN Connections.

🔘 **Assigned Data rate:** Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for a ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

🔘 **Data Ratio**: percentage for the data rate to be controlled by this policy. As above FTP server examples, it is 20.

🔘 **Rate Type**: We provide 2 types here:.

⊙ **Fixed (Maximum):** specify a fixed data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to "throttle" the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

⊙ **Guaranteed (Minimum):** specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

🔘 **Priority for Non-used Bandwidth:** Specify the priority for the bandwidth that is not used. For examples, you may specify two different QOS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

⊙ **High**

⊙ **Normal**: The default is normal priority.

⊙ **Low**

For the sample priority assignment for different policies, it is seved in a First-In-First-Out way.

🔘 **DSCP Marking**: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

| DSCP Mapping Table | |
| --- | --- |
| 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) |

● **Local Machine IPs**: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

● **Remote Machine IPs**: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

● **Local Application Ports**: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

● **Remote Application Ports**: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

● **Schedule Time**: Schedule your QOS policy.

## ◼ QOS example for your Network
**Connection Diagram**



## ADSL Subscription Rate
Upstream: 256 kbps
Downstream: 1024 Mbps

## Example QOS Plan
:.

| Application | IP or Ports | Control Flow | Data Rate | Time Schedule |
|---|---|---|---|---|
| VoIP User | 192.168.1.1 | Outgoing | Minimal 20% with high priority for non-used bandwidth with SDCP marking Class 1 Gold Service | Always |
| FTP Sever | 192.168.1.100 | Incoming and Going | outgoing :minimal 30%. Data rate. incoming :minimal 30%. Data rate. Both with low priority for non-used bandwidth. | Only Working Hours 9:00 to 18:00 Monday to Friday. |
| HTTP web browsing users | 80 | Incoming and Going | outgoing : limited 20%. Data rate. incoming : limited 30%. Data rate. | Always |

## Example QOS Setup

### QoS

**Maximum ISP Bandwidth**

| Type: | Manual Input | Upstream(LAN->WAN): | Downstream(WAN->LAN): |
|---|---|---|---|
| | | 256 Kbps | 1024 Kbps |

**QoS Rule List**

| | Application | Time Schedule | Direction | Assigned Bandwidth Ratio |
|---|---|---|---|---|
| ○ | VoIP | Always On | LAN to WAN | 20% (46kbps) Minimum Guaranteed Rate with High priority |
| ○ | FTP_Server_Out | Day Time | LAN to WAN | 30% (69kbps) Minimum Guaranteed Rate with Low priority |
| ○ | FTP_Server_IN | Day Time | WAN to LAN | 30% (261kbps) Minimum Guaranteed Rate with Low priority |
| ○ | HTTP_Out | Always On | LAN to WAN | 20% (46kbps) Fixed Rate |
| ◉ | HTTP_IN | Always On | WAN to LAN | 30% (261kbps) Fixed Rate |

**Non-Assigned Bandwidth Ratio**

| LAN to WAN : **30%** | WAN to LAN : **40%** |
|---|---|

[Add] [Edit] [Delete]

[Apply] [Cancel]

**VoIP application**
Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.



Above settings will help to improve quality of your VoIP service when traffic is full loading.

## FTP Server Application
Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.
LAN to WAN direction:

### QoS

| Parameters | | | |
|---|---|---|---|
| Controlled Traffic Flow | ⊙ LAN to WAN ○ WAN to LAN | | |
| Application | FTP_Server_Out | | |
| Packet Type | TCP ▼ | | |
| Assigned Data Rate | Rate Type: Guaranteed (Minimum) ▼ | Data Ratio: 30 % | Priority for Non-used Bandwidth: Low ▼ |
| DSCP Marking (LAN to WAN only) | Disabled ▼ | | |
| Local Machine IPs | From 192.168.1.100 | To 192.168.1.100 | |
| Remote Machine IPs | From | To | |
| Local Application Ports | From | To | |
| Remote Application Ports | From | To | |
| Schedule Time | ○ Always | | |
| | ⊙ Schedule from | 09 ▼ : 00 ▼ to 18 ▼ : 00 ▼ | |
| | ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat | | |

Return   Cancel

WAN to LAN direction:

## QoS

### Parameters

| | |
|---|---|
| Controlled Traffic Flow | ○ LAN to WAN ● WAN to LAN |
| Application | FTP_Server_IN |
| Packet Type | TCP ▼ |
| Assigned Data Rate | Rate Type: Guaranteed (Minimum) ▼  Data Ratio: 30 %  Priority for Non-used Bandwidth: Low ▼ |
| DSCP Marking (LAN to WAN only) | Disabled ▼ |
| Local Machine IPs | From 192.168.1.100  To 192.168.1.100 |
| Remote Machine IPs | From  To |
| Local Application Ports | From  To |
| Remote Application Ports | From  To |
| Schedule Time | ○ Always ● Schedule from 09 ▼ : 00 ▼ to 18 ▼ : 00 ▼ □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat |

Return  Cancel

With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at day time.

**HTTP Web Browsing**
You can control the internet web browsing by specify the HTTP 80 (8080 for some proxy server).
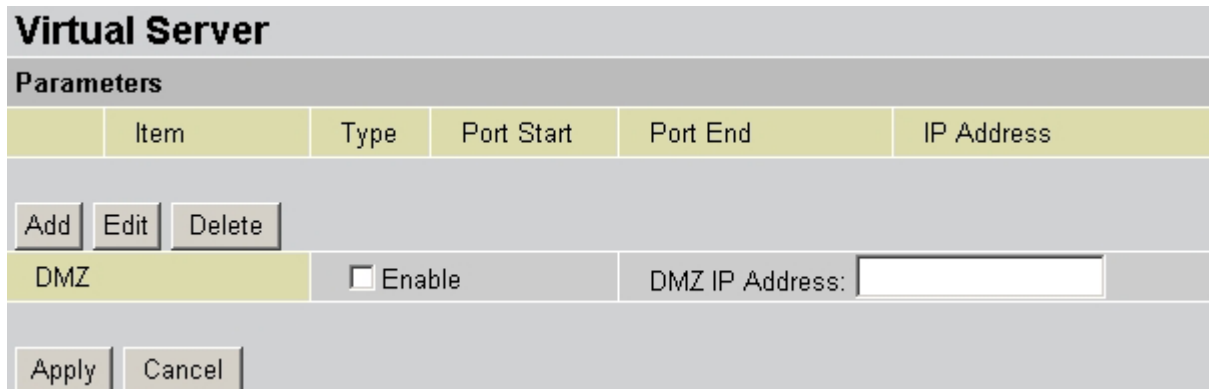
LAN to WAN direction:

**QoS**

| Parameters | |
|---|---|
| Controlled Traffic Flow | ⦿ LAN to WAN    ○ WAN to LAN |
| Application | HTTP_Out |
| Packet Type | TCP ▾ |
| Assigned Data Rate | Rate Type:     Data    Priority for Non-used Bandwidth:<br>Fixed (Maximum) ▾   Ratio: 20 %   Normal ▾ |
| DSCP Marking (LAN to WAN only) | Disabled ▾ |
| Local Machine IPs | From [ ]   To [ ] |
| Remote Machine IPs | From [ ]   To [ ] |
| Local Application Ports | From [ ]   To [ ] |
| Remote Application Ports | From 80   To 80 |
| Schedule Time | ⦿ Always<br>○ Schedule from     08 ▾ : 00 ▾ to 18 ▾ : 00 ▾<br>□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat |

Return   Cancel

WAN to LAN direction:

## QoS

### Parameters

| Controlled Traffic Flow | ○ LAN to WAN  ⊙ WAN to LAN | | |
|---|---|---|---|
| Application | HTTP_IN | | |
| Packet Type | ANY ▼ | | |
| Assigned Data Rate | Rate Type: Fixed (Maximum) ▼ | Data Ratio: 30 % | Priority for Non-used Bandwidth: Normal ▼ |
| DSCP Marking (LAN to WAN only) | Disabled ▼ | | |
| Local Machine IPs | From [ ] | To [ ] | |
| Remote Machine IPs | From [ ] | To [ ] | |
| Local Application Ports | From [ ] | To [ ] | |
| Remote Application Ports | From 80 | To 80 | |
| Schedule Time | ⊙ Always<br>○ Schedule from     08 ▼ : 00 ▼ to 18 ▼ : 00 ▼<br>☐ Sun  ☐ Mon  ☐ Tue  ☐ Wed  ☐ Thu  ☐ Fri  ☐ Sat | | |

[ Return ]  [ Cancel ]

## 3.6.3.6 Virtual Server

When you click Virtual Server, you get the following figure.



Being a natural Internet firewall, this network router protects your network from being accessed by outside users. When it needs to allow outside users to access internal servers, e.g. Web server, FTP server, E-mail server or News server, this modem can act as a virtual server. You can set up a local server with specific a port number that stands for the service, e.g. Web (80), FTP (21), Telnet (23), SMTP (25), POP3 (110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.

For example, if you set the Service Port number 80 (Web) to be mapped to the IP Address 192.168.1.2, then all the http requests from outside users will be forwarded to the local server with IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.



If you have disabled the NAT option in the WAN-ISP section, this 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 easy way is that the IP address assigned to each virtual server should 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 is still in the same subnet with the router.

| Application | OutBound | Inbound |
|---|---|---|
| ICQ 98, 99a | N/A | N/A |
| NetMeeting 2.1 a 3.01 | N/A | 1503 TCP, 1720 TCP |
| VDO Live | N/A | N/A |
| MIRC | N/A | N/A |
| 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 | N/A | 4660-4662 TCP , 4665 UDP |
| MSN Messanger | N/A | TCP da 6891-6900<br>TCP 1863<br>TCP 6901<br>UDP 1863, 6901 e 5190 |

| Services | 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 |

## 3.6.3.7 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.

- **Static Route**
- **Dynamic DNS**
- **VLAN Control**
- **Device Management**
- **IGMP**

## 3.6.3.7.1 Static Routed

Click on the **Static Routing** and then choose **Create IP V4Route** to get the below figure to add a routing table.



- **Destination:** Enter the destination subnet IP.
- **Gateway:** Enter the gateway IP address which the packet is forwarded to.
- **Netmask:** Subnet mask of destination IP addresses based on above destination subnet IP.
- **Cost:** This is the same meaning as Hop. Usually, leave it as 1.
- **Interface:** Enter the interface, which the packet is forwarded to.

**E.G.**





### 3.6.3.7.2 Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still 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.

Click **Dynamic DNS** to get the below figure then check the "**Enable**" button to access the Dynamic DNS service.

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 this free Web server http://www.dyndns.org/. There are more than 8 DDNS servers supported.

- **Dynamic DNS:** Select the registered DDNS server.
- **Domain Name, Username and Password:** Enter the registered domain name, username and password.
- **Period:** Set the time period for the Router to exchange information with the DDNS server. In addition to update periodically according to this period setting, the Router will take the same action automatically whenever the assigned IP changes.
- **Wildcard:** Select this check box to enable the DYNDNS Wildcard.

### 3.6.3.7.3 VLAN
VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



Select **Port Base** and after click on **Apply**.

## Vlan Control

**Parameters**

| Vlan | ⦿ Port Base ○ Disable | | | |
|---|---|---|---|---|
| Vlan Port Setting | P1 | P2 | P3 | P4 |
| vlan1 | ☐ | ☐ | ☐ | ☐ |
| vlan2 | ☐ | ☐ | ☐ | ☐ |
| vlan3 | ☐ | ☐ | ☐ | ☐ |
| vlan4 | ☐ | ☐ | ☐ | ☐ |

Apply   Cancel

Group individual ports into a small "Virtual" network of their own to be independent of the other ports. To add a VLAN group check on the port to be a member to this VLAN Group, and press *"Apply"* button to execute the setting.

### 3.6.3.7.4 Device Management

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

**Device Management:** Is possible to move the port number used for remote configuration of the router, is also possible to block access for a determined period of time and to a precise IP address (leaving instead 0,0,0,0 it is possible to configurare the Router from whichever IP). Is moreover possible Enable/Disable the function Universal Plug and Play and establish the door used for this service. Finally is possible to configure protocol SNMP.

## Device Management

**Embedded Web Server**

| * HTTP Port | 8081 | (80 is default HTTP port) |
|---|---|---|

**Universal Plug and Play (UPnP)**

| UPnP | ⦿ Enable   ○ Disable |
|---|---|
| * UPnP Port | 2800 |

**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 | | |

Apply   Cancel

**Embedded Web Server:**
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.
For Example: User A changes HTTP port number to 8081. The router will only allow User A access typing: http://192.168.1.254:8081 in their web browser.

**Universal Plug and Play (UPnP):**
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.
- 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.

**Simple Network Management Protocol:**
SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function)
SNMP V1 and V2:
- 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.
SNMP V3:
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.

**SNMP Version: SNMPv2c and SNMPv3**
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
- **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

## 3.6.3.7.5 IGMP

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The WebShare 242W Wireless supports both IGMP version 1 (IGMP-v1) and IGMP version 2 (IGMP-v2). At start up, the WebShare 242W Wireless queries all directly connected networks to gather group membership. After that, the WebShare 242W Wireless periodically updates this information. IP multicasting can be enabled/disabled on the ADSL Router LAN and/or WAN interfaces in the web configurator (LAN; WAN). Select None to disable IP multicasting on these interfaces.

**IGMP**

| Parameters | | |
|---|---|---|
| IGMP Proxy | ○ Enable | ◉ Disable |
| IGMP Snooping | ○ Enable | ◉ Disable |

Apply   Cancel

# 3.6.4 SAVE Config

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.

# Chapter 4
# Troubleshooting

If the Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save you time and effort but if the symptoms persist, then consult your service provider.

## Problems Starting Up the ADSL Router

| Problem | Corrective Action |
|---|---|
| None of the LEDs are on when you turn on the ADSL Router. | Check the connection between the adapter and the ADSL Router. If the error persists, you may have a hardware problem. In this case you should contact technical support. |

## Problems with the WAN Interface

| Problem | Corrective Action |
|---|---|
| Initialization of the PVC connection failed. | Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the ADSL Firewall Router should be on. Check with your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP. Reboot the WebShare 242W Wireless . If you still have problems, you may need to verify these variables with the telephone company and/or ISP. |

## Problems with the LAN Interface

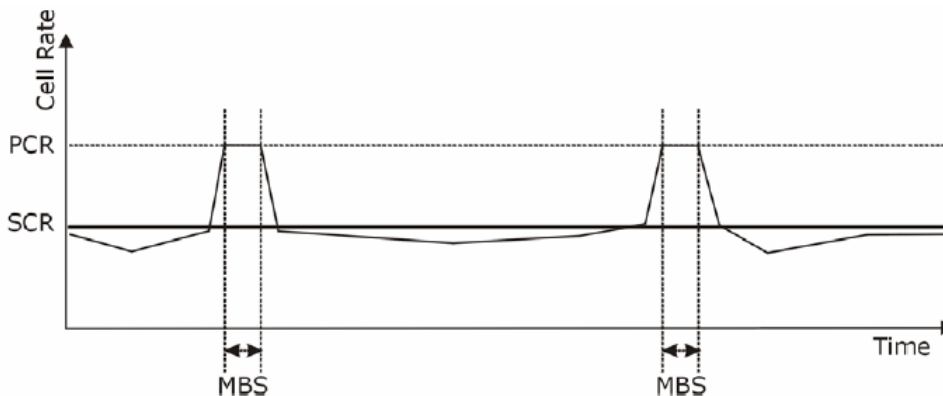| Problem | Corrective Action |
|---|---|
| Can't ping any station on the LAN. | Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your ADSL Router and the station. Make sure you have uninstalled any software firewall. |
| | Verify that the IP address and the subnet mask are consistent between the WebShare 242W Wireless and the workstations. |

# APPENDIX A

## Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and "burstiness" or fluctuation of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832 Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again. The following figure illustrates the relationship between PCR, SCR and MBS.

# APPENDIX B

## Technical Features

| | |
|---|---|
| **Protocols** | IP, NAT, ARP, ICMP, IGMP,  DHCP(server, client and relay), RIP1/2 , SNTP client, UPnP, Telnet server, SNMP |
| **LAN port** | 4 x RJ45 10/100 Base-T ports |
| **WAN port** | RJ-11 (1 port ADSL) |
| **Antenna** | 1*5dBi Antenna (R-SMA) |
| **External buttons** | Reset/Power Button |
| **LED Indicators** | Power, System, WLAN, 4 X Lan,  ADSL and PPP |
| **Wireless** | IEEE802.11g/IEEE802.11b (WDS) |
| **Standard ADSL Compliance** | ANSI T1.413 Issue 2, ITU-T G.992.1(Full Rate DMT), ITU-T G.992.2 (Lite DMT), ITU-T G.994.1 (Multimode), ITU G.992.3 (G.dmt.bis), ITU G.992.5 (G.dmt.bisplus) |
| **Protocols ADSL** | RFC2364(PPPoA), RFC2516(PPPoE) and RFC1483 |
| **ATM** | ATM AAL2/AAL5 and ATM service class : CBR, UBR, VBR-rt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0 |
| **Firewall** | Static Packet Filtering, URL Filtering, MAC Filtering and NAT |
| **VLAN** | Per Port VLAN |
| **QoS** | **QoS:** The Prioritization functions allow you to specify which packets have priority and should not be delayed, and/or which packets have low priority and should be moved to the end of upload queues. **IP Throttling:** Using IP Throttling, bandwidth limits can be enforced on any system within your LAN, or even on a  particular application |
| **VPN** | Pass Through |
| **Input Power** | 12V DC @ 1A |
| **Power Consumption** | < 9watts |
| **Agency and Regulatory** | CE |
| **Dimensions** | 175 x 129 x 39 mm3 |
| **Weight** | 350g |
| **Operating Temperature** | 0° to 40°C |
| **Storage Temperature** | -10° to 70°C |
| **Operating Humidity** | 5-95% non-condensing |

# APPENDIX C

# Firmware Recovery

**The detail instruction in Emergency/Failure Recovery Button**

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):
Hold the Emergency/Failure Recovery Button on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the Emergency/Failure Recovery Button. The modem's emergency-reflash web interface will then be accessible via http://192.168.1.254/ where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

2. Recovery procedures for a lost web interface password:
After turning the router on press the Emergency/Failure Recovery Button on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. The login will be reset to admin and the password will be reset to admin, and the modem will be accessible via its default IP address at http://192.168.1.254/

Before powered on the router to enter the recovery process. please configure the IP address of the PC as 192.168.1.1 and process step by step.
1. Power the router off.
2. Hold the " Emergency/Failure Recovery Button".
3. Power on the router. Then Router's IP will reset to Default (Say 192.168.1.254)
4. Upload the firmware.

# APPENDIX D

## Support

If you have any problems with the WebShare 242W Wireless , 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 SpA**
**Viale De Gasperi, 122**
**20017 Mazzo di Rho(MI)**
**Tel: +39. 02.93906085, +39. 02.93907634(help desk)**
**Fax: +39. 02.93906161**

Email: info@atlantis-land.com or tecnici@atlantis-land.com
WWW: http://www.atlantis-land.com