



VoIPMaster 260W

VoIP ADSL2+ Wireless Router

A02-RAV260-W54



USER'S MANUAL
A02-RAV260-W54_ME01



Copyright

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

Disclaimer

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

CAUTION

1. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

TABLE OF CONTENTS

CHAPTER 1	1
1.1 AN OVERVIEW OF THE ADSL2+ VOIP ROUTER	1
1.2 PACKAGE CONTENTS	2
1.3 ADSL2+ VOIP ROUTER FEATURES	2
1.4 ADSL2+ VOIP ROUTER APPLICATION	6
CHAPTER 2	7
2.1 CAUTIONS FOR USING THE ADSL2+ VOIP ROUTER	7
2.2 THE FRONT LEDS	7
2.3 THE REAR PORTS	8
2.4 CABLING	9
2.4.1 Connecting your router	10
CHAPTER 3	13
3.1 BEFORE CONFIGURATION	13
3.2 CONNECTING THE ADSL2+ VOIP ROUTER	13
3.3 CONFIGURING PC IN WINDOWS	14
For Windows 95/98/ME	14
For Windows NT4.0	16
For Windows 2000	17
For Windows XP	19
3.3.1 Configuration Check	21
3.4 FACTORY DEFAULT SETTINGS	21
3.4.1 Username and Password	21
3.4.2 LAN and WAN Port Addresses	22
3.5 INFORMATION FROM THE ISP	22
3.6 CONFIGURING WITH THE WEB BROWSER	22
3.6.1 STATUS	23
3.6.1.1 ARP Table	25
3.6.1.2 Wireless Association Table (Wireless Router only)	25
3.6.1.3 Routing Table	25
3.6.1.4 DHCP Table	26
3.6.1.5 Email Status	27
3.6.1.6 VoIP Status	27
3.6.1.7 Event Log	27
3.6.1.8 Error Log	28
3.6.1.9 NAT Sessions	28
3.6.1.10 Diagnostic	28
3.6.1.11 UPnP Portmap	29
3.6.2 Quick Start Guide	30
3.6.3 CONFIGURATION	32
3.6.3.1 LAN	32
3.6.3.1.1 Bridge Filtering	32
3.6.3.1.2 Ethernet	34

3.6.3.1.4 Ethernet Client Filter	34
3.6.3.1.6 Wireless Security	38
3.6.3.1.7 Wireless Client (MAC Address).....	40
3.6.3.1.9 DHCP Server.....	41
3.6.3.2 WAN.....	44
3.6.3.2.1 ISP	44
3.6.3.2.2 DNS	49
3.6.3.2.3 ADSL	50
3.6.3.3 SYSTEM.....	51
3.6.3.3.1 Time Zone.....	51
3.6.3.3.2 Remote Access.....	51
3.6.3.3.3 Firmware Upgrade.....	52
3.6.3.3.4 Backup/Restore	53
3.6.3.3.5 Restart.....	54
3.6.3.3.6 User Management.....	54
3.6.3.4 FIREWALL	56
3.6.3.4.1 General Settings	57
3.6.3.4.2 Packet Filing	59
3.6.3.4.3 Intrusion Detection.....	62
3.6.3.4.4 Url Filtering	64
3.6.3.4.5 Firewall Log	66
3.6.3.5 VOIP	67
3.6.3.5.1 Wizard	68
3.6.3.5.2 General Settings	69
3.6.3.5.3 Phone Ports.....	71
3.6.3.5.4 PSTN Dial Plan	73
3.6.3.5.5 VoIP Dial Plan	77
3.6.3.5.6 Ring & Tone.....	80
3.6.3.6 QoS	83
3.6.3.6.1 Prioritization.....	83
3.6.3.6.2 Outbound IP Throttling (LAN to WAN)	85
3.6.3.6.3 Inbound IP Throttling (WAN to LAN)	86
3.6.3.6.4 Example: QoS for your Network.....	87
3.6.3.7 Virtual Server.....	90
3.6.3.8 TIME SCHEDULE.....	93
3.6.3.9 ADVANCED	95
3.6.3.9.1 Static Route	95
3.6.3.9.2 Dynamic DNS.....	95
3.6.3.9.3 Check Emails	96
3.6.3.9.4 Device Management	96
3.6.3.9.5 IGMP.....	99
3.6.3.9.6 VLAN	100
Advanced VLAN Setup Example (Triply Play).....	100
3.6.4 Save Config To Flash.....	104
3.6.5 Logout.....	104

CHAPTER 4..... 105

WHAT IS VOIP?.....	105
WHAT IS VOIP?.....	106
WHAT IS HOW DOES IT WORK?	107
WHAT IS VOIP WHAT IS THE ADVANTAGES USING VOIP RATHER PSTN?	107



THEN, WHY EVERYBODY DOESN'T USE IT YET? 108
WHAT IS SIP? 108
DOES VOIPMASTER 260W SUPPORT H.323? 108
DOES MY COMPUTER HAVE TO BE TURNED ON?..... 108
HOW TO MAKE A CALL WITH REMOVE IP ADDRESS ONLY, NOT THROUGH SIP SERVER? 109
WHICH VOIP PROVIDERS CAN SUPPORT THEVOIPMASTER 260W? 110
CAN I USE THE DDNS TO MAKE A VOICE CONNECTION ? 110
WHAT IS STUN?..... 110

APPENDIX A 111

APPENDIX B 112

APPENDIX C 113

APPENDIX D 115

Chapter 1

Introduction

1.1 An Overview of the ADSL2+ VOIP Router

Broadband Sharing and IP sharing

The ADSL VOIP Firewall 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.

VoIP feature

The device is provided with a FXS port which allows using the normal PSTN phone like an actual VoIP phone.

The VoIP feature of the Router allows to make voice phone calls via Internet with an important reduction of the costs.

Moreover, with the subscription of a contract with a VoIP service provider, it will be possible to make conversations with normal phones with very low fares. The router integrates RJ11 FXO port for inbound and outbound calls transmitted through PSTN. Users can receive phone calls from PSTN while enjoying VoIP call service at the same time. In addition, the device automatically fallbacks to lifeline POTS to enable making normal phone calls when there is power outage, or when the Internet connection is down.

Security: Firewall & 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

- Adsl2+ VOIP Router (VoIPMaster 260W)
- One CDROM containing the online manual
- Vera (Multilangue Intercative Tutorial)
- One Quick Start Guide
- One RJ11 ADSL/telephone cable
- One 5 dBi Antenna
- One CAT-5 LAN cable
- One Console Cable(DB9 cable)
- One AC-DC power adapter (12VDC, 1A)

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

1.3 ADSL2+ VOIP Router Features

ADSL2+ VOIP Router provides the following features:

- **ADSL Multi-Mode Standard:** Supports downstream transmission rates of up to 8Mbps 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)].
- **Voice over IP compliance with SIP standard:** The router supports cost-effective, toll-quality voice calls over the Internet. It complies with the most popular industrial standard, SIP protocol, to ensure the interoperability with SIP devices and major VoIP Gateways. The VoIP ADSL router supports call waiting, silence suppression, voice activity detection (VAD), comfort noise generation (CNG), line echo cancellation, caller ID (Bell 202, V3) and so on. Il Dispositivo è dotato di una porta FXS che permette di utilizzare un normale telefono PSTN come un telefono VoIP a tutti gli effetti.
- **LifeLine Support:** The router integrates RJ11 FXO port for inbound and outbound calls transmitted through PSTN. Users can receive phone calls from PSTN while enjoying VoIP call service at the same time. In addition, the device automatically

fallbacks to lifeline POTS to enable making normal phone calls when there is power outage, or when the Internet connection is down.

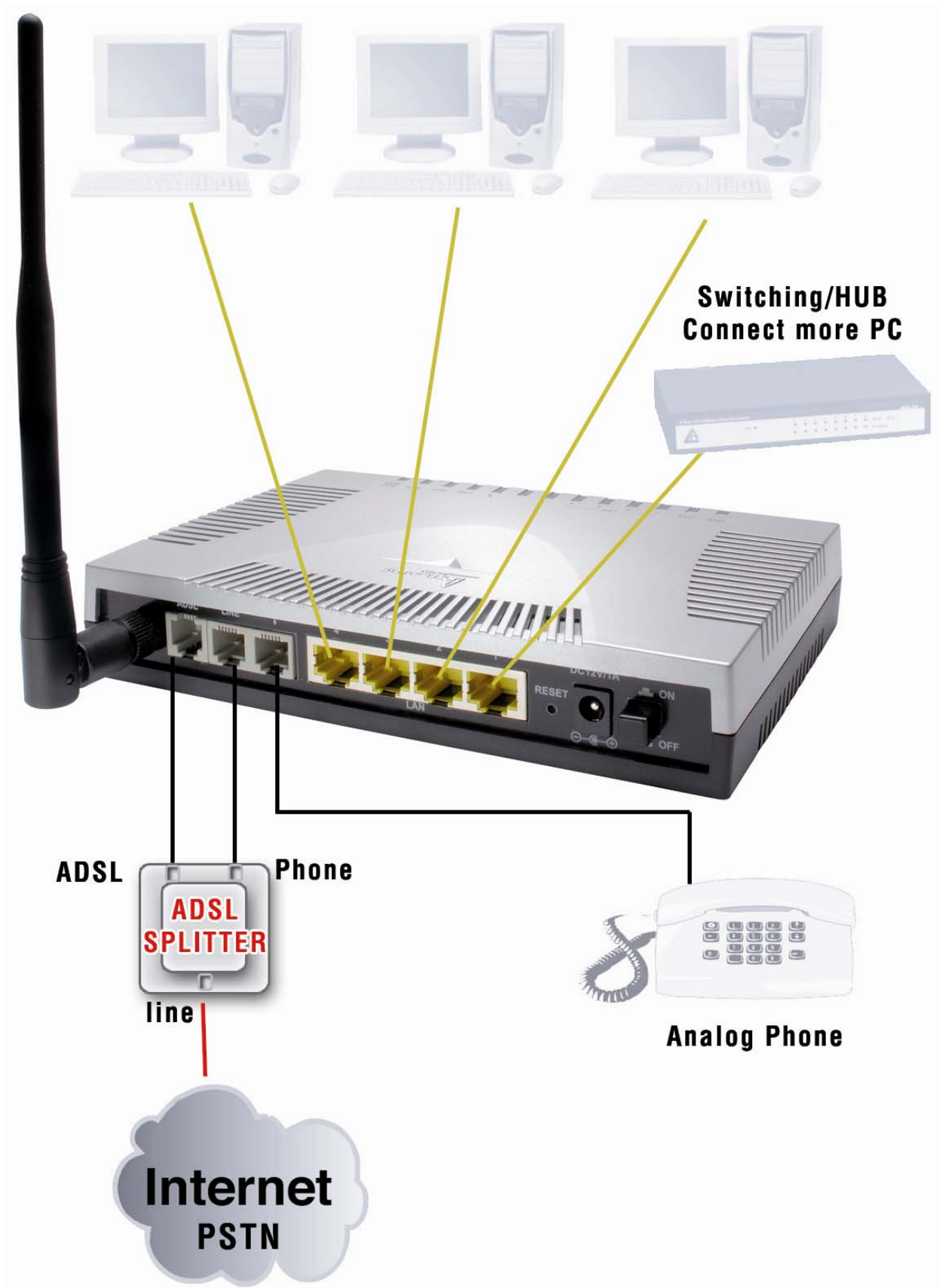
- **Fast Ethernet Switch:** A 4-port 10/100Mbps fast Ethernet switch is supported in the LAN site and automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports is supported. An Ethernet straight or cross-over cable can be used directly, this fast Ethernet switch will detect it automatically.
- **802.11g Wireless AP with WPA Support:** With integrated 802.11g Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection (ADSL) with single device simplicity, and as a result, mobility to the users. In addition to 54 Mbps 802.11g data rate, it also interoperates backward with existing 802.11b equipment. The Wireless Protected Access (WPA) and Wireless Encryption Protocol (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.
- **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.
- **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 ADSL2+ VOIP Router Application



Chapter 2

Using ADSL2+ VOIP Router

2.1 Cautions for using the ADSL2+ VOIP Router



Do not place the ADSL2+ VOIP Router under high humidity and high temperature.

Do not use the same power source for ADSL2+ VOIP Router with other equipment.

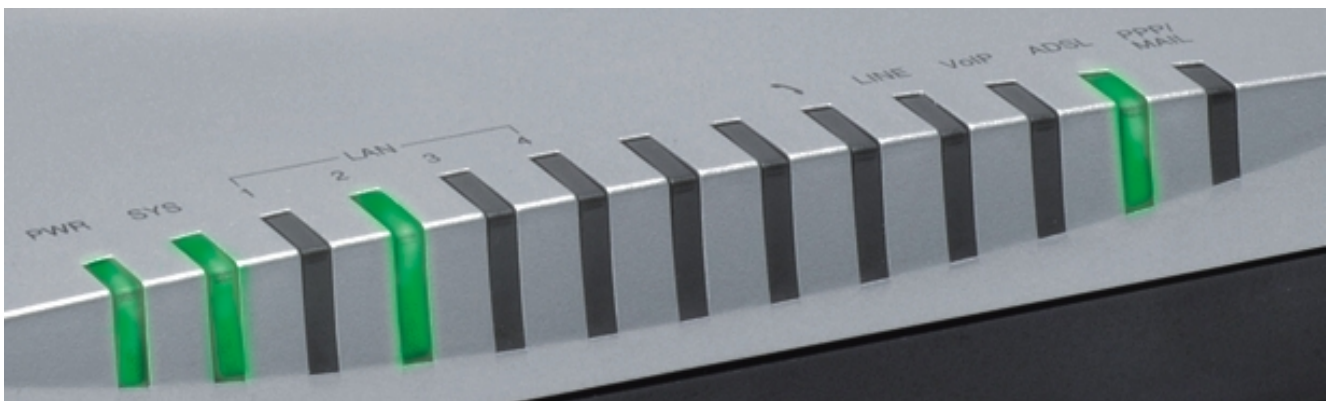
Do not open or repair the case yourself. If the ADSL2+ VOIP Router is too hot, turn off the power immediately and have a qualified serviceman repair it.



Place the ADSL2+ VOIP Router on a stable surface.

Only use the power adapter that comes with the package.

2.2 The Front LEDs



LED	Meaning
POWER	Lit when power ON.
SYS	Lit when system is ready.
LAN (1-4)	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received.
WLAN	Lit green when the wireless connection is established. Flashes when sending/receiving data.
PHONE	Lit green when the phone is off-hook.

LINE	Lit when the inbound and outbound calls transmitted through PSTN.
VoIP	Lit when SIP registration is OK.
ADSL	Lit when successfully connected to an ADSL DSLAM.
PPP/MAIL	Steady glow when there is a PPPoA / PPPoE connection. Blinking if there is a new incoming mail.

2.3 The Rear Ports



PORT	Meaning
Antenna (R-SMA)	Connect the detachable antenna to this port.
ADSL (RJ11)	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network.
LINE (RJ11)	Connect RJ-11 cable to this port when connecting to the telephone wall jack.
PHONE (RJ11)	Connect RJ-11 cable to this port when connecting to an analog phone set.
LAN (4 *RJ-45)	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	Press this button in order to reset the router or restore configuration. Refer to the following timing: 0-3 seconds: Router reset 3-6 seconds: no action 6 seconds or more: Restore factory settings.
POWER (Jack)	Connect the supplied power adapter to this

	jack.
POWER Switch	A Power ON/OFF switch



The Ethernet Port # 4 (close the Phone Port) can be connected to the computer and console. You need a special console tool which is included in this package to connect the LAN cable of Port 4 when connecting to a PC's RS-232 port (9-pin serial port).

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 and SYS LEDs are lit. If they are not, verify that you are using the proper cables.

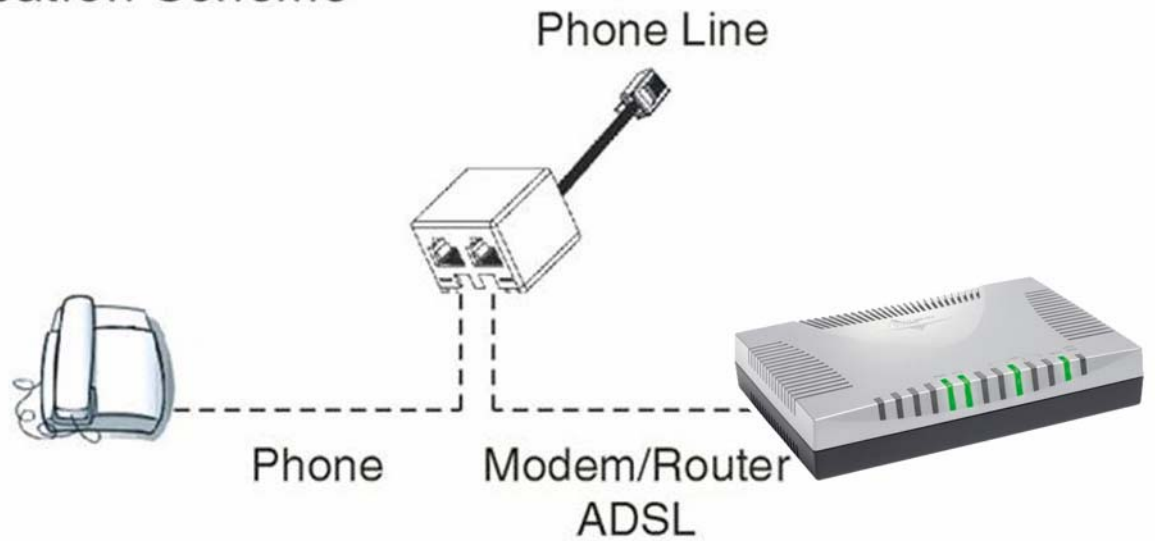
If the **LED ADSL** continually flashes You have to read Note (into section **3.6.3.2.3**) in order to solve this problem

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.

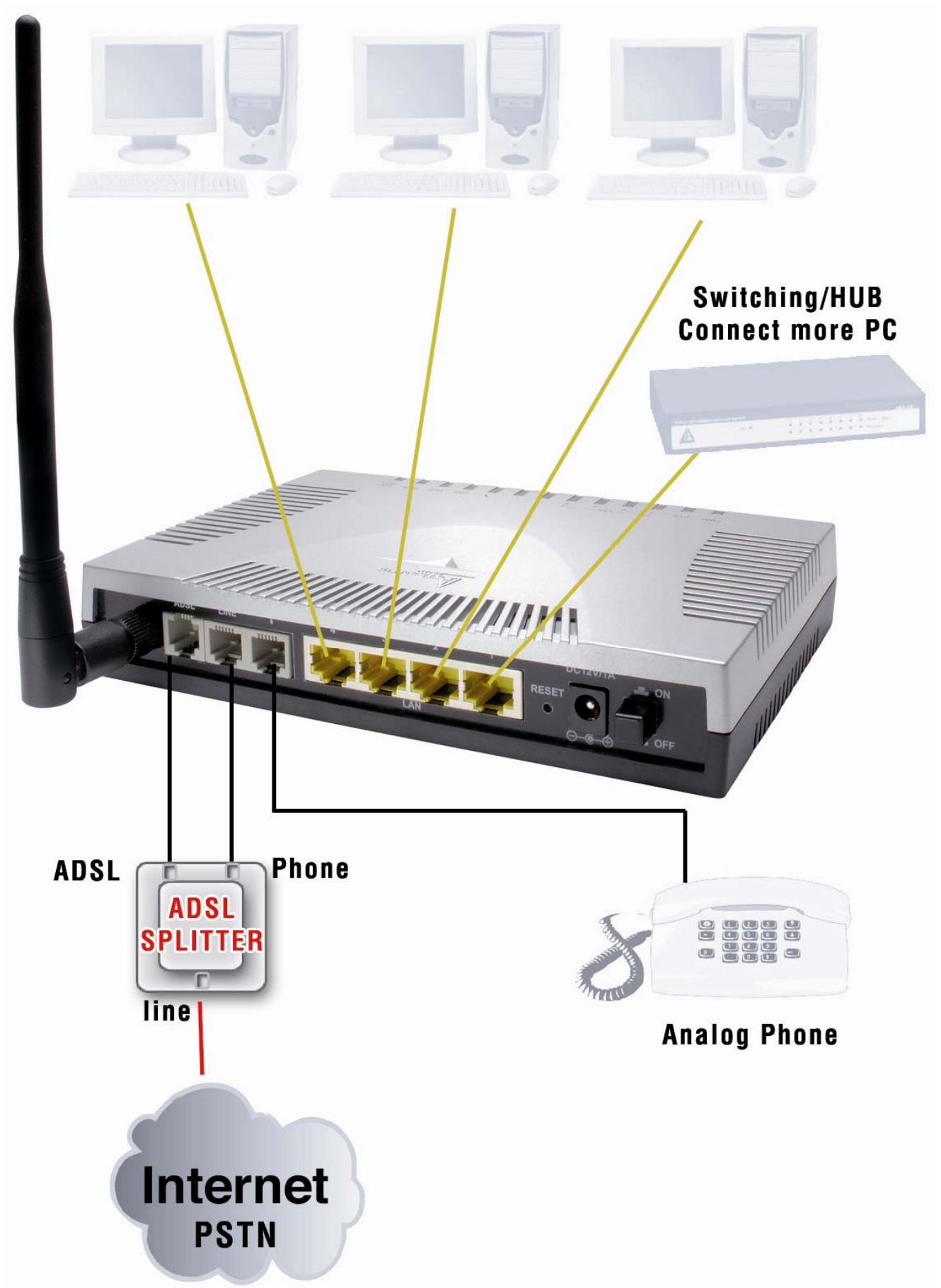


Application Scheme



2.4.1 Connecting your router

1. Connect this router to a **LAN** (Local Area Network) and the ADSL/telephone (**ADSL**) network.
2. Power on the device.
3. Make sure the **PWR** and **SYS** LEDs are lit steadily and that the **LAN** LED is lit.
4. Connect an RJ11 cable to VoIP port when connecting to an analog phone set.
5. Connect RJ-11 cable to LINE Port when connecting to the telephone wall jack.





If the **ADSL Led** flashes periodically You have to force modulation. Click on **Configuration, WAN** then **ADSL**. On the combo-box **Connection Mode** please choose **ADSL**. Press **Apply** and then click on **Save Config to Flash**.

ADSL	
Parameters	
Connect Mode	ADSL
Modulation	ADSL2, auto-fallback ADSL2+, auto-fallback ADSL
Profile Type	
Activate Line	true
Coding Gain	auto
Tx Attenuation	Dmt_0DB
DSP Firmware Version	E.38.2.12
Connected	true
Operational Mode	G.Dmt
Annex Type	AnnexA
Upstream	608000
Downstream	1504000
CO Vendor	BCLA
Elapsed Time	0 day 3 hr 11 min 57 sec

[Advanced Options](#)

Chapter 3

Configuration

The ADSL2+ VOIP Router 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 ADSL2+ VOIP Router, either to configure the device or for network access. These PCs must have an Ethernet interface installed properly, be connected to the ADSL2+ VOIP 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 ADSL2+ VOIP Router.

The default IP address of the ADSL2+ VOIP Router 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 ADSL2+ VOIP Router.

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.



Any TCP/IP capable workstation can be used to communicate with or through the ADSL2+ VOIP Router. To configure other types of workstations, please consult the manufacturer's documentation.

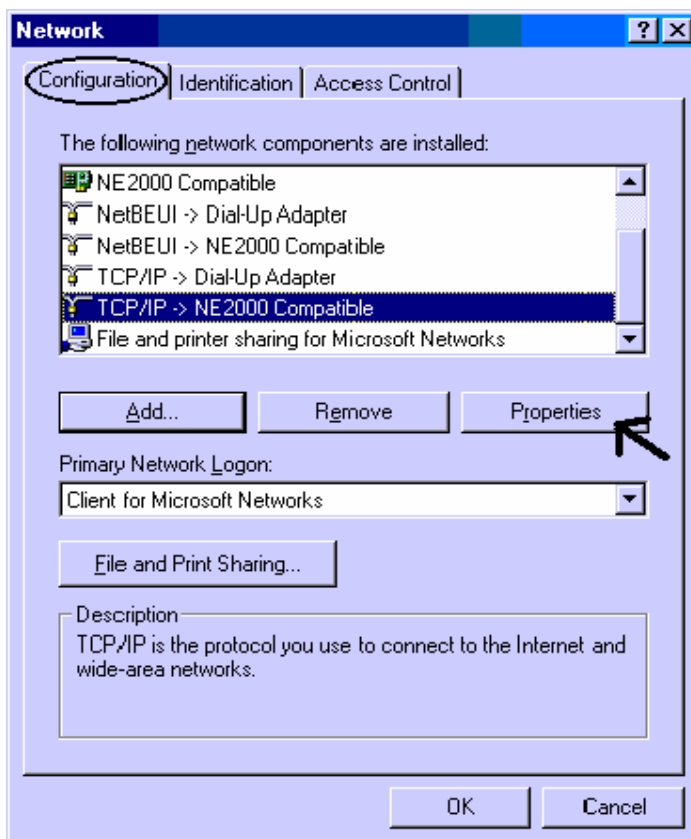
3.2 Connecting the ADSL2+ VOIP Router

- Connect the ADSL2+ VOIP Router 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.

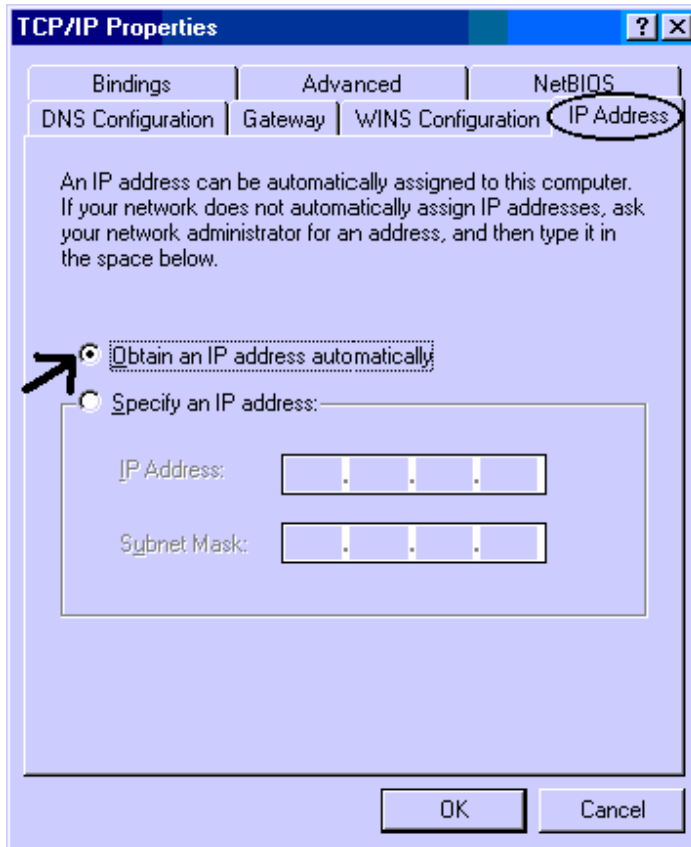
3.3 Configuring PC in Windows

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.

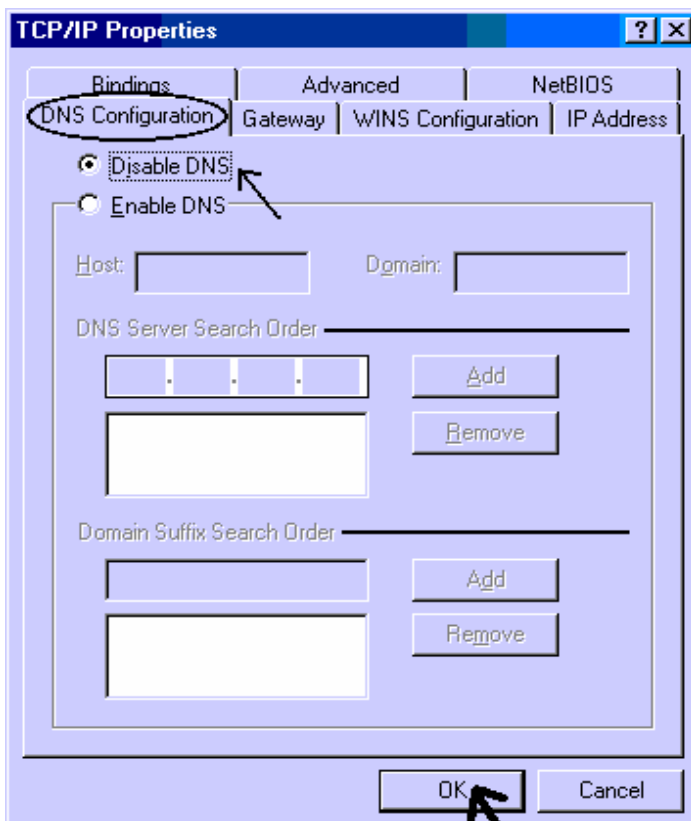


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.



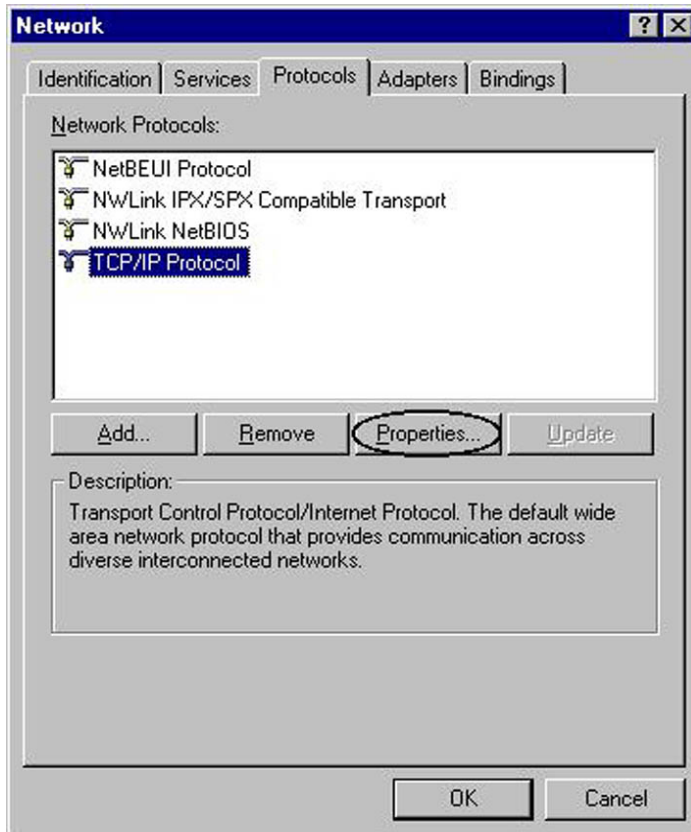
5. Then select the **DNS Configuration** tab.

6. Select the **Disable DNS** radio button and click “**OK**” to finish the configuration.

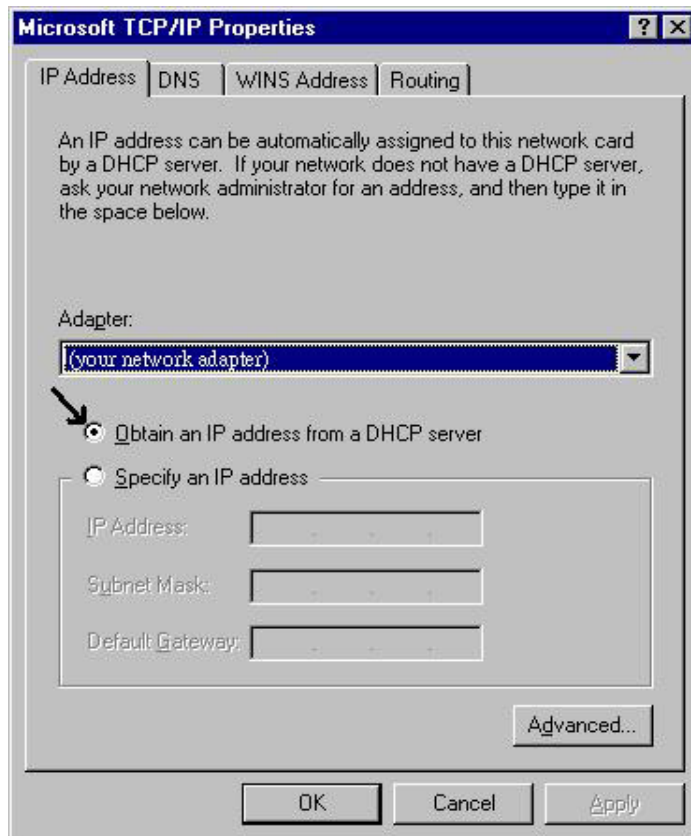


For Windows NT4.0

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”**.

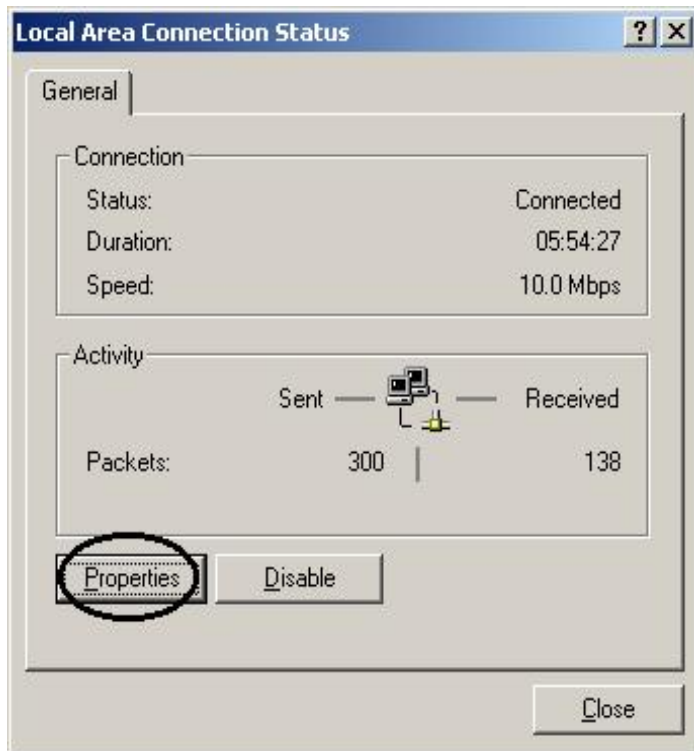


For Windows 2000

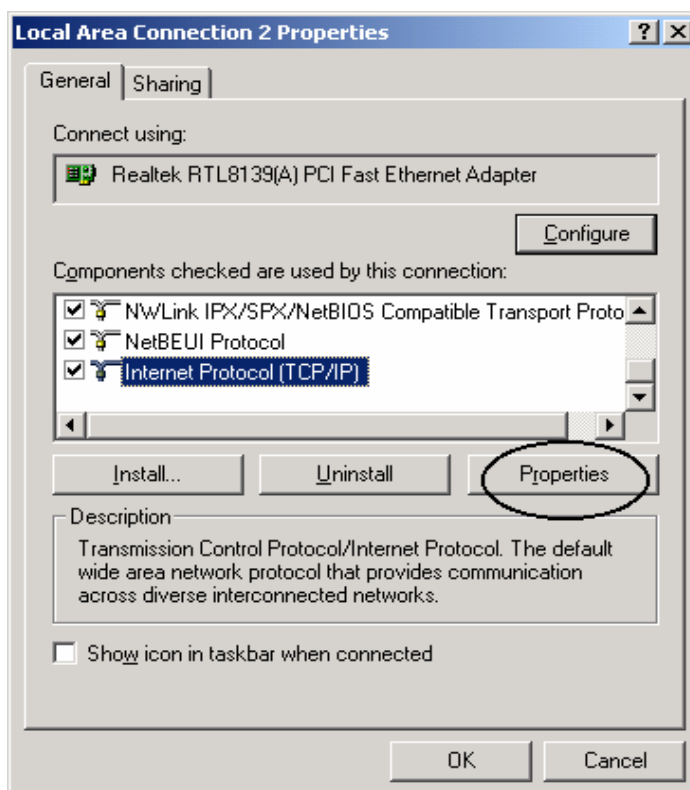
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **LAN Area Connection**.



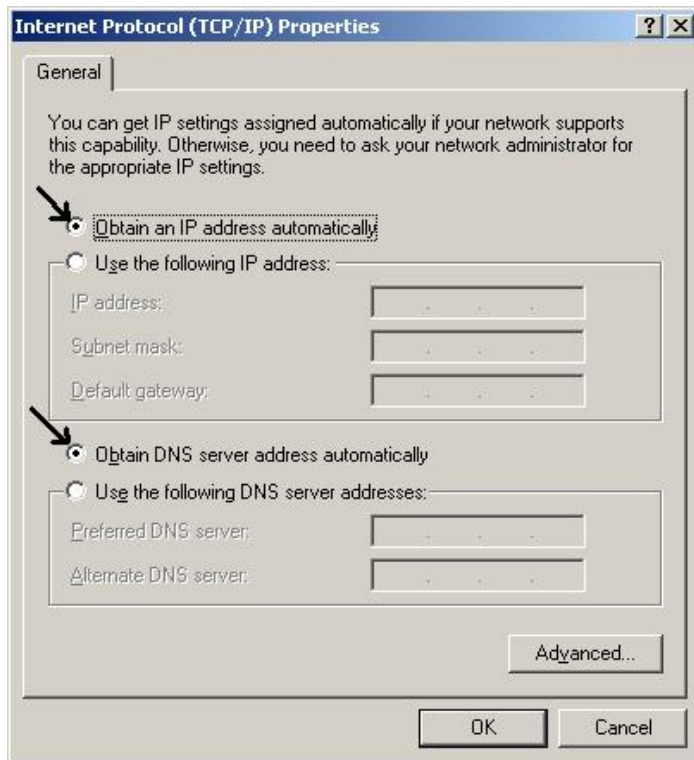
3. In the **LAN Area Connection Status** window, click **Properties**.



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

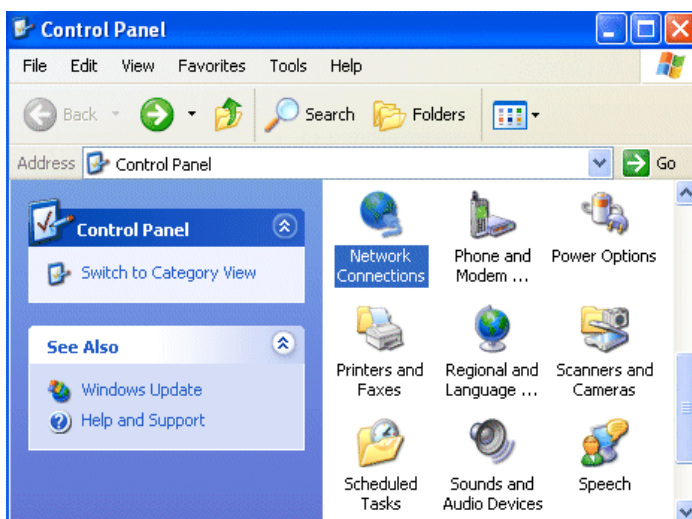


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **“OK”** to finish the configuration.

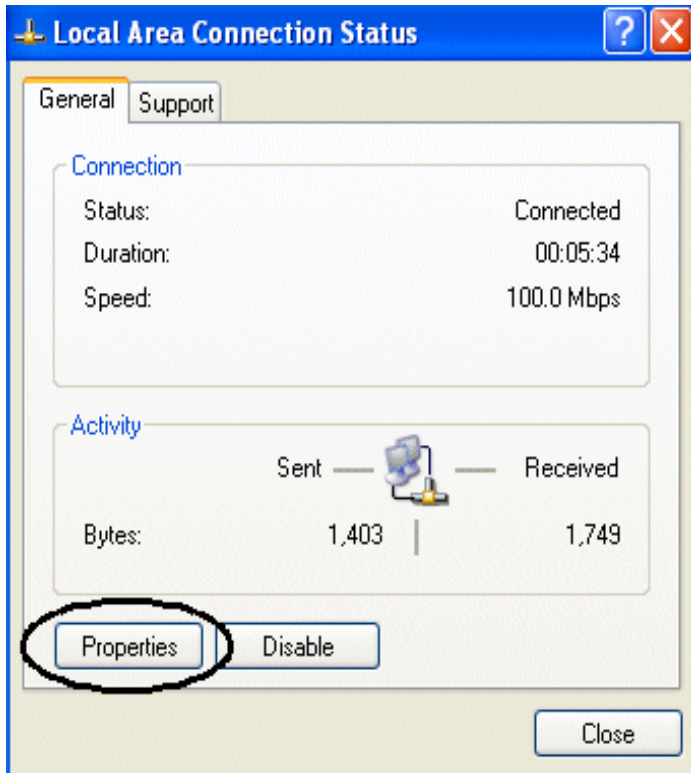


For Windows XP

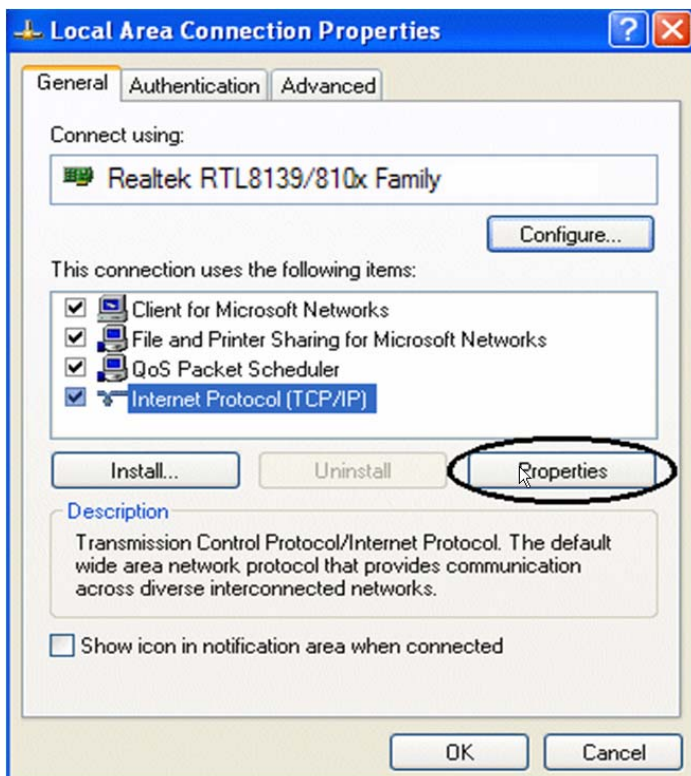
1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**



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

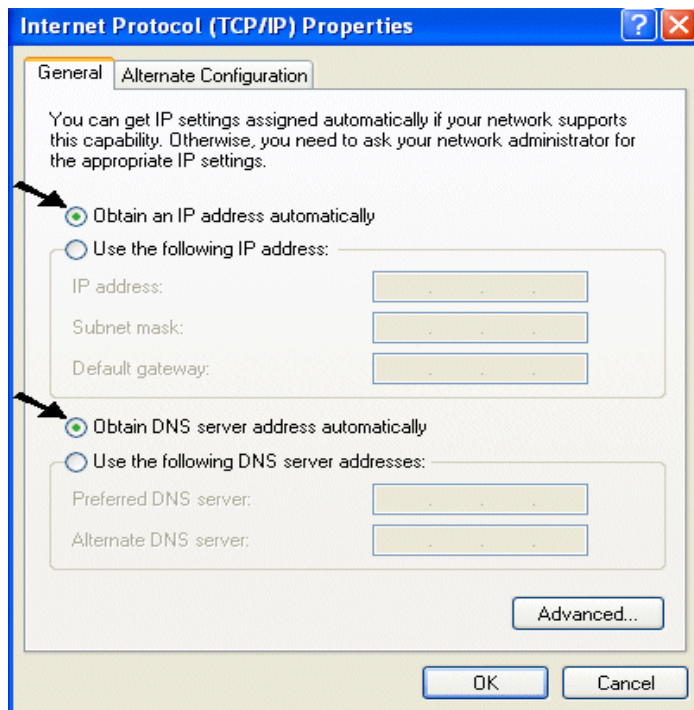


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



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

6. Click **“OK”** to finish the configuration.



3.3.1 Configuration Check

In order to verify the Ethernet Card configuration, please refer to the following steps:

1. Click on Start, then Run; type in the Open field **cmd**.
2. When DOS window appears, type **ping 192.168.1.254**

The following output will be shown:

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 times<10ms TTL=64

Reply from 192.168.1.254: bytes=32 times<10ms TTL=64

Reply from 192.168.1.254: bytes=32 times<10ms TTL=64

3. If the ping command doesn't work, please check your Ethernet Card configuration.

3.4 Factory Default Settings

Before configuring this ADSL2+ VOIP Router, 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: **enable**
- WAN=PPPoA Routing, VPI=8, VCI=35, VC-Mux
- SSSID= **A02-RAV260-W54** , Channel=6, WEP/WPA=**disable**

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. 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

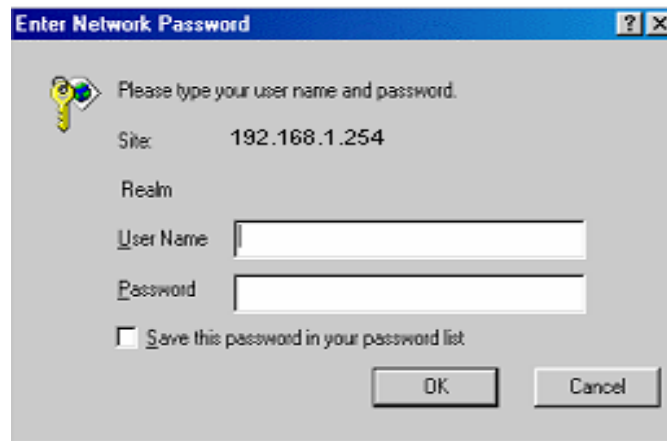
Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IpoA.

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 ADSL2+ VOIP Router, 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, Wireless Association, Routing Table, DHCP Table, Email Status, VoIP Status, Event Log, Error Log, NAT Sessions, Diagnostic, UPnP PortMap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, VoIP, QoS, Virtual Server, Time Schedule, Advanced)
- **Save Config to Flash**
- **Language** (English, Francais)

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

3.6.1 STATUS

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 various and useful information for user to exam the status of the device.

- **ARP Table**
- **Routing Table**
- **DHCP Table**
- **PPTP Status**
- **IPSec Status**
- **L2TP Status**
- **Email Status**
- **Event Log**
- **Error Log**
- **NAT Sessions**
- **Diagnostics**
- **UPnP PortMap**

When you click the **ARP Table**, you will see the data of the IP address of each PC in your LAN as well as its associated MAC address.

When you click the **DHCP Table**, you can see the status of the assigned IP addresses with its associated information.

When you click the **PPTP Status**, it gives you a quick view to know the ADSL Router's current status. The status of PPTP connection will be shown.



When you click the **Email Status**, it gives you a quick view to know if there is email in your predefined email account. You will see the unread emails in the email server and, once you have configured successfully the “Check Emails” in **Configuration -> Advance**.

When you click the **Event Log**, it displays the valuable system event logging information and status after the power is turned on, such as ADSL line, WAN port, SNTP, Firewall, and etc.

When you click the **Error Log**, it shows the error message log. When you face a problem, please send this error log to support for a quick feedback.

Please see the relevant sections of this manual for detailed instructions on how to configure the VoIP ADSL Router.

3.6.1.1 ARP Table

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

ARP Table			
IP <> MAC List			
IP Address	MAC Address	Interface	Static
192.168.1.187	00:0c:6e:bd:11:6d	iplan	no

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

- “no” for dynamically-generated ARP table entries
- “yes” for static ARP table entries added by the user

3.6.1.2 Wireless Association Table (Wireless Router only)

Wireless Association Table	
Wireless client's MAC address and the corresponding IP address	
IP Address	MAC
192.168.1.100	00:04:23:73:9a:86

IP Address: It is IP address of wireless client that joins this network.

MAC: The MAC address of wireless client.

3.6.1.3 Routing Table

Routing Table				
Routing Table				
Valid	Destination	Netmask	Gateway/Interface	Cost

RIP Routing Table			
Destination	Netmask	Gateway	Cost

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

Destination: The IP address of the destination network.

Netmask: The destination netmask address.

Gateway: The IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

3.6.1.4 DHCP Table

DHCP Table

Type

[Leased](#)
[Expired](#)
[Permanent](#)

Leased: The DHCP assigned IP addresses information.

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table

Leased Table

IP Address	MAC Address	Client Host Name	Expiry
------------	-------------	------------------	--------

IP Address: The IP address that assigned to client.

MAC Address: The MAC address of client.

Client Host Name: The Host Name (Computer Name) of client.

Expiry: The current lease time of client.

Expired Table

Expired Table

IP Address	MAC Address	Client Host Name	Expiry
------------	-------------	------------------	--------

Please refer the **Leased Table**.

Permanent Table

Permanent Table

Name	IP Address	MAC Address	Maximum Lease Time
------	------------	-------------	--------------------

Name: The name you assigned to the Permanent configuration.

IP Address: The fixed IP address for the specify client.

MAC Address: The MAC Address that you want to assign the fixed IP address

Maximum Lease Time: The maximum lease time interval you allow to clients

3.6.1.5 Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.

Email Status	
Email Account	
Account Name	username
POP3 Mail Server	pop3.mail.com
Email Status	No mail

3.6.1.6 VoIP Status

Details and status for the VoIP Account you have configured the router to check. Please see the **Phone Configuration** section of this manual for details on this function.

VoIP Status				
Phone Port				
Index	Phone Number	User Domain	Display Name	Registered
1				unknown

3.6.1.7 Event Log

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

Event Log
<pre> ----- system log buffer head ----- ----- system log buffer tail ----- </pre>

3.6.1.8 Error Log

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

Error Log

Error Log (times are in seconds since last reboot)

When	Process	Error Log
------	---------	-----------

3.6.1.9 NAT Sessions

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

NAT Sessions

Active NAT sessions between interface of types external and internal:

Prot	Local IP: Port	local/public	Remote IP: Port	Idle (sec.)
TCP	192.168. 1.201:	1110/ 1110	64. 94.110. 12: 80	29
TCP	192.168. 1. 99:	1982/ 1982	210.184.108.126: 80	729
TCP	192.168. 1. 99:	1979/ 1979	207. 68.178.239: 80	542
TCP	192.168. 1.202:	2011/ 2011	207. 46.107. 27: 1863	21
TCP	192.168. 1.100:	1166/ 1166	207. 46.106. 90: 1863	18
TCP	192.168. 1. 99:	1969/ 1969	207. 46.107. 22: 1863	673
ICMP	192.168. 1.201:	512/ 512	168. 95. 4.211: 512	0

TCP : 6 sessions
 UDP : 0 sessions
 Others : 1 sessions
 Total : 7 sessions

Refresh

3.6.1.10 Diagnostic

It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection. If **PING www.google.com** is shown **FAIL** and the rest is **PASS**, you ought to check your PC's DNS settings is set correctly.

Diagnostic

LAN Connection

Testing Ethernet LAN connection PASS

WAN Connection

Testing ADSL Synchronization FAIL

Testing WAN connection FAIL

Ping Primary Domain Name Server FAIL

PING www.google.com FAIL

Refresh

3.6.1.11 UPnP Portmap

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

UPnP Portmap

UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address
emwebigd1024	udp	35324 ~ 35324	15852 ~ 15852	192.168.1.205
emwebigd1025	tcp	48888 ~ 48888	14811 ~ 14811	192.168.1.205
emwebigd1063	udp	9210 ~ 9210	15169 ~ 15169	192.168.1.202
emwebigd1064	tcp	50937 ~ 50937	14500 ~ 14500	192.168.1.202

3.6.2 Quick Start Guide

Quick Start	
Connection	
Encapsulation	PPPoE <input type="button" value="Auto Scan"/>
VPI	0
VCI	33
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Optional Settings	
IP Address	0.0.0.0 <small>(0.0.0.0 means 'Obtain an IP address automatically')</small>
SubNetmask	0.0.0.0
Default Gateway	0.0.0.0
DNS	
Obtain DNS automatically	<input type="checkbox"/> Enable
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPP	
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

If you use this device to access the Internet through the ISP, this web page is enough for you to configure this router and access the Internet without a problem. Please check Information from the ISP, then enter the proper values into this web page, click the **Apply** button and then **Save Config to FLASH** in the left panel. After the router reboot, you may check the Status web page to check whether the router is connected to the ISP or not. In most cases, you can access the Internet immediately. If not, please refer to the sections below for more information.

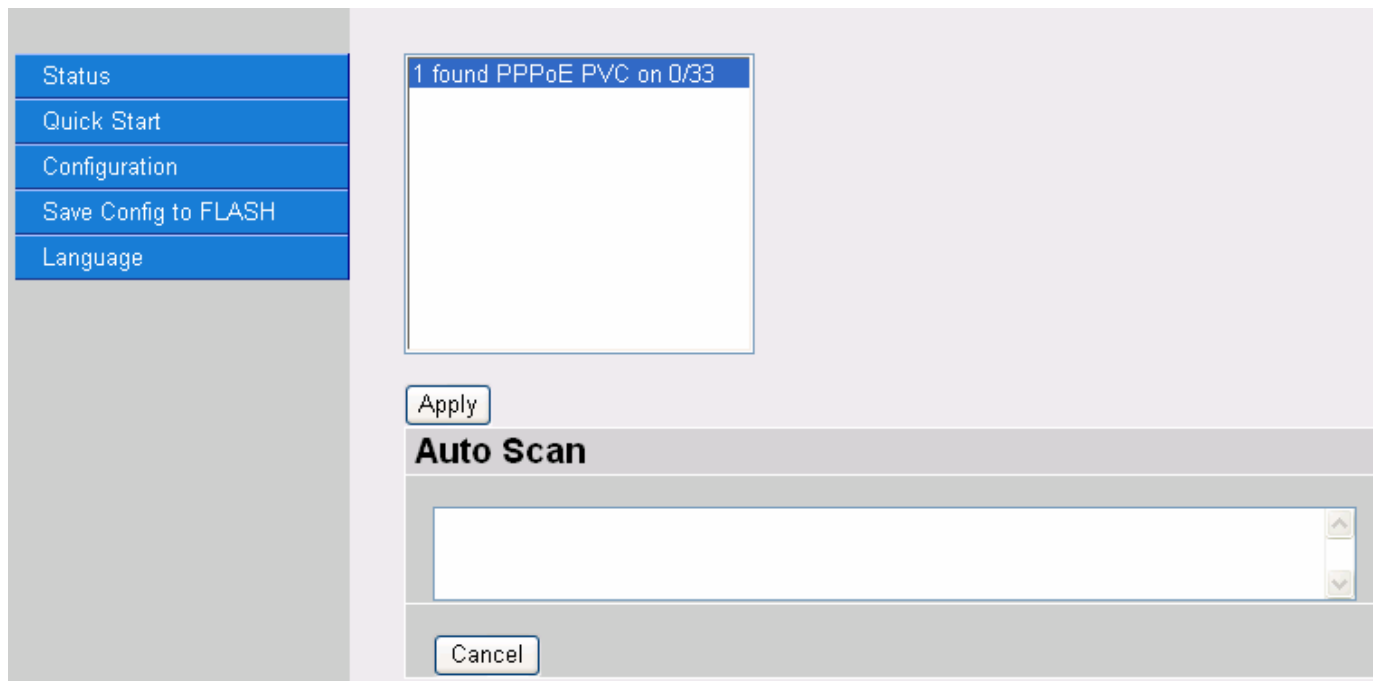
For detailed instructions on configuring your WAN settings, please see the **WAN** section of this manual.

Usually, the only details you will 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. In addition, you have the option to provide specific DNS as your desire, or check the **Enable** box to get the DNS automatically from your ISP.

Your ISP will be able to 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 attempt to determine the Encapsulation types offered by your ISP.

Auto Scan	
Before you scan the PVCs, please DELETE all the WAN interfaces.	
IP Address	<input type="text"/> if provided by ISP
Gateway	<input type="text"/> if provided by ISP
<input type="button" value="Start"/>	

Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful you will then be presented with a list of supported options:



Select the desired option from the list and click **Apply** to return to the Quick Start interface to continue configuring your ISP connection. Please note that the contents of this list will vary, depending on what is supported by your ISP.

3.6.3 CONFIGURATION


When you click this item, you get following sub-items to configure ADSL2+ VOIP Router:

- LAN
- WAN
- System
- Firewall
- VoIP
- QoS
- Virtual Server
- Time Schedule
- 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 four items within the LAN section: **Bridge Filtering, Ethernet, Ethernet Client Filtering, Port Setting, DHCP Server**

3.6.3.1.1 Bridge Filtering

Bridge Interface	
Parameters	
Bridge Interface	VLAN Port
ethernet 	<input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4
ethernet1	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
ethernet2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
ethernet3	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Device Management	
Management Interface	<input checked="" type="radio"/> ethernet
<input type="button" value="Apply"/>	

You can setup member for each port of each VLAN group under Bridge Interface section.

Bridge Interface: Is the name of VLAN Group

VLAN Port: To select which port/ports are parts of this VLAN Group

Management Interface: To specify which VLAN group has possibility to do device management, like doing web management.

Click on Bridge Interface name to edit **Bridge Interface Parameters**.

Bridge Interface	
Parameters	
Bridge Interface	VLAN Port
Ethernet	<input checked="" type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Ethernet1	<input type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4
Ethernet2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Ethernet3	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Device Management	
Management Interface	<input checked="" type="radio"/> Ethernet
<input type="button" value="Apply"/>	

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

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4) Please uncheck P2, P3, P4 from Ethernet VLAN port first.



You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4



Management Interface: To specify which VLAN group has possibility to do device management, like doing web management.



NAT/NAPT can be applied to management interface only.

Edit ethernet Interface	
Parameters	
Acceptable Frame Type	ALL
Filter Type	All
PVID for Untagged Frames	1
<input type="button" value="Apply"/> <input type="button" value="Return"/>	

3.6.3.1.2 Ethernet

Ethernet				
Primary IP Address				
IP Address	192	168	1	254
SubNetmask	255	255	255	0
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast			
<input type="button" value="Apply"/>				
IP Alias				
IP Address	SubNetmask	Security Interface		
<input type="button" value="Add"/>				

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.

3.6.3.1.3 IP Alias

IP Alias				
Parameters				
IP Address				
SubNetmask				
Security Interface	<input checked="" type="radio"/> Internal <input type="radio"/> External <input type="radio"/> DMZ			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

IP Address: Insert the secondary IP Address

SubNetMask: Set the related SubNetMask

Security Interface: Assign the interface type to the secondary Ip Address

- **Internal:** The network is behind NAT. All traffic will do network address translation when sending out to Internet if NAT is enabled.
- **External:** There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface.
- **DMZ:** Specify this network to DMZ area. There is no NAT on this interface.

3.6.3.1.4 Ethernet Client Filter


The Ethernet Client Filter supports up to 16 Ethernet network machines that helps you to manage your network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access your LAN.

There are no pre-define Ethernet MAC address filter rules; you can add the filter rules to meet your requirements.

Ethernet Client Filter

Filtering Rules

Ethernet Client Filter	<input checked="" type="radio"/> Disable	<input type="radio"/> Allowed	<input type="radio"/> Blocked
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	
	<input type="text"/>	<input type="text"/>	

MAC Address List Candidates 

(MAC Address Format is 'xxxx:xxxx:xxxx:xx')

Ethernet Client Filter: Default setting is set to **Disable**.

- **Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided. Make sure your PC's MAC is listed.
- **Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided. Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number **0 - 9** and letters **a - f** are acceptable.

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

Candidates: automatically detects devices connected to the router through the Ethernet. Active PC in LAN displays a list of individual Ethernet device's IP Address & MAC Address which connecting to the router. You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table. The maximum Ethernet client is 16.

Active PC in LAN	
IP Address	MAC Address
<input type="checkbox"/> 192.168.1.188	00:e0:18:df:7b:64
<input type="checkbox"/> 192.168.1.67	00:0a:e6:56:74:e5
<input type="checkbox"/> 192.168.1.240	00:06:1b:ca:db:e6
<input type="checkbox"/> 192.168.1.1	00:04:ed:1d:18:9d
<input type="button" value="Add"/>	

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

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table. The maximum Ethernet client is 16.

3.6.3.1.5 Wireless

Wireless	
Parameters	
WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11b + g
ESSID	wlan-ap
ESSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Connected	true
AP MAC address	00:04:ed:1e:14:b1
AP Firmware Version	1.38.1.7.06.2004
Wireless Distribution System (WDS)	
WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Peer WDS MAC address	00:00:00:00:00:00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WLAN Service: Default setting is set to **Enable**. If you do not have any wireless, both 802.11g and 802.11b, device in your network, select **Disable**.

Mode: The default setting is **802.11b+g** (Mixed mode). If you do not know or have both 11g and 11b devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **802.11g** if you have only 11g card. If you have only 11b card, then select **802.11b**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default **wlan-ap** to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.



It is case sensitive and must not excess 32 characters.

ESSID Broadcast: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enable**.

- **Disable:** If you do not want broadcast your ESSID. Any client uses “any” wireless setting cannot discover the Access Point (AP) of your router.
- **Enable:** Any client that using the “any” setting can discover the Access Point (AP) in this mode.

Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America), Europe, France**, etc. The Channel ID will be different based on this setting.

Channel ID: Select the ID channel that you would like to use.

Connected: Representing in **true** or **false**. That it is the connection status between the system and the build-in wireless card.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

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

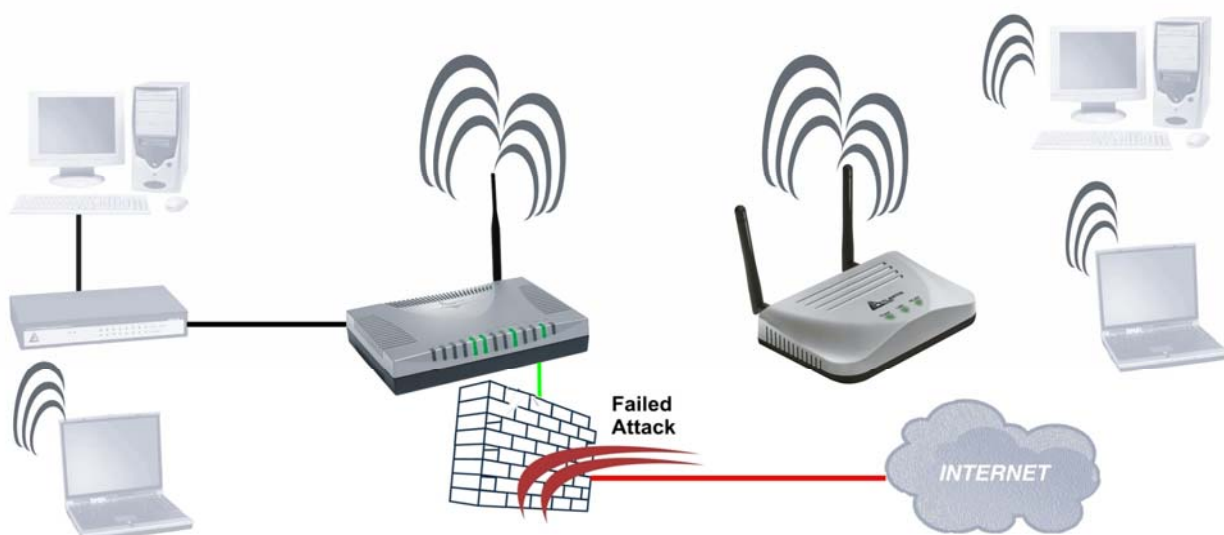
In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

WDS Service: The default setting is **Disable**. Check **Enable** radio button to activate this function.

Peer WDS MAC Address: It is the associated AP’s MAC Address. It is important that your peer’s AP must include your MAC address in order to acknowledge and communicate with each other.



For MAC Address, Semicolon (:) must be included





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 encryption 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 to extend wireless coverage.

3.6.3.1.6 Wireless Security

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

Wireless Security	
Parameters	
Security Mode	Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WPA Pre-Shared Key:

Wireless Security	
Parameters	
Security Mode	WPA Pre-Shared Key
WPA Algorithm	TKIP
WPA Shared Key	password
Group Key Renewal	3600 Seconds
Hide ESSID	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- 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).

WEP:

Wireless Security	
Parameters	
Security Mode	WEP
WEP Authentication	Open System
WEP Encryption	<input checked="" type="radio"/> WEP64 <input type="radio"/> WEP128 Hex
Passphrase	<input type="text"/> <input type="button" value="Generate"/>
Default Used WEP Key	0 (0~3)
Key 0	00-00-00-00-00
Key 1	00-00-00-00-00
Key 2	00-00-00-00-00
Key 3	00-00-00-00-00
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **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.
- **WEP Authentication:** There are three options to choose, Open System, Shared Key and Both. The default is set to Open System which does not request a shared key between the AP sender and the AP client, only supplying a correct SSID and an encryption key if there is any. With Share Key authentication, the AP client is granted only if it provided correct challenge response to the AP.
- **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.
- **Default Used WEP Key:** Select the encryption key ID; please refer to Key (0-3) below.
- **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.

3.6.3.1.7 Wireless Client (MAC Address)

The MAC Address supports up to 16 wireless network machines and helps you to manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) to access your LAN.

There are no pre-define MAC Address filter rules; you can add the filter rules to meet your requirements.

Wireless Client (MAC Address) Filter

Filtering Rules

Filter Action	<input checked="" type="radio"/> Disable	<input type="radio"/> Allowed	<input type="radio"/> Blocked
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Ethernet Client Filter: Default setting is set to Disable.

- Allowed: check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▶. Make sure your PC's MAC is listed.
- Blocked: check to prevent unwanted device accessing the LAN by insert the MAC Address in the space provided or click Candidates ▶. Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number 0 - 9 and letters a - f are acceptable.



For MAC Address, Semicolon (:) must be included

Candidates: it automatically detects devices connected to the router through the Ethernet.

Candidates ▶ → Associated Wireless Clients

Associate Wireless Client displays a list of individual wireless device's MAC Address that currently connects to the router.

You can easily by checking the box next to the MAC address to be blocked or allowed. Then, Add to insert to the Wireless Client (MAC Address) Filter table. The maximum Ethernet client is 16.

3.6.3.1.8 Port Setting

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

Port Setting	
Parameters	
Port1 Connection Type	Auto
Port2 Connection Type	Auto
Port3 Connection Type	Auto
Port4 Connection Type	Auto
IPv4 TOS Priority Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Set High Priority TOS	
<input type="checkbox"/> 63 <input type="checkbox"/> 62 <input type="checkbox"/> 61 <input type="checkbox"/> 60 <input type="checkbox"/> 59 <input type="checkbox"/> 58 <input type="checkbox"/> 57 <input type="checkbox"/> 56 <input type="checkbox"/> 55 <input type="checkbox"/> 54 <input type="checkbox"/> 53 <input type="checkbox"/> 52 <input type="checkbox"/> 51 <input type="checkbox"/> 50 <input type="checkbox"/> 49 <input type="checkbox"/> 48	
<input type="checkbox"/> 47 <input type="checkbox"/> 46 <input type="checkbox"/> 45 <input type="checkbox"/> 44 <input type="checkbox"/> 43 <input type="checkbox"/> 42 <input type="checkbox"/> 41 <input type="checkbox"/> 40 <input type="checkbox"/> 39 <input type="checkbox"/> 38 <input type="checkbox"/> 37 <input type="checkbox"/> 36 <input type="checkbox"/> 35 <input type="checkbox"/> 34 <input type="checkbox"/> 33 <input type="checkbox"/> 32	
<input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 26 <input type="checkbox"/> 25 <input type="checkbox"/> 24 <input type="checkbox"/> 23 <input type="checkbox"/> 22 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16	
<input type="checkbox"/> 15 <input type="checkbox"/> 14 <input type="checkbox"/> 13 <input type="checkbox"/> 12 <input type="checkbox"/> 11 <input type="checkbox"/> 10 <input type="checkbox"/> 9 <input type="checkbox"/> 8 <input type="checkbox"/> 7 <input type="checkbox"/> 6 <input type="checkbox"/> 5 <input type="checkbox"/> 4 <input type="checkbox"/> 3 <input type="checkbox"/> 2 <input type="checkbox"/> 1 <input type="checkbox"/> 0	
<input type="button" value="Apply"/>	

Port # Connection Type: Five options to choose from: Auto, 10M half-duplex, 10M full duplex, 100M half-duplex or 100M full-duplex. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is Auto, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-2 are used to specify the priority (precedence) of the packet, and bits 3-5 are specified the delay, throughput and reliability. This feature uses bits 0-2 to classify the packet’s priority. If the packet is high priority, it will flow first. Therefore, when this feature is enabled, the router’s Ethernet switch will check the 2nd octet of each IP packet. If the value in the Precedence of TOS field matches the checked values in the table (0 to 63), this packet will be treated as high priority.

3.6.3.1.9 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	<input type="radio"/> Disable
	<input checked="" type="radio"/> DHCP Server
	<input type="radio"/> DHCP Relay Agent

DHCP

DHCP Server

Allow Bootp	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Allow Unknown Clients	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Use Default Range	<input type="checkbox"/>
Starting IP Address	<input type="text" value="192.168.1.100"/>
Ending IP Address	<input type="text" value="192.168.1.199"/>
Default Lease Time	<input type="text" value="43200"/> seconds
Maximum Lease Time	<input type="text" value="86400"/> seconds
Use Router as DNS Server	<input checked="" type="checkbox"/>
Primary DNS Server Address	<input type="text" value="0.0.0.0"/>
Secondary DNS Server Address	<input type="text" value="0.0.0.0"/>
Use Router as Default Gateway	<input checked="" type="checkbox"/>

[Fixed Host](#) 

If you check **Disabled** and click **Next**, then click **Apply**. The DHCP server function is disabled. Each PC in the LAN should assign a fixed IP address and set the PC's gateway to the ADSL Router.

If you check **DHCP Server** and click **Next**, you can configure parameters of the DHCP server including the IP pool (starting IP address and ending IP address), leased time for each assigned IP address, DNS IP address, and Gateway IP address. Those messages are sent to the DHCP client when

it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "Use Router as a DNS Server", the ADSL Router will find the IP address from the outside network automatically and forward it back to requesting PC in the LAN.

If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server, which will assign an IP address back to the DHCP client in the LAN. Click **Apply** to enable this function.

DHCP Server:

- **Disable:** Check to disable the ADSL Firewall Router from distributing IP Addresses to the local network.
If you check this selection, remember to specify a static IP address, subnet Mask, and DNS setting for each of your local computers. Be careful NOT to assign the same IP address to different computers.

- **DHCP Server:** Check to enable the ADSL Firewall Router to distribute IP Addresses, subnet mask and DNS setting to computers. Hence, the following fields will be activated.

Starting IP Address: Enter the starting address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.1.100**.

Ending IP Address: Enter the ending address of this local IP network address pool. The pool is a piece of continuous IP address segment. The default value is **192.168.1.199**

Defaul Lease Time: Value that expresses in second the validity time of assigned address.

Maximum Lease Time: Value that expresses in second the maximum validity time of assigned address.

Use Router as DNS Server: Each DNS request will be received by router and forwarder to DNS Server.

Primary/Secondary DNS Server Address: Insert here remote DSN server addresses, it will be forwarded to LAN hosts by DHCP server.

Use Router as Default Gateway: Specify here which address will be used by LAN hosts as Default Gateway

DHCP Relay: Selecting this option the DHCP request performed by LAN host will by delivered by a remote DHCP server passing through ADSL Firewal Router.

Is possibile to force a static IP assignment through function **Fixed Host:**

Fixed Host	
Create	
Name	<input type="text"/>
IP Address	<input type="text"/>
MAC Address	<input type="text" value="00:00:00:00:00:00"/> (MAC Address Format is 'xx:xx:xx:xx:xx:xx')
Maximum Lease Time	<input type="text"/>
<input type="button" value="Apply"/>	

3.6.3.2 WAN

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	<input checked="" type="radio"/> RFC 1483 Routed	<input type="radio"/> RFC 1483 Bridged
	<input type="radio"/> PPPoA Routed	<input type="radio"/> IPoA Routed
	<input type="radio"/> PPPoE Routed	Quick Start ▶
<input type="button" value="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.

It provides access control and billing functionality in a manner similar to dial-up services using PPP.

WAN Connection	
PPPoE Routed	
Description	PPPoE Routed
VPI	0
VCI	0
ATM Class	UBR
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	
Password	
Service Name	
IP Address	 (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast
MTU	1492
TCP MSS Clamp	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

- **Description:** User-definable name for the connection.
- **VPI/VCI:** Enter the information provided by your ISP.
- **ATM Class:** The Quality of Service for ATM layer.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing 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 will usually be 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 will provide you the information. Maximum input is 20 alphanumeric characters.
- **IP Address:** Specify an IP address allowed to logon and access the router's web server. Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.
- **Authentication Protocol Type:** Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.
- **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
- **Connect to Demand:** 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.
- **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.
- **RIP:** RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding mediaspecific headers) that IP will attempt to send through the interface.
- **TCP MSS Clamp:** It is enabled by default. All TCP traffic routed through the interface will be examined. If a TCP SYN (synchronize/start) segment is sent with a maximum segment size larger than the interface MTU (Maximum Transmission Unit), the MSS option will be rewritten in order to allow TCP traffic to pass through the interface without requiring fragmentation

Advanced Options (PPPoE)

- **LLC Header:** Selects encapsulation mode, true for using LLC or false for using VC-Mux.
- **Create Route:** This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to enabled, a route will be created which directs packets to the remote end of the PPP link.
- **Specific Route:** Specifies whether the route created when a PPP link comes up is a specific or default route. If set to enabled, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.
- **Subnet Mask:** sets the subnet mask used for the local IP interface connected to the PPP transport. If the value 0.0.0.0 is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.
- **Route Mask:** Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to 0.0.0.0, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.
- **MRU:** Maximum Receive Unit. This is negotiated during the LCP protocol stage.
- **Discover Primary / Secondary DNS:** This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is enabled.
- **Give DNS to Relay:** Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

- **Give DNS to Client:** Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.
- **Give DNS to DHCP Server:** Similar to the above, but gives the DNS server address to the DHCP server.
- **Discover Primary NBNS / Discover Secondary NBNS:** This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.
- **Discover Subnet Mask:** Specifies if the subnet mask given by IPCP negotiation process is to be used.
- **Give Subnet Mask To DHCP Server:** Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

RFC 1483 Routing or IPoA routed(RFC1577)

WAN Connection	
RFC 1483 Routed	
Description	<input type="text" value="RFC 1483 routed mode"/>
VPI	<input type="text" value="8"/>
VCI	<input type="text" value="35"/>
ATM Class	<input type="text" value="UBR"/>
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Encapsulation Method	<input type="text" value="LLC Bridged"/>
IP Assignment	<input checked="" type="radio"/> Obtain an IP address automatically via DHCP client
	<input type="radio"/> Use the following IP address
	IP Address <input type="text"/>
	Netmask <input type="text"/>
	Gateway <input type="text"/>
RIP	<input type="checkbox"/> RIP v1 <input type="checkbox"/> RIP v2 <input type="checkbox"/> RIP v2 Multicast
MTU	<input type="text" value="1500"/>
TCP MSS Clamp	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

- **Description:** Your description of this connection.
- **VPI and VCI:** Enter the information provided by your ISP.
- **ATM Class:** The Quality of Service for ATM layer.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **Encapsulation method:** Select the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP. (Only for RFC1483 Routed). Usually You have to select **LLC Routed**.
- **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.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding mediaspecific headers) that IP will attempt to send through the interface.
- **TCP MSS Clamp:** It is enabled by default. All TCP traffic routed through the interface will be examined. If a TCP SYN (synchronize/start) segment is sent with a maximum segment size larger than the interface MTU (Maximum Transmission Unit), the MSS option will be rewritten in order to allow TCP traffic to pass through the interface without requiring fragmentation

BRIDGE (PPPoE)

WAN Connection	
RFC 1483 Bridged	
Description	RFC 1483 bridged mode
VPI	8
VCI	35
ATM Class	UBR
Encapsulation Method	LLC Bridged
Acceptable Frame Type	acceptall
Filter Type	All
PVID for Untagged Frames	1
<input type="button" value="Apply"/>	

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the information provided by your ISP.
- **ATM Class:** The Quality of Service for ATM layer.
- **Encapsulation method:** Select the encapsulation format, this is provided by your ISP.
- **Acceptable Frame Type:** Specify what kind of traffic can through this connection, all traffic or only VLAN tagged.
- **Filter Type:** Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

- **PVID for Untagged Frames:** PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID. The valid value range for PVID is 1~4094.

3.6.3.2.2 DNS

DNS	
Parameters	
Obtain DNS Automatically	<input checked="" type="checkbox"/> Enable
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="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
Modulation	Multimode
Type de profil	MAIN
Activate Line	true
Coding Gain	auto
Tx Attenuation	Dmt_0DB
DSP Firmware Version	E.38.2.12
Connected	true
Operational Mode	G.Dmt
Annex Type	AnnexA
Upstream	320000
Downstream	4832000
CO Vendor	BCLA
Elapsed Time	0 day 4 hr 18 min 5 sec
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **Connect Mode:** There are three modes "ADSL", "ADSL2" and "ADSL2+" that user can select for this connection.
- **Modulation:** The default is Multimode; it will detect the ADSL line code, G.dmt, G.lite, and T1.413 automatically. But in some area, it cannot detect the ADSL line code well. At this time, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.
- **Activate Line:** Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of **Connect Mode**.
- **Coding Gain:** Select to Coding gain from 0 to 7 dB or leave to auto
- **Tx Attenuation:** Setting ADSL transmission gain, the value is between 0~12.
- **DSP Firmware Version:** DSP code version
- **Connected:** Display current ADSL line sync 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
- **CO Vendor:** Show your DSLAM Vendor
- **Elapsed Time:** Show ADSL activity time from last synchronization

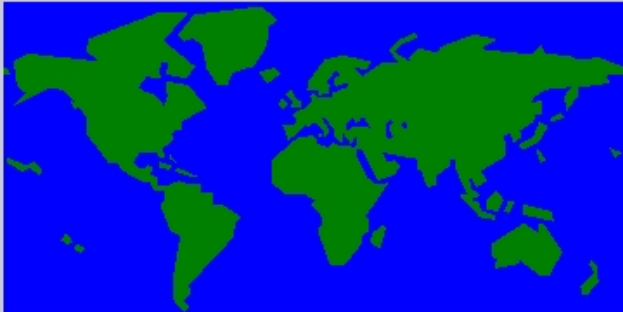


If the **ADSL Led** flashes periodically You have to force modulation. Click on **Configuration, WAN** then **ADSL**. On the combo-box **Connection Mode** please choose **ADSL**. Press **Apply** and then click on **Save Config to Flash**.

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

Time Zone	
Parameters	
Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Local Time Zone (+GMT Time)	(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▾
SNTP Server IP Address	192.43.244.18 128.138.140.44
	129.6.15.29 131.107.1.10
Daylight Saving	<input checked="" type="checkbox"/> Automatic
Resync Period	1440 minutes
	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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.

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

Resync Period (in minutes) is the periodic interval the router 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.

Remote Access	
You may temporarily permit remote administration of this network device	
Allow Access for	30 minutes.
<input type="button" value="Enable"/>	




If you wish to permanently enable remote access, choose a time period of 0 minutes. This setting cannot be saved into flash when timer set to zero.

If You wish to permanently enable remote access, You have to da a Virtual Server. Please check on this section.

3.6.3.3.3 Firmware Upgrade

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.



The screenshot shows a web interface titled "Firmware Upgrade". Below the title is a subtitle: "You may upgrade the system software on your network device". There is a text input field labeled "New Firmware Image" with a "Sfoglia..." (Browse) button next to it. Below the input field is an "Upgrade" button.

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 .afw 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.

Restore Configuration

Configuration File

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

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.

Restart Router

Hyper Link to <http://192.168.1.243:8081/>

Please wait for

seconds

3.6.3.3.5 Restart

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

Restart Router

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

Restart Router with	<input checked="" type="radio"/> Current Settings <input type="radio"/> Factory Default Settings
---------------------	-----------------------------------------------------------------------------------------------------

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

You may also reset your router to factory settings by 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	<i>admin</i>	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	<input type="password" value="*****"/>
Valid	true

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 SPI (Stateful Packet Inspection) 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 six items under the Firewall section: General Settings, Packet Filter, Intrusion Detection, MAC Address Filter, URL Filter 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. The Packet Filter is divided into two sections: Port Filters and Address Filters, used to filter packets based-on Applications (Port) or IP addresses.

There are four options when you enable the Firewall, they are:


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

Select either **High**, **Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall unfunctionality is the same for all levels; it is only the list of preset port filter that changes between each setting.

If you choose of the preset security levels and then add custom filters, you may temporarily disable the firewall and recover your custom filter settings by re-selecting the same security level.

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

3.6.3.4.1 General Settings

General Settings	
Firewall Security	
Security	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Policy	<input type="radio"/> All blocked/User-defined
	<input type="radio"/> High security level
	<input checked="" type="radio"/> Medium security level
	<input type="radio"/> Low security level
<p> <i>If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)</i></p>	
Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

Firewall Security: When you enable Firewall function, you can select one of the firewall security policies.

All blocked/User-defined: By default, all of traffic between WAN and LAN are blocked. You have to configure the type of traffic passed between WAN and LAN, please refer to Packet Filter below.

High, Medium and Low security level: By default, your system uses High, Medium and Low firewall security level between the WAN and LAN. For example, when you select High, the Port Filters of Packet Filter screen will be set automatically according to High security level settings. Look the table below for details:

Application	Protocol	Port Number		Firewall - High		Firewall - Medium		Firewall - Low	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
FTP(21)	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet(23)	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(119) (Network News Transfer Protocol)	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH(22)	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	NO	NO	NO	YES	NO	YES
ICQ (5190)	TCP(6)	5190	5190	NO	NO	NO	NO	YES	YES

3.6.3.4.2 Packet Filing

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, starting 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

Add TCP/UDP Filter
Add Raw IP Filter

Packet Filter Rules							
Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound	Edit	Delete
		Destination IP / Netmask		Destination port(s)	Outbound		
lei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
lei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
lei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
lei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		21 ~ 21	Allow		
lei_tnet	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		23 ~ 23	Allow		
lei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		25 ~ 25	Allow		
lei_pop3	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		110 ~ 110	Allow		

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, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

- **Add TCP/UDP Filter:** Click this button to add a new packet filter rule. After click, next figure will appear.

- **Add Raw IP Filter:** Click this button to add a new Protocol Filter.
- **Packet Filter Rules:** On this table, you see packet filter rules; you can click on **Edit** to modify rule or **Delete**

Packet Filter			
Add TCP/UDP Filter			
Rule Name	<input type="text"/>		
Time Schedule	Always On <input type="button" value="v"/>		
Source IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>
Destination IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>
Type	TCP <input type="button" value="v"/>		
Source Port	<input type="text" value="0"/>	-	<input type="text" value="65535"/>
Destination Port	<input type="text" value="0"/>	-	<input type="text" value="65535"/>
Inbound	Allow <input type="button" value="v"/>		
Outbound	Allow <input type="button" value="v"/>		
<input type="button" value="Apply"/> <input type="button" value="Return"/>			

- **Rule Name:** Insert rule name; rule name must be different
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section
- **Source IP Address(es) / Destination IP Address(es):** This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Selecting the **Subnet Mask** of the IP address range you wish to allow/block the traffic to or from; set IP address and Subnet Mask to **0.0.0.0** to inactive the Address-Filter rule.
- **Type:** Specify the packet type (UDP or TCP) that the rule will be applied to.
- **Source Port:** This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.
- **Destination Port:** This is the Port or Port Ranges that defines the application.
- **Inbound / Outbound:** Select **Allow** or **Block** the access to the Internet (“**Outbound**”) or from the Internet (“**Inbound**”).

Packet Filter			
Add TCP/UDP Filter			
Rule Name	<input type="text" value="Cindy_HTTP"/>		
Time Schedule	<input type="text" value="Always On"/> ▼		
Source IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>
Destination IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>
Type	<input type="text" value="TCP"/> ▼		
Source Port	<input type="text" value="0"/>	-	<input type="text" value="65535"/>
Destination Port	<input type="text" value="80"/>	-	<input type="text" value="80"/>
Inbound	<input type="text" value="Allow"/> ▼		
Outbound	<input type="text" value="Allow"/> ▼		
<input type="button" value="Apply"/> <input type="button" value="Return"/> ▶			

In this example, all TCP packets generated from every IP Address to every IP Address are allowed.

In this situation, you can surf on Internet and you can host a Web Server.

If you block Inbound, you can surf on Internet but you can't host a Web Server because all packets to TCP port 80 Inbound will be blocked.

Packet Filter	
Add Raw IP Filter	
Rule Name	<input type="text"/>
Time Schedule	<input type="text" value="Always On"/> ▼
Protocol Number	<input type="text"/>
Inbound	<input type="text" value="Allow"/> ▼
Outbound	<input type="text" value="Allow"/> ▼
<input type="button" value="Apply"/> <input type="button" value="Return"/> ▶	

In this window, you can decide to block or allow any protocol type.

- **Rule Name:** Insert rule name; rule name must be different
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section
- **Protocol Number:** Insert protocol number to allow or block
- **Inbound / Outbound:** Select **Allow** or **Block** the access to the Internet (“**Outbound**”) or from the Internet (“**Inbound**”).

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.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is false (disabled). Some attack types are denied immediately without using the Blacklist function, such as Land attack and Echo/CharGen scan.

Block Duration:

- **DoS Attack Block Duration:** This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include Ascend Kill and WinNuke. Default value is 1800 seconds.
- **Scan Attack Block Duration:** This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include X'mas scan, IMAP SYN/FIN scan and similar attempts. Default value is 86400 seconds.
- **Victim Protection Block Duration:** This is the duration for blocking Smurf attacks. Default value is 600 seconds.

Victim Protection: If enabled, IDS will block Smurf attack attempts. Default is false.

Max TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

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

Intrusion Detection	
Parameters	
Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Victim Protection Block Duration	<input type="text" value="600"/> seconds
Scan Attack Block Duration	<input type="text" value="86400"/> seconds
DOS Attack Block Duration	<input type="text" value="1800"/> seconds
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second
<input type="button" value="Apply"/>	
<input type="button" value="Clear Blacklist"/>	

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Dst Port: Destination Port

Src Port: Source Port
Dst IP: Destination IP

3.6.3.4.4 Url Filtering

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	
Configuration	
URL Filtering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block Mode	Disabled ▾
Keywords Filtering	<input type="checkbox"/> Enable Details ▶
Domains Filtering	<input type="checkbox"/> Enable Details ▶
	<input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict URL Features	<input type="checkbox"/> Block Java Applet
	<input type="checkbox"/> Block surfing by IP address

Enable/Disable: To enable or disable URL Filter feature.

Block Mode: A list of the modes that you can choose to check the URL filter rules. The default is set to **Disabled**.

- **Disabled:** No action will be performed by the Block Mode.
- **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.
- **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

Keywords Filtering

Create

Keyword	<input type="text"/>
<input type="button" value="Apply"/>	

Block WEB URLs which contain these keywords

Name	Keyword	
item0	abcde	Delete

Domains Filtering: This function checks the domain name only, not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, **both check-boxes must be checked**. 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.abc.com will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.sex.com or ww.sex.com will be dropped, because sex.com is in the forbidden list.

Domains Filtering

Domain Name	
Domain Name	<input type="text" value="sex"/>
Type	Forbidden Domain
<input type="button" value="Apply"/> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> Forbidden Domain Trusted Domain </div>	

Trusted Domain		
Name	Domain	
item1	abc	Delete
Forbidden Domain		
Name	Domain	
item0	sex	Delete

Restrict URL Features: This function enhances the restriction to your URL rules.

Example: Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites.

Andy selects both functions in the Domain Filtering and thinks that it will stop Bobby. But Bobby knows this function, Domain Filtering, ONLY disables all WEB traffic except for **Trusted Domain**,

BUT not its **IP address**. If this is the situation, **Block surfing by IP address** function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing other sites.

- **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage your system via standard HTTP protocol.
- **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping **Domains Filtering** function. Activates only and if Domain Filtering enabled.

3.6.3.4.5 Firewall Log

Firewall Log display log information of any unexpected action with your firewall settings.

Check the **Enable** box to activate the logs.

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

Firewall Log	
Event will be shown in the Status - Event Log	
Filtering Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
URL Blocking Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

3.6.3.5 VOIP

VoIP enables telephone calls through existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long distance telephone charges, but also toll-quality voice calls over the Internet.




*After completing VoIP configuration, remember to **apply** the changes, **SAVE CONFIG** and **restart** to activate your VoIP.*

There are six items within the **VoIP** section:

- **Wizard**
- **General Settings**
- **Phone Port**
- **PSTN Dial Plan**
- **VoIP Dial Plan**
- **Ring & Tone**

3.6.3.5.1 Wizard

This section provides easy setup for your VoIP service.

VoIP Wizard	
Voice QoS	
DSCP Marking	Best Effort <input type="button" value="v"/>
Setting for Phone Port 1 Select Profile <input type="button" value="▶"/>	
SIP Service Provider	FWD <input type="button" value="v"/>
Phone Number	<input type="text"/>
Authentication Username	<input type="text"/>
Authentication Password	<input type="text"/>
 <i>Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.</i>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> User-defined Profiles <input type="button" value="▶"/>	

Voice QoS


- **DSCP:** 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.

Setting for Phone Port 1

- **SIP Service Provider:** This section allows you to select the service provider. When the selection is done, respective parameters below are automatically displayed. If this section is empty, when You click on Apply You can manually setup the SIP accounts by entering SIP information to **User-defined Profile**. See below for details.
- **Phone Number:** This parameter holds the registration ID of the user within the SIP registrar.
- **Authentication Username:** Same as Phone Number.
- **Authentication Password:** This parameter holds the password used for authentication within SIP registrar.

3.6.3.5.2 General Settings

This section reflects and contains basic settings for the VoIP module from selected provider in the Wizard section. Fail to provide correct information will halt making calls out to the Internet.

General Settings	
SIP Device Parameters Advanced ▾	
SIP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Silence Suppression (VAD)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Echo Cancellation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
RTP Port	<input type="text" value="5100"/>
Region	<input type="text" value="Italy"/> ▾
Voice QoS,	<input type="text" value="Best Effort"/> ▾
Setting for Phone Port 1 Sync Now	
Registrar Address(or Hostname)	<input type="text"/>
Registrar Port	<input type="text" value="5060"/>
Expire	<input type="text" value="3600"/> seconds
User Domain/Realm	<input type="text"/> (If empty, it is the same as Registrar Address.)
Outbound Proxy Address	<input type="text"/> (If empty, it is the same as Registrar Address.)
Outbound Proxy Port	<input type="text" value="5060"/>
<p> Please note: VoIP configuration changes will only take effect when you use apply changes and select Sync Now for the relevant line, or when you apply changes, save configuration and restart the device.</p>	
<p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>	

SIP Device Parameters

- **SIP:** To use SIP as VoIP call signaling protocol. Default is set to **Disable**.
- **Silence Suppression (VAD):** Voice Activation Detection prevents transmitting the nature silence to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. Default is set to **Enable**.
- **Echo Cancellation:** G.168 echo canceller is an ITU-T standard. It is used for isolating the echo while you are on the phone. This helps you not to hear much of your own voice reflecting on the phone while you talk. Default is set to **Enable**.
- **RTP Port:** Provide the based value from the media (RTP) ports that are assigned for various endpoints and the different call sessions that may exist within an end-point. (Range from 5100 to 65535, default value is 5100)
- **Region:** This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.
- **Voice QoS, 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.

Setting for Phone Port 1

- **Registrar Address(or Hostname):** Indicate the SIP registrar IP address.
- **Registrar Port:** Specify the port of the SIP registrar on which it will listen for register requests from VoIP device.
- **Expire:** Expire time for the registration message sending.
- **User Domain/Realm:** Set different domain name for the SIP proxy server.
- **Outbound Proxy Address:** Indicate the SIP outbound proxy server IP address. This parameter is very useful when VoIP device is behind a NAT.




- **Outbound Proxy Port:** Specify the port of the SIP outbound proxy on which it will listen for messages.


How to register to SIP Server

- 1) In Wizard Section, select your SIP Service Provider and input information in the filed of *Phone Number, Authentication Username* and *Authentication Password*.
- 2) In Wizard Section, click Apply button to apply the settings.
- 3) In General Settings, make sure general SIP information are correctly inserted.
- 4) In General Settings, click Apply button to apply the settings.
- 5) In General Settings, click Synch Now button to register the account(s) with your SIP server.
- 6) In Status->VoIP Status check if the profile is registered.

3.6.3.5.3 Phone Ports

This section displays status and allows you to edit the account information of your Phones. Click **Edit** to update your phone information.

Phone Configuration				
Phone Port				
Index	Phone Number	Display Name	Registered	
1			unknown	Edit 

 *Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.*

Phone Port 1

Login Account Configuration

Phone Number	<input type="text"/>
Authentication Username	<input type="text"/>
Authentication Password	<input type="text"/>
Confirm Password	<input type="text"/>
Display Name	<input type="text"/>

Codec Preference

Priority 1	<input type="text" value="G.729"/>
Priority 2	<input type="text" value="PCMU (G.711 u-Law)"/>
Priority 3	<input type="text" value="PCMA (G.711 A-Law)"/>

Speed Dial

2#	<input type="text"/>
3#	<input type="text"/>
4#	<input type="text"/>
5#	<input type="text"/>
6#	<input type="text"/>
7#	<input type="text"/>
8#	<input type="text"/>
9#	<input type="text"/>

Volume Control

Microphone	-	#	#	#	#	#	#	#	+
Speaker	-	#	#	#	#	#	#	#	+

Login Account Configuration

- **Phone Number:** This parameter holds the registration ID of the user within the SIP registrar.
- **Authentication Username:** Same as Phone Number.
- **Authentication Password:** This parameter holds the password used for authentication within SIP registrar.
- **Confirm Password:** Re-enter the password for confirmation.
- **Display Name:** This parameter will be appeared on the Caller ID.

Codec Preference

Codec is known as Coder-Decoder used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority.

- **G.729:** It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption. 8kbps bandwidth is needed.
- **G.711 μ -LAW:** It is a basic non-compressed encoder and decoder technique. μ -LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample. 64kbps bandwidth is needed.
- **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. μ -LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample. 64kbps bandwidth is needed.
- **Non-used:** Only available in Priority 2 and 3. It is selected if codec is not to be used.



Codec priority is assigned in the order as G.729 > G.711 μ -LAW > G.711A-LAW

Speed Dial

It is for you to store frequently used telephone numbers which you can press number from 0 to 9 and the pound sign (#) to activate this function. For example, speed dial to phone number lists on 9, just press **9** then **#**. Your router will automatically call out to number listed on entry 9. Indicate remote user's IP address or domain name if this remote user does not register in the SIP server. If remote user is registered in the SIP server, this field is related to the SIP server's IP / Domain name.

For examples:

- If your friend Tommy gives you a SIP URL as sip: 98765@192.146.19.205 then you can fill in as 98765@192.146.19.2035.
- If your friend Robin gives you a SIP URL as sip: robin@iptel.org then you can fill in as robin@iptel.org.
- If your friend Greg gives you an IP address "201.226.61.56" only, then you can fill in as "201.226.61.56". In case, some of users may use DDNS, you can fill in with domain name as well.

Volume Control

Volume control helps you to adjust the voice quality of telephone to the best comfortable listening level.

Press "-", the minus sign, to reduce either microphone or/both speaker's level of your telephone. Press "+", the plus sign, to increase either microphone or/both speaker's level of your telephone.


3.6.3.5.4 PSTN Dial Plan

This section enables you to configure “VoIP with PSTN switching” on your system. You can define a range of dial plans to make regular call from VoIP switching to PSTN line. Prefix numbers is essential key to make a distinguishing between VoIP and Regular phone call. If actual numbers dialed matches with prefix number defined in this dial plan, the dialed number will be routed to the PSTN to make a regular call. Otherwise, the number will be routed to the VoIP networks.



In order to utilize this feature, you must have registered and connected to your SIP Server fist.


PSTN Dial Plan

Add Entry 

Dial Plan			
Prefix	Number of Digits	Action	

Add Dial Plan Entry

Parameters

Prefix	<input style="width: 90%;" type="text"/>
Number of Digits	<input style="width: 90%;" type="text"/> (15: at most)
Action	Dial with Prefix 

Prefix: Specify number(s) for switching to a PSTN call.

Number of Digits: Specify the total number of digits wish to dial out. Maximum digit number is 15.

Action: Specify a dialing method you wish to make PSTN call(s).

- **Dial with Prefix:** The dialed number *with* prefix will be sent call through the PSTN.
NOTE: The actual dialed number of valid digits length **requires** matching in the **Number of Digits** filed.
- **Dial without Prefix:** The dialed number will be sent call through the PSTN *without* prefix.
NOTE: The actual dialed number of valid digits length **requires** matching in the **Number of Digits** filed.
- **Dial at Timeout:** The dialed number will be sent call through the PSTN *with* the prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.
NOTE: The actual dialed number of valid digits length **MUST NOT** exceed in the **Number of Digits** filed.
- **Dial at Timeout no Prefix:** The dialed number will be sent call through the PSTN *without* prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.
NOTE: The actual dialed number of valid digits length **MUST NOT** exceed in the **Number of Digits** filed.



The following situation will make phone port 1 relay to PSTN line automatically.

- **Power down**
- **Internet Service fail**, i.e., lost of WAN IP Address
- **SIP service is not accessible**. This excludes when:
 - User manually disables Registration.
 - User inserts a wrong authentication username or password.
 - User dials a wrong SIP number.

PSTN Dial Plan Examples:

1) Dial with Prefix

Add Dial Plan Entry	
Parameters	
Prefix	<input type="text" value="01223"/>
Number of Digits	<input type="text" value="6"/> (0..15)
Action	Dial with Prefix <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

If you dial 01223 707070, number 01223707070 will be dialed out via FXO to make a regular phone call.

2) Dial without Prefix

Add Dial Plan Entry	
Parameters	
Prefix	<input type="text" value="9"/>
Number of Digits	<input type="text" value="3"/> (0..15)
Action	Dial without Prefix <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

If you dial 9102, the number 102 will be dialed out via FXO port to make a regular phone call.

3) Dial at Timeout

Add Dial Plan Entry	
Parameters	
Prefix	<input type="text" value="01223"/>
Number of Digits	<input type="text" value="6"/> (0..15)
Action	Dial at Timeout <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Return"/>	

If you only dial 01223 7070 and no more numbers, after the timeout activates, 012237070 will be dialed to make a regular call via FXO port.


Even though 0707 (only 4 digits) does not match with number of digits 6 defined in the filed, 7070 is still a valid phone number since it has not exceed 6 digits.

4) Dial at Timeout no Prefix

Add PSTN Dial Plan Entry

Parameters

Prefix	<input type="text" value="9"/>
Number of Digits	<input type="text" value="6"/> (0..15)
Action	Dial at Timeout no Prefix <input type="button" value="v"/>



If you only dial 9 7070 and no more numbers, after the timeout activates, 7070 will be dialed without prefix to make a regular call via FXO port.

Even though 0707 (only 4 digits) does not match with number of digits 6 defined in the file, 7070 is still a valid phone number since it has not exceed 6 digits

3.6.3.5.5 VoIP Dial Plan

This section helps you to make a telephony number dialed as making a regular call via VoIP. You no longer need to memorize a long dial string of number for making a VoIP call.

VoIP Dial Plan	
Parameters	
Special Digit Sequences	<input type="checkbox"/> *69 Return Call
	<input type="checkbox"/> *20 enable 'Don't Disturb' / *80 disable 'Don't Disturb'
	<input checked="" type="checkbox"/> *90x. Blind Call Transfer
	<input checked="" type="checkbox"/> x# Speed Dial (x: 2..9)
	<input checked="" type="checkbox"/> ## Redial
<input type="button" value="Apply"/> <input type="button" value="Test"/>	
Dial Plan Rules List	
Rule Name	
<input type="button" value="Add"/>	

Parameters

A listed of special dial feature comes handy when you have a miss call or need to transfer a call to a third party. Details please refer to the section **Special dial codes** below.

- ***69 (Return Call):** Dial *69 to return the last missed call. It is only available for SIP call(s).
- ***20 (Do not Disturb ON):** Dial *20 to set the No Disturb on. Your phone will not ring if someone calls.
- ***80 (Do not Disturb OFF):** Dial *80 to set the No Disturb off. Your will be able to hear ring tone when someone calls.
- ***90x (Blind Call Transfer):** Dial *90 + phone-number to translate a call to a third party. This feature is enabled by default.
- **x# Speed Dial (x:2..9):** Refer to **Phone Port** section in the Web GUI. Set up your Speed Dial phone book first before accessing the Speed Dial feature. It is enabled by default.
- **## Redial:** Press ## to redial the latest number you dialed. This feature is enabled by default.

Note: Refer to **Special Dial Code** section in this Manual for more details.

Test: Test displays the actual number will be called out to the VoIP service.

Click **Apply** to apply the settings.

Dial Plan Rules List

Click **Add** to create and define VoIP dial-plan rule(s).

Create Rule

Parameters

Prefix Processing	<input type="radio"/> Prepend <input style="width: 100px;" type="text"/> unconditionally
	<input type="radio"/> If prefix is <input style="width: 100px;" type="text"/> , delete it.
	<input type="radio"/> If prefix is <input style="width: 100px;" type="text"/> , replace with <input style="width: 100px;" type="text"/>
	<input checked="" type="radio"/> No prefix
Main Digit Sequence	<input style="width: 150px;" type="text"/>

Examples:

x.	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3 digit number only between 0 and 9. Total length is 3. No common needed (.)
xxxx.	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum Length is 16.
123x.	Any number (0-9) starting with 123. Maximum length is 16.
{124}x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
{1-3}x.	Any number(0-9) starting with number 1 to 3. Maximum length is 16.
9{4-6}8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.

Prefix Processing:

Prepend xxx unconditionally: xxx number is appended unconditionally to the front of the dialing number when making a call.

If Prefix is xxx, delete it: Prefix xxx is removed from the dialing numbers before making a call.

If Prefix is xxx, replace with: Prefix xxx is appended to the front of the dialing numbers when making a call.

No prefix: No prefix is appended to the front of the dialing numbers. It is set as in default settings.

Main Digit Sequence:

x: Any numeric number between 0 and 9.

. (period): Repeat numeric number(s) between 0 and 9.

Here are some Examples for your reference:

Main Digit Sequence Lists:	Description
x.	Any digit number between 0 and 9 in variable length. Maximum length is 16.
xxx	Any 3 digit number only between 0 and 9. Total length is 3. Note: No period is needed (.)
xxx.	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length is 16.
123x.	Any number (0-9) starting with 123. Maximum length is 16.
[x...x]x. For example: [124]x.	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[x-x]x. For example: [1-3]x.	Any number (0-9) starting with number 1 to 3. Maximum length is 16.
x[x-x]x. For example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.

3.6.3.5.6 Ring & Tone

This section allows advanced user to change the existing or newly defined parameters for the various ring tones (dial tone, busy tone, answer tone and etc.)

Ring & Tone Configuration							
Country Specific Ring & Tone							
Region	UK <input type="button" value="v"/>						
Ring Parameters							
	On 1	Off 1	On 2	Off 2	On 3	Off 3	
Ring Cadence (in ms)	<input type="text" value="400"/>	<input type="text" value="200"/>	<input type="text" value="400"/>	<input type="text" value="2000"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	
Tone Parameters							

Country Specific Ring & Tone

Region: Select a country ring-tone, from the drop-down list, where you are located. This VoIP router provides default parameter of ring tones according to different countries. The ring-tone parameters are automatically displayed after entering a specific country. If your country is not in the list, you may manually create ring-tone parameters.

Ring Parameters

Ring Cadence (in ms): Ring cadence is defined by three fields, Frequency: On Time1, Off Time1, On Time2, Off Time2 and On Time3, Off Time3. Frequency is specified in Hertz. Time is given in milliseconds.

Tone Parameters

You may need to check with your local telephone service provider for such information. Also, it is recommended that this option be configured by an advanced user, unless you are instructed to do so.

Click **Apply** to apply the settings.

Special dial codes

The following table lists the special dial codes that are built-in to the system:

Option	Description
<p>Flash-hook (Wireless Router with LINE port only)</p>	<p>Switch to PSTN line</p> <p>Note: A quick press of the hook. On some phones a button is provided which provides Flash-hook functionality. The button is marked "FLASH" or "RECALL".</p>
<p>*69</p>	<p>Return the last missed call for SIP service only</p> <p>Note: Entering this on a phone will call the last number which made a call to the phone. For example A makes a call to B, but hangs up before B answers. If B enters *69, A will be called.</p>
<p>##</p>	<p>Last number redial</p>
<p>*20</p>	<p>Set do not disturb on</p> <p>Note: It is possible to set a Do-Not-Disturb feature on a phone such that any phone which calls the phone will receive an engaged tone and the phone called will not ring. For example, B enters *20 and hangs up. A makes a call to B, and receives the engaged tone and phone B does not ring.</p>
<p>*80</p>	<p>Set do not disturb off</p>
<p>*74<x><number>#</p>	<p>Set the number for Speed dial code 'x', where 'x' is a number between 2 and 9.</p> <p>Note: Where <x> is a number between 2 and 9, and <number> is the number to dial. The code needed to dial a speedial from a phone connected to a VoIP Router is: <x>#, where <x> is a number between 2 and 9.</p> <p>The settings will infect to your setting in Speed Dial on WEB GUI.</p>
<p>*90<phone-number></p>	<p>Set the number for performing Blind Call Transfer, where <phone-number> is the number that you wish to transfer the call to. It's for SIP service only.</p> <p>Note: In Blind Call Transfer, you have a call in progress (incoming or outgoing) and decide you wish to transfer the call to another phone. To transfer the call, perform the following steps:</p> <ol style="list-style-type: none"> 1. Hook-flash to get a dial tone.



	<p>2. Dial *90<phone-number> (e.g. *907401), there will be a confirmation tone then hang up. The other end will hear ring back and the called third-party phone will ring. When the third-party phone is picked up the two calls will be connected.</p> <p>If the third-party phone does not answer then the caller being transferred can hang up to cancel the connect attempt.</p>
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.6.3.6 QoS

QoS function helps you to control your network traffic for each application from LAN (Ethernet) to WAN (Internet). It facilitates you to control the different quality and speed of through put for each application when the system is running with full loading of upstream. You can find two items under the **QoS** section: **Prioritization** and **IP Throttling** (bandwidth management).

3.6.3.6.1 Prioritization

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

- **High**
- **Normal** (The default is normal priority for all of traffic without setting).
- **Low**

The trigger of check can base on IP protocol, port number and address.

And the balance of utilization of each priorities are High(60%), Normal(30%) and Low(10%).

Prioritization						
Configuration (from LAN to WAN packet)						
Application	Time Schedule	Priority	Protocol	Source Port	Source IP Address Range ('0.0.0.0' means Any)	DSCP Marking
				Destination Port	Destination IP Address Range ('0.0.0.0' means Any)	
PPTP	Always On	High	GRE	none	0.0.0.0 ~ 0.0.0.0	Gold service (L)
				none	0.0.0.0 ~ 0.0.0.0	
VoIP	Always On	High	any	0 ~ 0	192.168.1.1 ~ 192.168.1.1	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Restricted	TimeSlot1	Low	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	

Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy.

Priority: The priority given to each policy/application. Its default setting is set to High; you may adjust this setting to fit your policy/application.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

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

DSCP Mapping Table	
(Wireless) ADSL Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

3.6.3.6.2 Outbound IP Throttling (LAN to WAN)

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

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Application	Time Schedule	Protocol	Source Port		Source IP Address Range (0.0.0.0 means Any)		Rate Limit
			Destination Port	Destination IP Address Range (0.0.0.0 means Any)			
PPTP	Always On	gre	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	6 *32 (kbps)
VoIP	Always On	any	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	4 *32 (kbps)
Restricted	TimeSlot1	any	0 ~ 0	0	192.168.1.100	~ 192.168.1.100	5 *32 (kbps)
Others	TimeSlot1	any	0 ~ 0	0	192.168.1.2	~ 192.168.1.5	14 *32 (kbps)
	Always On	any	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)

Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Outbound Rate Limit: To limit the speed of outbound traffic

3.6.3.6.3 Inbound IP Throttling (WAN to LAN)

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

Inbound IP Throttling						
Configuration (from WAN to LAN packet)						
Application	Time Schedule	Protocol	Source Port	Source IP Address Range (0.0.0.0 means Any)		Rate Limit
			Destination Port	Destination IP Address Range (0.0.0.0 means Any)		
Restricted	TimeSlot1	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	64 *32 (kbps)
			0 ~ 0	192.168.1.100	~ 192.168.1.100	
	Always On	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
			0 ~ 0	0.0.0.0	~ 0.0.0.0	
	Always On	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
			0 ~ 0	0.0.0.0	~ 0.0.0.0	
	Always On	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
			0 ~ 0	0.0.0.0	~ 0.0.0.0	
	Always On	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
			0 ~ 0	0.0.0.0	~ 0.0.0.0	
	Always On	any	0 ~ 0	0.0.0.0	~ 0.0.0.0	1 *32 (kbps)
			0 ~ 0	0.0.0.0	~ 0.0.0.0	

Application: A user-define description to identify this new policy/application.

Time Schedule: Scheduling your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Source Port: The source port of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

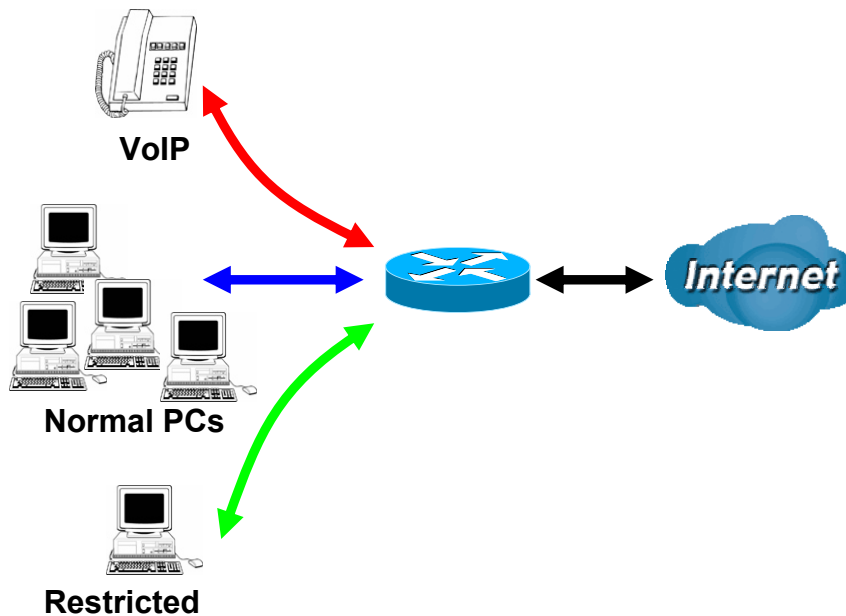
Source IP Address Range: The source IP address or range of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Inbound Rate Limit: To limit the speed of for inbound traffic.

3.6.3.6.4 Example: QoS for your Network

Connection Diagram

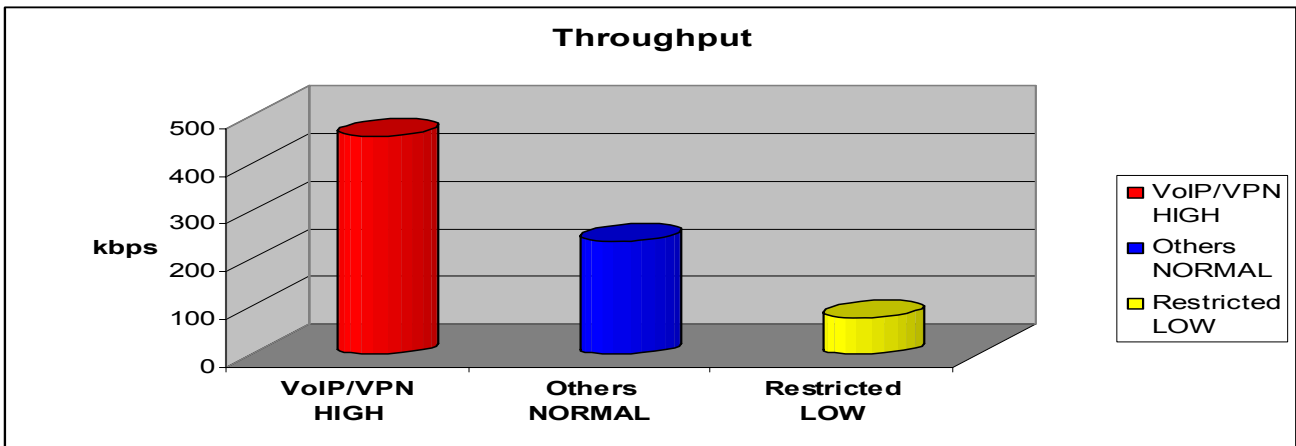


Information and Settings

Upstream: 928 kbps
Downstream: 8 Mbps

VoIP User : 192.168.1.1
Normal Users : 192.168.1.2~192.168.1.5
Restricted User: 192.168.1.100

Prioritization						
Configuration (from LAN to WAN packet)						
Application	Time Schedule	Priority	Protocol	Source Port	Source IP Address Range ('0.0.0.0' means Any)	DSCP Marking
				Destination Port	Destination IP Address Range ('0.0.0.0' means Any)	
PPTP	Always On	High	GRE	none	0.0.0.0 ~ 0.0.0.0	Gold service (L)
				none	0.0.0.0 ~ 0.0.0.0	
VoIP	Always On	High	any	0 ~ 0	192.168.1.1 ~ 192.168.1.1	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Restricted	TimeSlot1	Low	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	



Mission-critical application

The mission-critical application must be sent out smoothly without any dropping. Set priority as high level for preventing any other applications to saturate the bandwidth.

Voice 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.

VoIP	Always On	High	any	0 ~ 0	192.168.1.1 ~ 192.168.1.1	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	

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

Restricted Application

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.

Restricted	TimeSlot1	Low	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	Gold service (L)
				0 ~ 0	0.0.0.0 ~ 0.0.0.0	

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

Advanced setting by using IP throttling

With IP throttling you can specify more detail for allocating bandwidth; even the applications are located in the same level.

- Upstream: 928kbps (29*32kbps)
- Mission-critical Application: 192kbps (6*32kbps)
- Voice Application: 128kbps (4*32kbps)
- Restricted Application: 160kbps (5*32kbps)
- Other Applications: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Application	Time Schedule	Protocol	Source Port	Source IP Address Range (‘0.0.0.0’ means Any)	Rate Limit
			Destination Port	Destination IP Address Range (‘0.0.0.0’ means Any)	
PPTP	Always On	gre	0 ~ 0	0.0.0.0 ~ 0.0.0.0	6 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
VoIP	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Restricted	TimeSlot1	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	5 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	
Others	TimeSlot1	any	0 ~ 0	192.168.1.2 ~ 192.168.1.5	14 *32 (kbps)
			0 ~ 0	0.0.0.0 ~ 0.0.0.0	

Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below help you to limit bandwidth for the restricted application.

Inbound IP Throttling

Configuration (from WAN to LAN packet)

Application	Time Schedule	Protocol	Source Port	Source IP Address Range (‘0.0.0.0’ means Any)	Rate Limit
			Destination Port	Destination IP Address Range (‘0.0.0.0’ means Any)	
Restricted	TimeSlot1	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	64 *32 (kbps)
			0 ~ 0	192.168.1.100 ~ 192.168.1.100	

3.6.3.7 Virtual Server

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

Virtual Server (Port Forwarding)

Add Virtual Server ▶
Edit DMZ Host ▶
Edit One-to-one NAT ▶

Virtual Server Table					
Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address

If you click on Add Virtual Server, you see the follow window

Add Virtual Server in 'ipwan' IP Interface

Virtual Server Entry

Time Schedule	Always On ▼
Application Helper ▶	<input type="text"/>
Protocol	tcp ▼
External Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Redirect Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Internal IP Address Candidates ▶	<input type="text"/>

Time Schedule: A self-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Application: Users-define description to identify this entry or click to select existing predefined rules. Click the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application.

Edit DMZ Host

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

Edit DMZ Host

DMZ Host for 'ipwan' IP Interface

Enabled Disabled

Internal IP Address [Candidates](#)

[Return](#)

- **Disabled:** As set in default setting, it disables the DMZ function.
- **Enabled:** It activates your DMZ function.

Internal IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

One-to-One NAT (Network Address Translation)

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

Global IP Pool in 'ipwan' IP interface

Global Address Pool

NAT Type Disable Public to Private Subnet Public to DMZ Zone

Global IP Addresses

<input checked="" type="radio"/> Subnet	IP Address	<input type="text"/>	Netmask	<input type="text"/>
<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>

[Return](#)

NAT Type: Select desired NAT type. As set in default setting, it disables the One-to-One NAT function.

Global IP Address:

Subnet: The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.

IP Range: The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

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

Check to **Add Entry** create a new One-to-One NAT rule:

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry

Time Schedule	Always On <input type="button" value="v"/>
Application Helper <input type="button" value="v"/>	<input type="text"/>
Protocol	tcp <input type="button" value="v"/>
Global IP	<input type="text"/>
External Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Redirect Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Internal IP Address Candidates <input type="button" value="v"/>	<input type="text"/>

[Return](#)

Time Schedule: A self-defined time period to enable your virtual server. You may specify a time schedule or Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

Application: Users-defined description to identify this entry or click to select existing predefined rules. Click the Radio button to select the rule; Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP;

Global IP: Define a public/ WAN IP address for this Application to use. This Global IP address must be defined in the **Global IP Address**.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

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

3.6.3.8 TIME SCHEDULE

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock onboard; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. Your router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.

Time Schedule						
Time Slot						
ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Edit	Clear
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Edit	Clear
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Edit	Clear
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Edit	Clear
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Edit	Clear
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Edit	Clear
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Edit	Clear
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Edit	Clear
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Edit	Clear
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Edit	Clear
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Edit	Clear
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Edit	Clear
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Edit	Clear
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Edit	Clear

Edit a Time Slot

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

A detailed setting of this Time Slot will be shown.

Time Schedule	
Edit Time Slot	
ID	1
Name	<input type="text" value="TimeSlot1"/>
Day	<input type="checkbox"/> Sun. <input checked="" type="checkbox"/> Mon. <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri. <input type="checkbox"/> Sat.
Start Time	08 : 00
End Time	18 : 00
<input type="button" value="Apply"/>	

ID: This is the index of the time slot.



Name: A user-define description to identify this time portfolio.

Day: The default is set from Monday through Friday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

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

Delete a Time Slot

Click **Clear** to delete the existing Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

3.6.3.9 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.

There are four items within the **Advanced** section: **Static Route**, **Dynamic DNS**, **Checking Email**, **Device Management** and **IGMP**.

3.6.3.9.1 Static Route

Click on **Routing Table** and then choose **Create Route** add a routing table.

Static Route			
Create			
Destination	<input type="text"/>		
Netmask	<input type="text"/>		
via Gateway	<input type="text"/>	or Interface	<input type="text" value="v"/>
Cost	<input type="text" value="1"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

Destination: This is the destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses based on above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

3.6.3.9.2 Dynamic DNS

Dynamic DNS	
Parameters	
Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Dynamic DNS Server	<input type="text" value="www.dyndns.org (dynamic)"/>
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	<input type="text" value="25"/> <input type="text" value="Day(s)"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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 Server: 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.

3.6.3.9.3 Check Emails

Click **Checking Email** to get the below figure then check the “Enable” button to access the service.

Check Email	
Parameters	
Check Email	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Account Name	<input type="text"/>
Password	<input type="text"/>
POP3 Mail Server	<input type="text"/>
Period	<input type="text" value="60"/> minutes
Dial-out for Checking Emails	<input type="checkbox"/> Automatic
<input type="button" value="Apply"/>	

This function allows you to have the router check your POP3 mailbox for new Email messages.

The **Mail** LED on your router will light when it detects new messages waiting for download. You may also view the status of this function using the **Status – Email Checking** section of the web interface, which also provides details on the number of new messages waiting. See the **Status** section of this manual for more information.

- **Disable:** Check to disable the router’s Email checking function.
- **Enable:** Check to enable the routers Emailing checking function. The following fields will be activated and required:

Account Name: Enter the name (login) of the POP3 account you wish to check.. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account’s password.

POP3 Mail Server: Enter your (POP) mail server name. Your Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Interval: Enter the value in minutes between periodic mail checks.

Automatically dial-out for checking emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time online.

3.6.3.9.4 Device Management

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

Device Management			
Device Host Name			
Host Name	<input type="text" value="home.gateway"/>		
Embedded Web Server			
* HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)	
Management IP Address	<input type="text" value="0.0.0.0"/>	(‘0.0.0.0’ means Any)	
Expire to auto-logout	<input type="text" value="180"/>	seconds	
Universal Plug and Play (UPnP)			
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
* UPnP Port	<input type="text" value="2800"/>		
SNMP Access Control			
SNMP V1 and V2			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write	IP Address	<input type="text"/>
* : This setting will become effective after you save to flash and restart the router.			
<input type="button" value="Apply"/>			

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.

Management IP Address: You may specify an IP address allowed to logon and access the router’s web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user’s configuration session.

Universal Plug’n’Play

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.

SNMP Access Control

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

3.6.3.9.5 IGMP

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

IGMP	
Parameters	
IGMP Forwarding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Apply"/>	

IGMP Forwarding: Accepting multicast packet. Default is set to **Enable**.

IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions.

Default is set to **Enable**

3.6.3.9.6 VLAN

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

VLAN Bridge					
Parameters					
Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet ,wireless ,wireless_wds ,	Edit ▶	
Create VLAN ▶					

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Advanced VLAN Setup Example (Triply Play)

VLAN_data:

Ethernet Port 1, Wireless and Wireless WDS are reserving for Internet
 - On Ethernet port 1 I also need VC 0/40 bridged.

VLAN_Vedio

Ethernet ports: 2, 3 and 4:

- 0/33 Bi-directional IP
- 0/34 Video
- 0/35 Video
- 0/36 Video Subscriber Services (EPG, EAS, etc.)
- 0/37 Video
- 0/38 Video
- 0/39 Spare

Step 1: Setup Member Ports

Go to **Configuration → LAN → Bridge Interface.**

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

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4) Please uncheck P2, P3, P4 from Ethernet VLAN Port first.

Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4

Bridge Interface	
Parameters	
Bridge Interface	VLAN Port
Ethernet	<input checked="" type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Ethernet1	<input type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4
Ethernet2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Ethernet3	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
Device Management	
Management Interface	<input checked="" type="radio"/> Ethernet
<input type="button" value="Apply"/>	

Step 2: Create WAN Interface

Go to **Configuration → WAN → ISP**

wanlink is the factory default WAN interface which in service for data/internet access. If your ISP uses this access protocol, click **Edit** to input other parameters if needed. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

From the example, 0/40 is used for data/internet and assumes PPPoE is used; click the **Edit** to change the VPI/VCI to 0/40.

Click **Create** to setup up additional WAN interface for video applications. Total of 8 VLAN is support; therefore, only 8 WAN interfaces can be created in the table.

WAN Connection						
WAN Services Table						
Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	QuickStart	0	40	Edit 	Change
Create 						

From the example, PVC 0/33 to 0/39 is assigned for video using 1483 Bridged mode. Check **RFC 1483 Bridged** and click **Next** to continue the setup.

ISP		
Please select the type of service you wish to create		
ATM	<input type="radio"/> RFC 1483 Routed	<input checked="" type="radio"/> RFC 1483 Bridged
	<input type="radio"/> PPPoA Routed	<input type="radio"/> IPoA Routed
	<input type="radio"/> PPPoE Routed	Quick Start
<input type="button" value="Next"/>		

Spaces next to VPI and VCI, type 0 and 33 in respectively. Select appropriate ATM Class, Encapsulation Method, Acceptable Frame Type, Filter Type and PVID for Untagged Frames.

WAN Connection	
RFC 1483 Bridged	
Description	RFC 1483 bridged mode
VPI	0
VCI	34
ATM Class	UBR <input type="button" value="v"/>
Encapsulation Method	LLC Bridged <input type="button" value="v"/>
Acceptable Frame Type	ALL <input type="button" value="v"/>
Filter Type	All <input type="button" value="v"/>
PVID for Untagged Frames	1
<input type="button" value="Apply"/>	

VPI and VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify what kind of traffic can through this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID.

From the example, VPI and VCI only section need to be filled-in and just leave the rest as is. Repeat the same procedure by clicking **Create** → select **RFC1483 Bridged** → fill-in the rest of PVC 0/34 to 0/39.

WAN Connection						
WAN Services Table						
Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	QuickStart	0	40	Edit <input type="button" value="▶"/>	Change <input type="button" value="▶"/>
rfc1483-0	RFC 1483 bridged mode	WebAdmin	0	33	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-1	RFC 1483 bridged mode	WebAdmin	0	34	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-2	RFC 1483 bridged mode	WebAdmin	0	35	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-3	RFC 1483 bridged mode	WebAdmin	0	36	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-4	RFC 1483 bridged mode	WebAdmin	0	37	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-5	RFC 1483 bridged mode	WebAdmin	0	38	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>
rfc1483-6	RFC 1483 bridged mode	WebAdmin	0	39	Edit <input type="button" value="▶"/>	Delete <input type="button" value="▶"/>

Step 3: Setup VLAN Service

Go to **Configuration → Advanced → VLAN Bridge**

DefaultVlan lists all member ports. It is necessary to group specific member ports for each VLAN.

From the example, two VLAN groups are requested: Data and Video.

To create another VLAN group for Video by clicking **Create VLAN**.

VLAN Bridge					
Parameters					
Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit	
Create VLAN					

Given a name and ID (PVID) to identify the Video group. The valid value range for PVID is 1 ~ 4094.

From the example:

VLAN untagged ports for Data/Internet: ethernet, wireless and wireless_wds.

VLAN untagged ports for Video: ethernet1, rfc-1483-0 ~ rfc-1483-6.

Click **Apply** to made change effective immediately.

Create VLAN			
Parameters			
VLAN Name	<input type="text" value="Video_VLAN"/>	VLAN ID	<input type="text" value="2"/> (2~4094)
Tagged Member Port(s)	<input type="checkbox"/> ethernet <input type="checkbox"/> wireless <input type="checkbox"/> wireless_wds <input type="checkbox"/> ethernet1 <input type="checkbox"/> rfc1483-0 <input type="checkbox"/> rfc1483-1 <input type="checkbox"/> rfc1483-2 <input type="checkbox"/> rfc1483-3 <input type="checkbox"/> rfc1483-4 <input type="checkbox"/> rfc1483-5 <input type="checkbox"/> rfc1483-6		
Untagged Member Port(s)	<input type="checkbox"/> ethernet <input type="checkbox"/> wireless <input type="checkbox"/> wireless_wds <input checked="" type="checkbox"/> ethernet1 <input checked="" type="checkbox"/> rfc1483-0 <input checked="" type="checkbox"/> rfc1483-1 <input checked="" type="checkbox"/> rfc1483-2 <input checked="" type="checkbox"/> rfc1483-3 <input checked="" type="checkbox"/> rfc1483-4 <input checked="" type="checkbox"/> rfc1483-5 <input checked="" type="checkbox"/> rfc1483-6		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> Return			

VLAN Bridge					
Parameters					
Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,	Edit	
Video_VLAN	2	None	ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit	Delete
Create VLAN					

Mapping the **VLAN Bridge** with **Bridge Interface** created in Step1, you will see the conformable relationship in these two screenshots.

3.6.4 Save Config To Flash

After configuring this network router, you have to save all of the configuration parameters to FLASH.

Save Config to FLASH

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to FLASH chips.

3.6.5 Logout

To exit the website, choose Logout to exit completely. Please ensure that you have save the configuration settings before logout.

Chapter 4

Troubleshooting

What is VoIP?

Question	Answer
What is VoIP?	VoIP stands for 'V'oice 'o'ver 'I'nternet 'P'rotocol. As the term says VoIP tries to let go voice (mainly human) through IP packets and, in definitive through Internet. VoIP can use accelerating hardware to achieve this purpose and can also be used in a PC environment.

What is VoIP?

Question	Answer
<p>What is VoIP?</p>	<p>The past: More than 30 years ago Internet didn't exist. Interactive communications were only made by telephone at PSTN line cost. Data exchange was expensive (for a long distance) and no one had been thinking to video interactions (there was only television that is not interactive, as known).</p> <p>Yesterday: Few years ago we saw appearing some interesting things: PCs to large masses, new technologies to communicate like cellular phones and finally the great net: Internet; people begun to communicate with new services like email, chat, etc. and business reborned with the web allowing people buy with a "click".</p> <p>Today: Today we can see a real revolution in communication world: everybody begins to use PCs and Internet for job and free time to communicate each other, to exchange data (like images, sounds, documents) and, sometimes, to talk each other using applications like Netmeeting or Internet Phone. Particularly starts to diffusing a common idea that could be the future and that can allow real-time vocal communication: VoIP.</p> <p>The future: We cannot know what is the future, but we can try to image it with many computers, Internet almost everywhere at high speed and people talking (audio and video) in a real time fashion. We only need to know what will be the means to do this: UMTS, VoIP (with video extension) or other? Anyway we can notice that Internet has grown very much in the last years, it is free (at least as international means) and could be the right communication media for future.</p>

What is How does it work?

Question	Answer
<p>What is How does it work?</p>	<p>Many years ago we discovered that sending a signal to a remote destination could have be done also in a digital fashion: before sending it we have to digitalize it with an ADC (analog to digital converter), transmit it, and at the end transform it again in analog format with DAC (digital to analog converter) to use it.</p> <p>VoIP works like that, digitalizing voice in data packets, sending them and reconverting them in voice at destination.</p> <p>Digital format can be better controlled: we can compress it, route it, convert it to a new better format, and so on; also we saw that digital signal is more noise tolerant than the analog one (see GSM vs TACS).</p> <p>TCP/IP networks are made of IP packets containing a header (to control communication) and a payload to transport data: VoIP use it to go across the network and come to destination.</p> <p>Voice (source) -- ADC ---- Internet --- DAC -- Voice (dest)</p>

What is VoIP What is the advantages using VoIP rather PSTN?

Question	Answer
<p>What is the advantages using VoIP rather PSTN?</p>	<p>When you are using PSTN line, you typically pay for time used to a PSTN line manager company: more time you stay at phone and more you'll pay. In addition you couldn't talk with other that one person at a time.</p> <p>In opposite with VoIP mechanism you can talk all the time with every person you want (the needed is that other person is also connected to Internet at the same time), as far as you want (money independent) and, in addition, you can talk with many people at the same time.</p> <p>If you're still not persuaded you can consider that, at the same time, you can exchange data with people are you talking with, sending images, graphs and videos.</p>

Then, why everybody doesn't use it yet?

Question	Answer
Then, why everybody doesn't use it yet?	Unfortunately we have to report some problem with the integration between VoIP architecture and Internet. As you can easy imagine, voice data communication must be a real time stream (you couldn't speak, wait for many seconds, then hear other side answering): this is in contrast with the Internet heterogeneous architecture that can be made of many routers (machines that route packets), about 20-30 or more and can have a very high round trip time (RTT), so we need to modify something to get it properly working. However with the new packets compression technologies we can overcome the problem.

What is SIP?

Question	Answer
What is SIP?	The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. Examples of multimedia sessions include multimedia conferences, distance learning, and Internet telephony.

Does VoIPMaster 260W support H.323?

Question	Answer
Does VoIPMaster 260W support H.323?	No, VoIPMaster 260W supports SIP for session initiation.

Does my computer have to be turned on?

Question	Answer
Does my computer have to be turned on ?	I f you finished the VoIP setting with the VoIPMaster 260W and you can use the phone to dial directly. So your computer does not need to be always on.

How to make a call with remove IP address only, not through SIP server?

Question	Answer
How to make a call with remove IP address only, not through SIP server?	You have to put directly IP address.

Which VoIP Providers can support the VoIPMaster 260W?

Question	Answer
Which VoIP Providers can support the VoIPMaster 260W?	Please check on Appendix C.

Can I use the DDNS to make a voice connection ?

Question	Answer
Can I use the DDNS to make a voice connection ?	Yes, You can use the DDNS domain name to make a P2P voice connection. Please input it in the phonebook and use speed dial to call.

What is STUN?

Question	Answer
What is STUN?	STUN (Simple Traversal of UDP through NATs (Network Address Translation)) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

APPENDIX A

Specifications

Technical Features	
Protocols	IP, NAT, PPTP, ARP, ICMP, DHCP(server, relay and client), RIP1/2 , SNMP, SNTTP client, UPnP, Telnet server, IGMP
LAN port	RJ-45, 4 10/100Base-T ports with autonegotiation and autopolarity
WAN port	RJ-11 (1 port ADSL/ADSL2/ADSL2+)
Console port	RS232 DB9(9600,8,N,1,N)
External buttons	Reset, Power On/Off
LED Indicators	Power, System, Lan (4), PPP ed ADSL , Wireless, VoIP, Line, Phone
Wireless	IEEE802.11g / IEEE802.11b
Standard ADSL/ADSL2/ADSL2+ 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)
ADSL/ADSL2/ADSL2+ Protocols	RFC2364(PPPoA), RFC2516(PPPoE), RFC1577 e RFC1483
ATM	ATM AAL2/AAL5 and ATM service class : CBR, UBR, VBRrt, VBR, ATM Forum UNI 3.0, 3.1 and 4.0
Firewall	Intrusion Detection, DoS, Port Filters, URL Blocking MAC Blocking
VLAN	Port Base VLAN
QoS	WAN-LAN e LAN-WAN
VoIP	1 FXS 1 FXO
Input Power	12V DC @ 1A
Power Consumption	< 10watts
Agency and Regulatory	CE
Dimensions	175 x 125 x 39 mm
Weight	350g
Operatine Umidity	5-95 % without condensation
Operating Temperature	0°C to 40°C
Storage Temperature	-20°C to 65°C

APPENDIX B

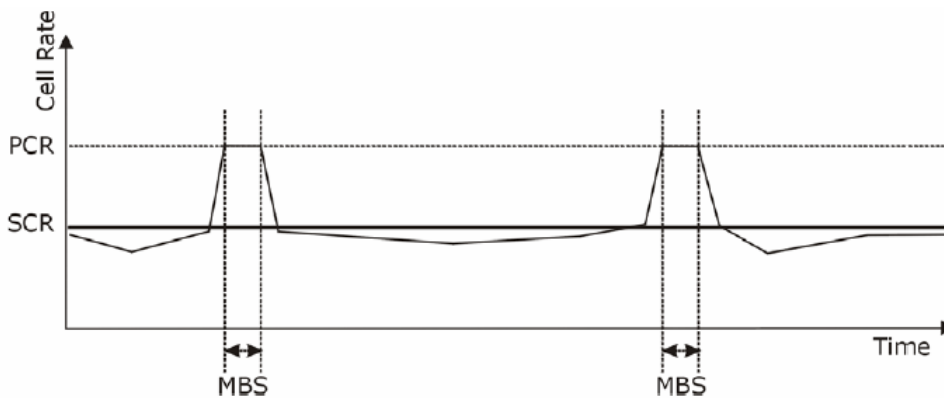
Traffic Shaping

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 C

VoIP Provider

Provider	Provider Official Website	Country
FWD	http://www.fwd.pulver.com	Globe
Iptel	http://www.iptel.org	Globe
FreelpCall	http://www.freeipcall.com	UK
VoIP Talk	http://www.voiptalk.org	UK
VoIPFone	http://www.voipfone.co.uk	UK
Nella	http://www.nella.net.au	Australia
ATP	http://www.austechpartnerships.com	Australia
Freshtel / Firefly	http://www.freshtel.net	Australia
Annatel	http://www.annatel.net	France
myTCOM	http://www.mytcom.it	Italy
ivoice	http://www.ivoice.it	Italy
APOL	http://www.apol.com.tw	Taiwan
SipGate	http://www.sipgate.de	Germany
Brujula	http://www.brujula.net	Spain
FonoSip	http://www.fonosip.com	Spain
InPhonex	http://www.inphonex.com	USA
NaturalVoice	http://www.naturalvoice.us	Brazil
Draytel	http://www.draytel.org	UK



Mitel	http://www.mitel.com	USA
--------------	---------------------------------------------------------	-----

APPENDIX D

Support

Support

If you have any problems with the ADSL2+ VoIP Router, 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 tecnic@atlantis-land.com
WWW: <http://www.atlantis-land.com>

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.