



WebShare 340/440 ADSL2+ VPN Router

A02-RA340

A02-RA440



USER'S MANUAL

A02-RA3(4)40_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.

TABLE OF CONTENTS

CHAPTER 1 1

1.1 AN OVERVIEW OF THE ADSL2+ VPN ROUTER	1
1.2 PACKAGE CONTENTS	2
1.3 ADSL2+ VPN ROUTER FEATURES	2
1.4 ADSL2+ VPN ROUTER APPLICATION	5

CHAPTER 2 6

2.1 CAUTIONS FOR USING THE ADSL2+ VPN ROUTER	6
2.2 THE FRONT LEDS	6
2.3 THE REAR PORTS	7
2.4 CABLING	8

CHAPTER 3 11

3.1 BEFORE CONFIGURATION	11
3.2 CONNECTING THE ADSL2+ VPN ROUTER	11
3.3 CONFIGURING PC IN WINDOWS	12
<i>For Windows 95/98/ME</i>	12
<i>For Windows NT4.0</i>	14
<i>For Windows 2000</i>	15
<i>For Windows XP</i>	17
3.3.1 Configuration Check	19
3.4 FACTORY DEFAULT SETTINGS	19
3.4.1 Username and Password	20
3.4.2 LAN and WAN Port Addresses	20
3.5 INFORMATION FROM THE ISP	20
3.6 CONFIGURING WITH THE WEB BROWSER	21
3.6.1 STATUS	21
3.6.2 Quick Start Guide	23
3.6.3 CONFIGURATION	24
3.6.3.1 LAN	24
3.6.3.1.1 Bridge Filtering	24
3.6.3.1.2 Ethernet	25
3.6.3.1.3 Ethernet Client Filter	26
3.6.3.1.4 DHCP Server	28
3.6.3.2 WAN	30
3.6.3.2.1 ISP	30
3.6.3.2.2 DNS	34
3.6.3.2.3 ADSL	35
3.6.3.3 System	36
3.6.3.3.1 Time Zone	36
3.6.3.3.2 Remote Access	36

- 3.6.3.3.3 Firmware Upgrade 37
- 3.6.3.3.4 Backup/Restore 38
- 3.6.3.3.5 Restart 39
- 3.6.3.3.6 User Management 39
- 3.6.3.4 Firewall 41
 - 3.6.3.4.1 General Settings 41
 - 3.6.3.4.2 Packet Filtering 43
 - 3.6.3.4.3 Intrusion Detection 46
 - 3.6.3.4.4 Url Filtering 47
 - 3.6.3.4.5 Firewall Log 49
- 3.6.3.5 VPN 50
 - 3.6.3.5.1 VPN - PPTP 50
 - 3.6.3.5.2 VPN - IPSec 59
- 3.6.3.6 QoS 65
 - 3.6.3.6.1 Prioritization 65
 - 3.6.3.6.2 Outbound IP Throttling (LAN to WAN) 66
 - 3.6.3.6.3 Inbound IP Throttling (WAN to LAN) 66
- 3.6.3.7 Virtual Server 67
- 3.6.3.8 Time Schedule 70
- 3.6.3.9 Advanced 71
 - 3.6.3.9.1 Static Route 71
 - 3.6.3.9.2 Dynamic DNS 72
 - 3.6.3.9.3 Check Emails 72
 - 3.6.3.9.4 Device Management 73
 - 3.6.3.9.5 IGMP 75
- 3.6.4 Save Config To Flash 76
- 3.6.5 Logout 76

APPENDIX A 77

APPENDIX B 78

APPENDIX C 79

A02-RA3(4)40_ME01 (January 2006, V1.00)

Chapter 1

Introduction

1.1 An Overview of the ADSL2+ VPN Router

Broadband Sharing and IP sharing

The ADSL VPN 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.

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.

VPN

The router supports embedded Virtual Private Network (VPN) protocols and up to 16 simultaneous IPSec VPN tunnels for users to establish private encrypted tunnels over the public Internet (up to 4 VPN tunnels on A02-RA340). With built-in DES/3DES optimized microcode, the router enhances IPSec VPN performance significantly and ensures data transmitted securely between two or more sites.

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+ VPN Router (WebShare 340 or WebShare 440)
- One CD-ROM containing the online manual
- Vera (Multilangue Intercative Tutorial)
- One Quick Start Guide
- One RJ-11 ADSL/telephone cable
- One CAT-5 LAN cable
- One PS2/RS232 (DB9 cable)
- One AC-DC power adapter (12VDC, 1A)

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

1.3 ADSL2+ VPN Router Features

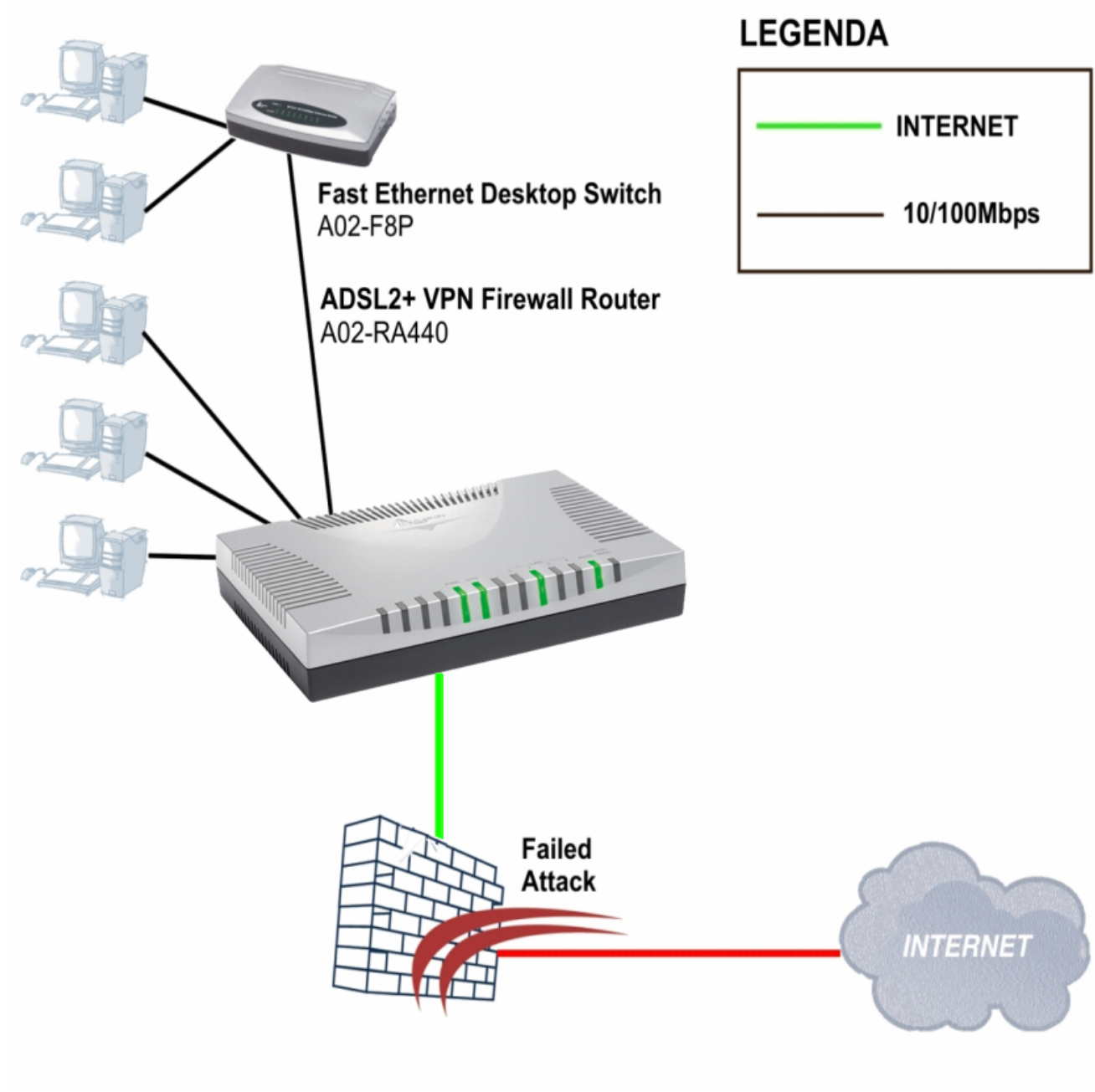
ADSL2+ VPN Router provides the following features:

- **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)].
- **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.
- **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+ VPN Router Application



Chapter 2

Using ADSL2+ VPN Router

2.1 Cautions for using the ADSL2+ VPN Router



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

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

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



Place the ADSL2+ VPN Router on a stable surface.

Only use the power adapter that comes with the package.

2.2 The Front LEDs

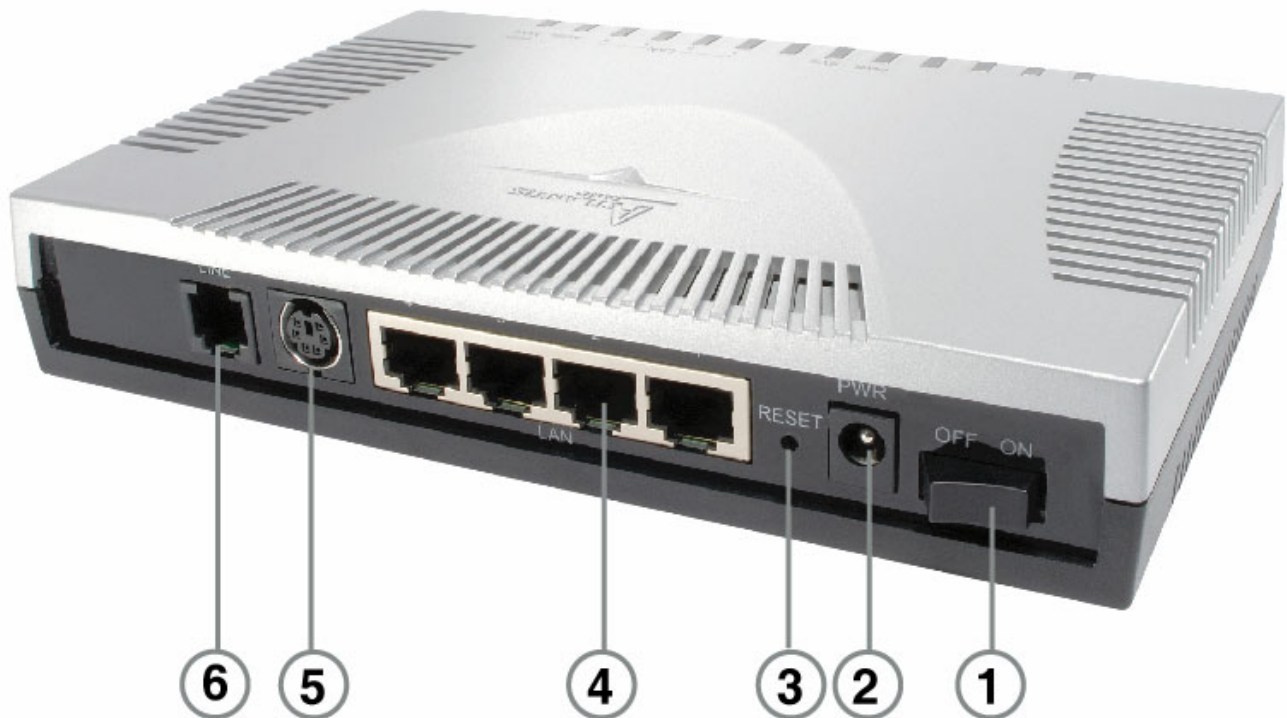


LED	Meaning
POWER	Lit when power ON.
SYS	Lit when system is ready.
LAN (1-4)	Lit when connected to Ethernet device Green for 100Mbps; Orange for 10Mbps Blinking when data transmit/received.



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
LINE (RJ-11) (6)	Connect the supplied RJ-11 cable to this port when connecting to the ADSL/telephone network.
PS2 (CONSOLE) (5)	Connect RS232 cable to the PC.
LAN (4 *RJ-45)* (4)	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 (3)	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) (2)	Connect the supplied power adapter to this jack.
POWER Switch (1)	A Power ON/OFF switch

2.4 Cabling

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

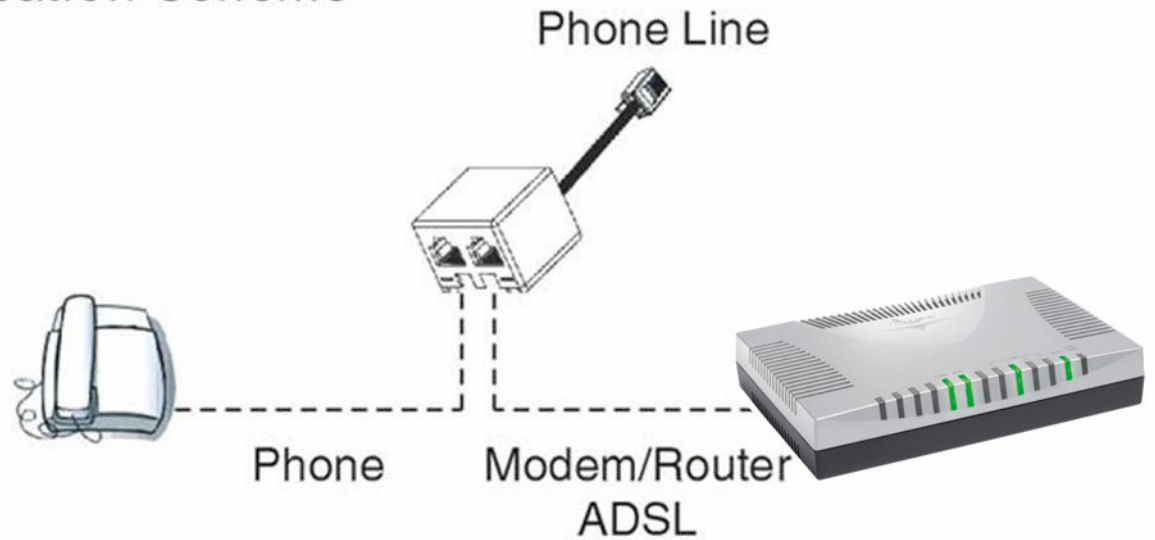
Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analog modems) have a line filter (**A01-AF2**) connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around.

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





Application Scheme



NOTE:

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

The default IP address of the ADSL2+ VPN 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+ VPN 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+ VPN Router. To configure other types of workstations, please consult the manufacturer's documentation.

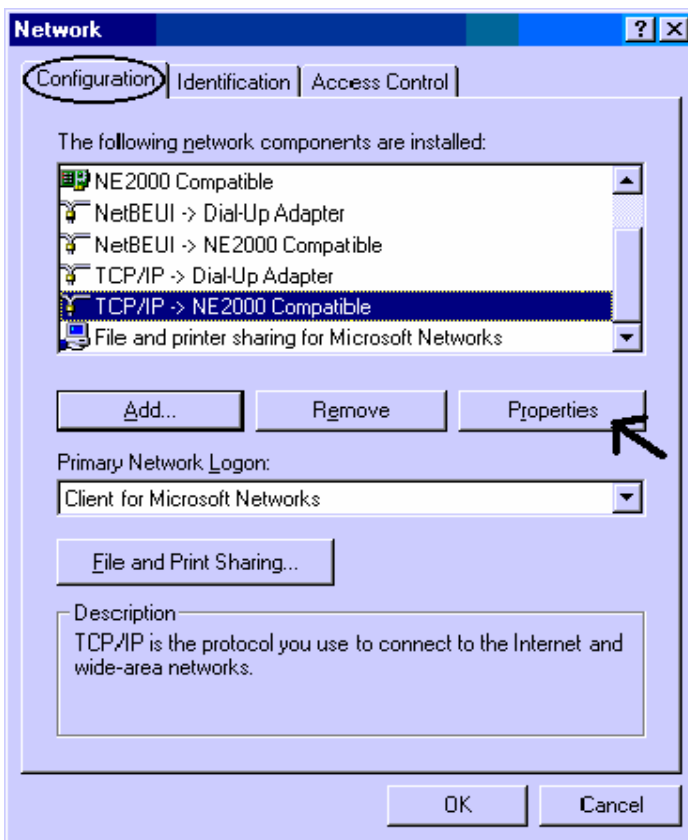
3.2 Connecting the ADSL2+ VPN Router

- Connect the ADSL2+ VPN 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.

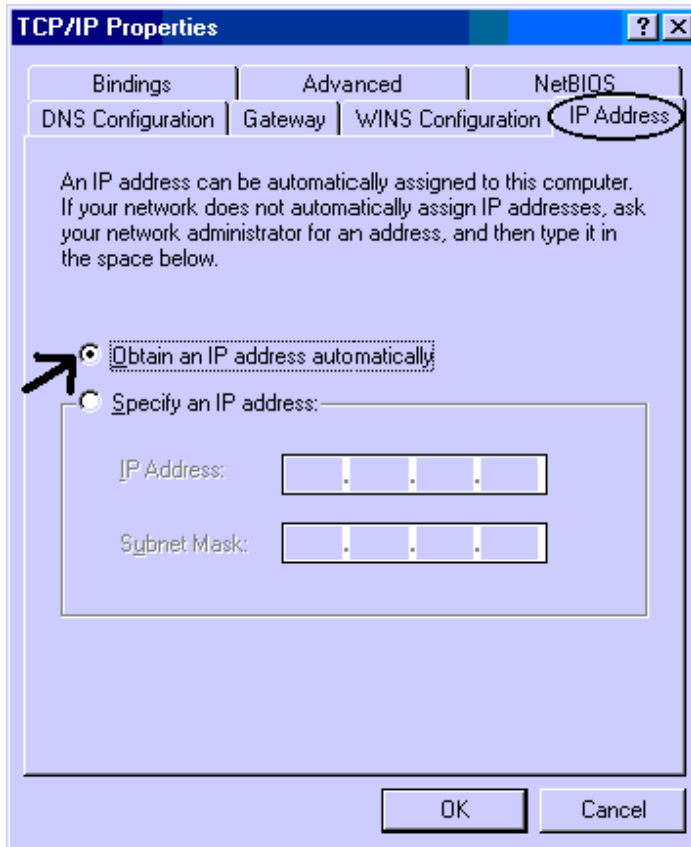
3.3 Configuring PC in Windows

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.

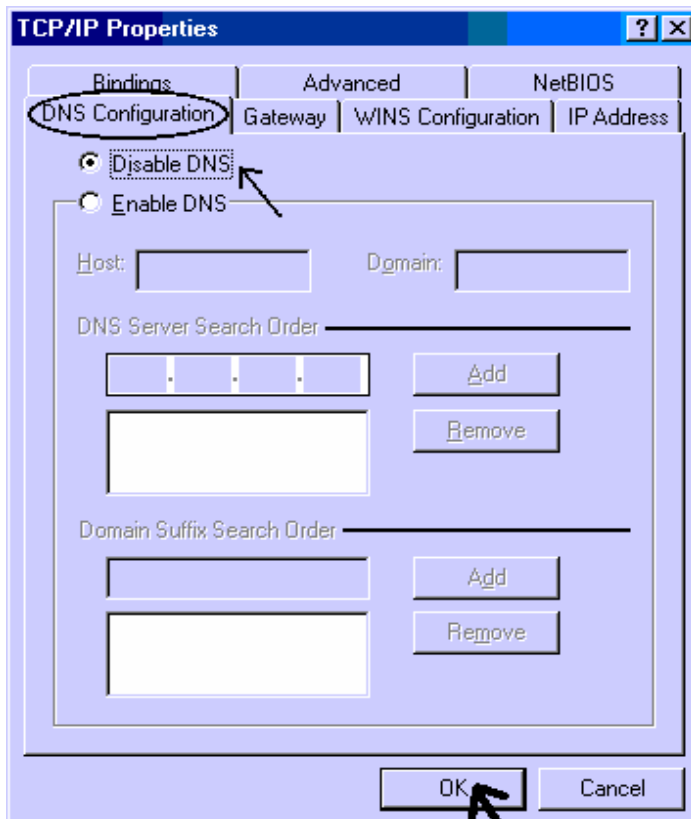


4. Select the **IP Address** tab. In this page, click the **Obtain an IP address automatically** radio button.



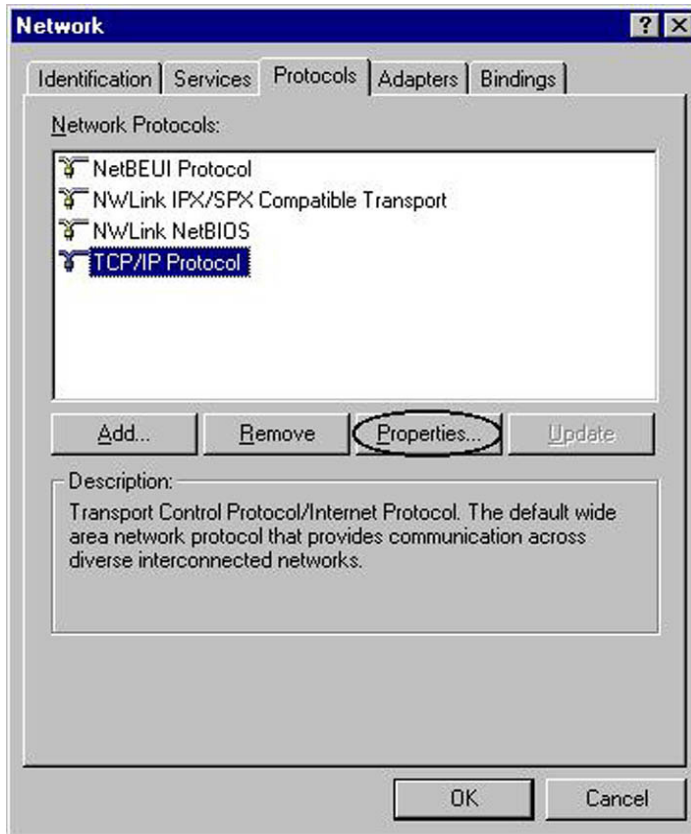
5. Then select the **DNS Configuration** tab.

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

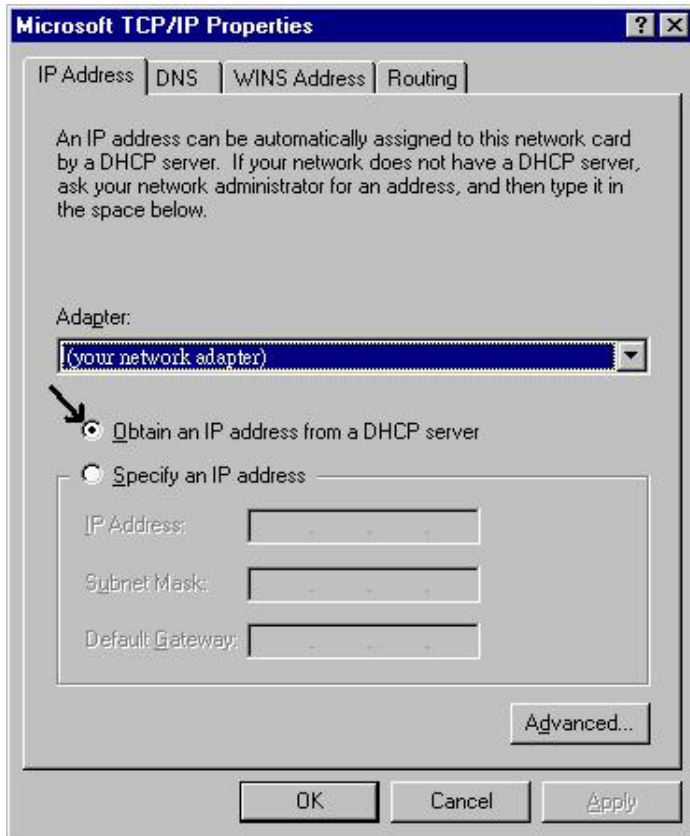


For Windows NT4.0

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**.

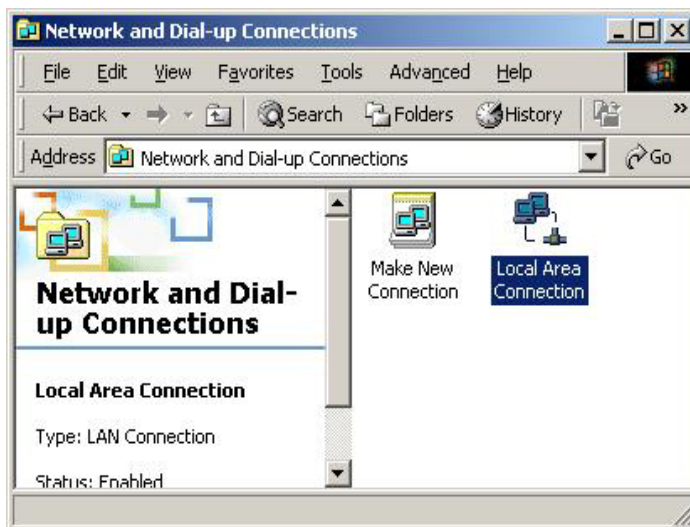


3. Select the **Obtain an IP address from a DHCP server** radio button and click **“OK”**.

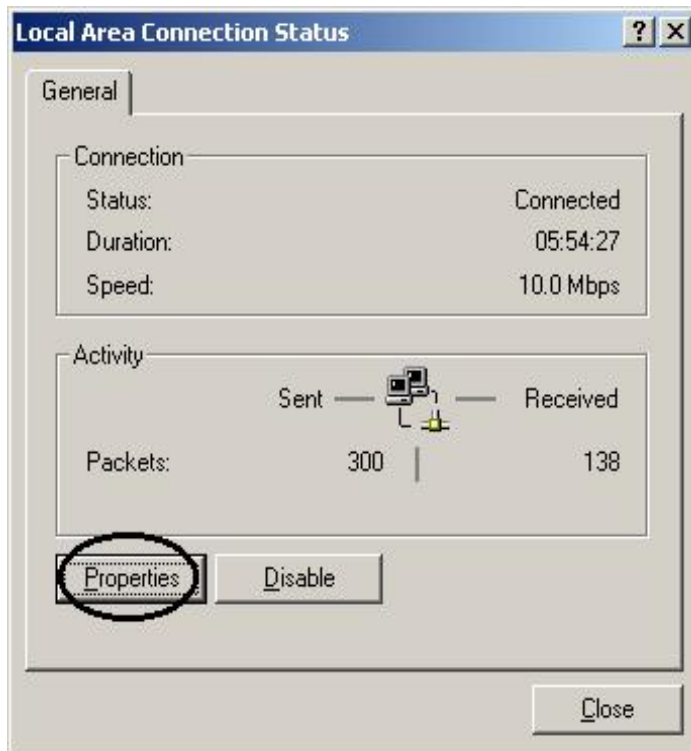


For Windows 2000

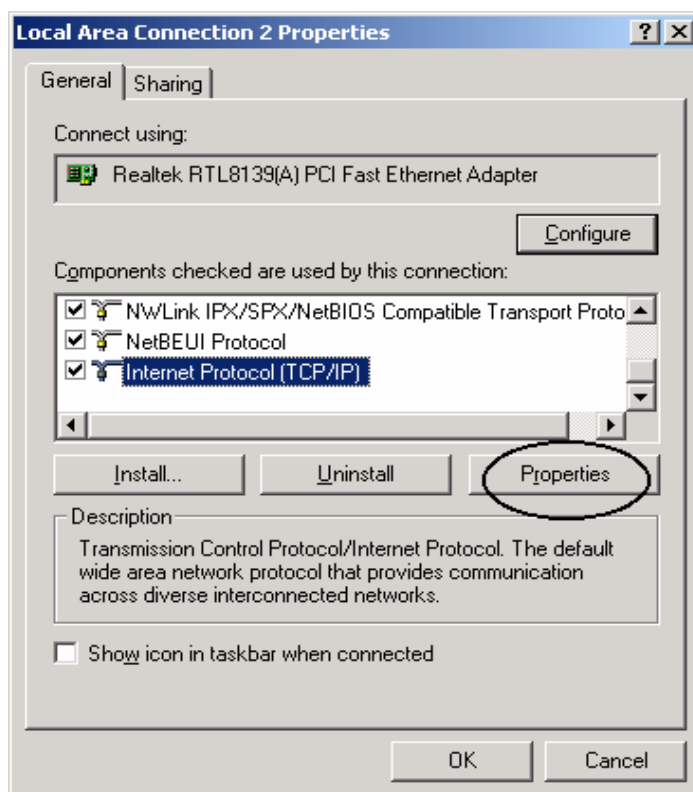
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **LAN Area Connection**.



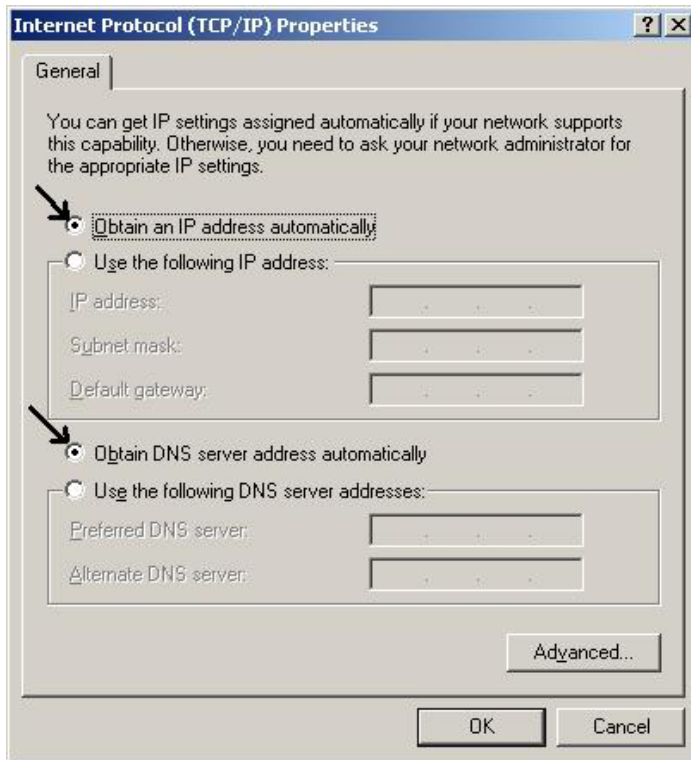
3. In the **LAN Area Connection Status** window, click **Properties**.



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

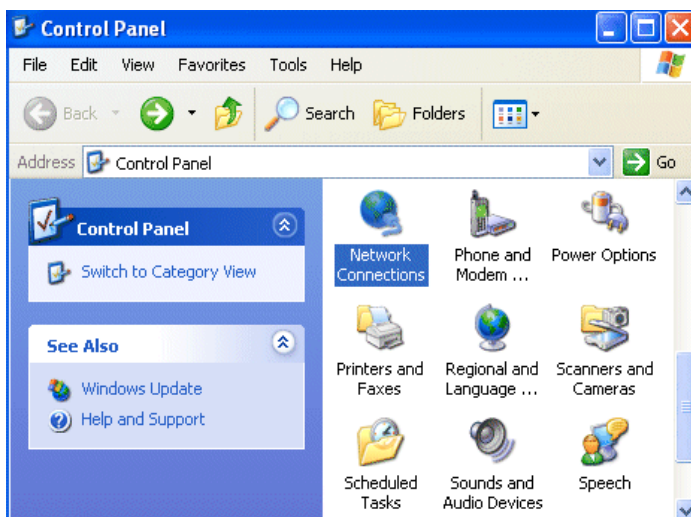


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **“OK”** to finish the configuration.

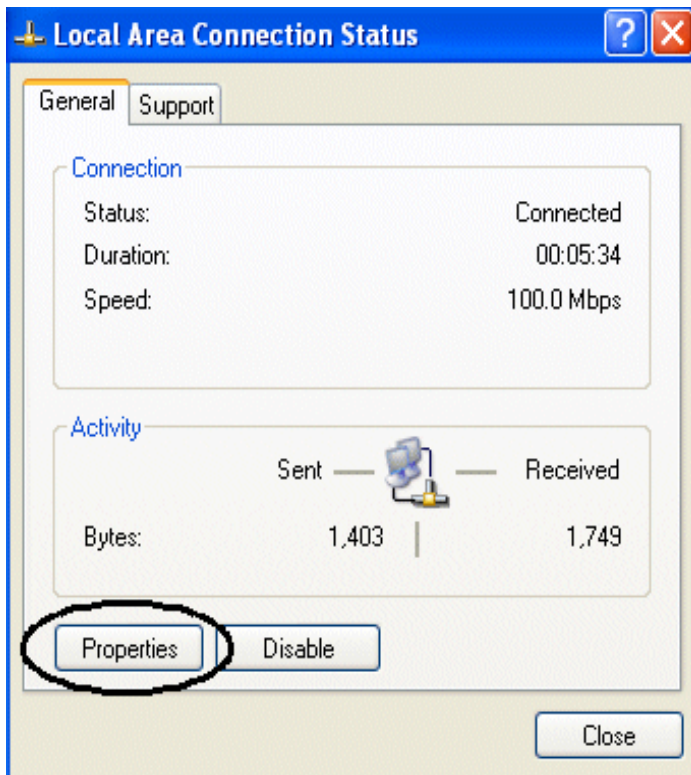


For Windows XP

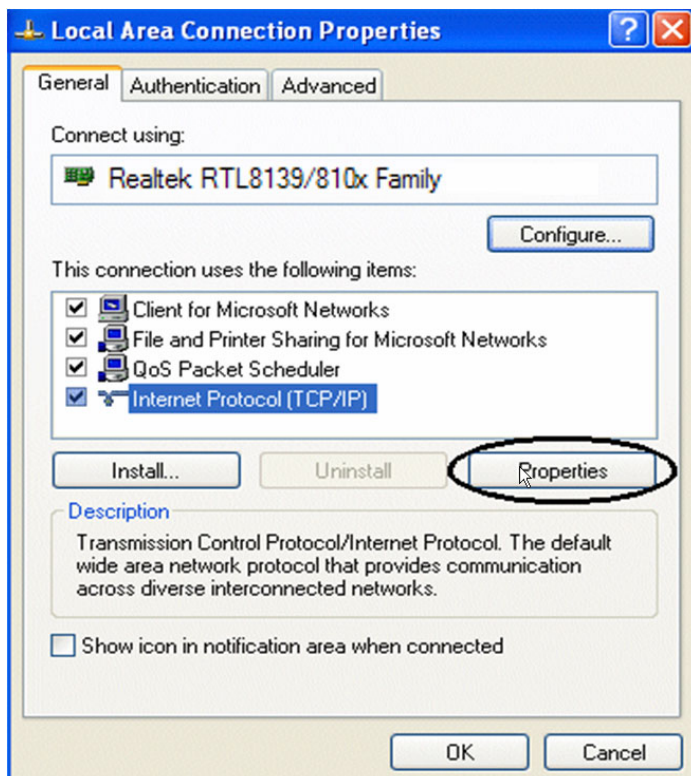
1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click on **Network Connections**.
2. Double-click **Local Area Connection**



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

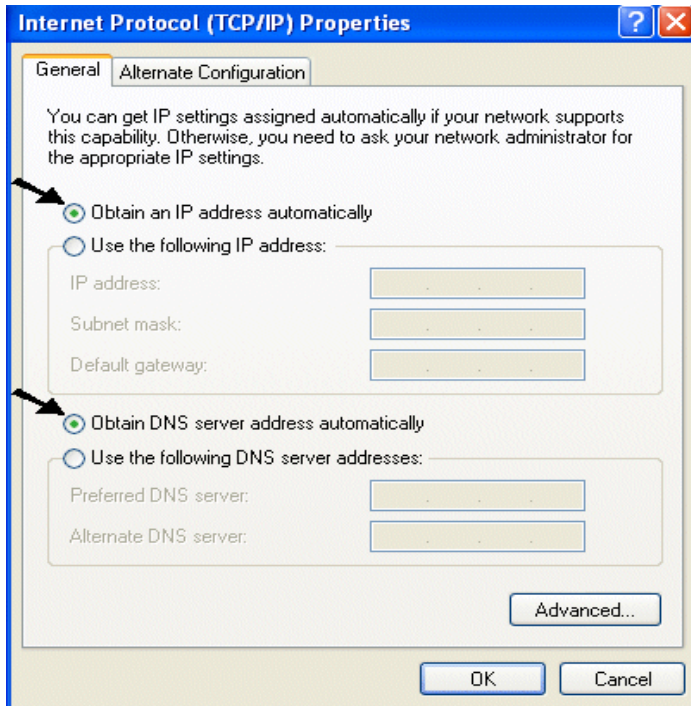


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



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+ VPN 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 is enabled.

3.4.1 Username and Password

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



If you ever forget the password to log in, you may press the RESET button to restore the factory default settings. After turning the router on press the Emergency/Failure Recovery Button on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. 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

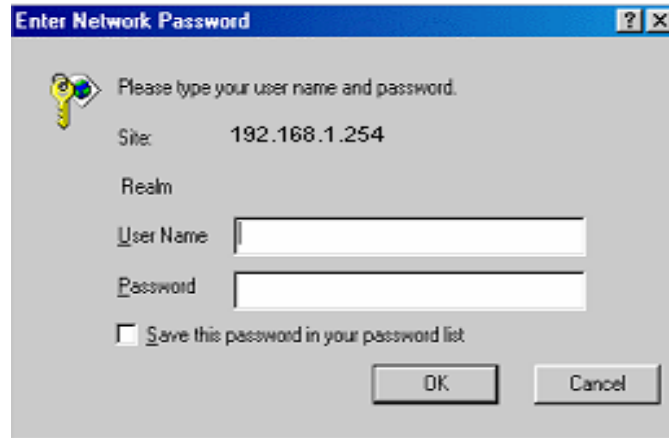
Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as PPPoE, PPPoA, RFC1483, IpoA.

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+ VPN 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, Routing Table, DHCP Table, PPTP Status, IPSec Status, L2TP Status, Email Status, Event Log, Error Log, Nat Sessions, UPnP PortMap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, VPN, QoS, Virtual Server & Advanced)
- **Save Config to FLASH**
- **Language** (provides user interface in multi-languages).

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.

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	
Secondary DNS	
PPP	
Username	
Password	
<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 Chapter 3.5 (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.

3.6.3 CONFIGURATION

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


- LAN
- WAN
- System
- Firewall
- VPN
- 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**.

Edit ethernet Interface

Parameters

Acceptable Frame Type	ALL
Filter Type	All
PVID for Untagged Frames	1

Note: NAT/NAPT can be applied to management interface only

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			

IP Alias

IP Address	SubNetmask	Security Interface

The default IP address for the router is 192.168.1.254.

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



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

3.6.3.1.2.1 IP Alias

IP Alias

Parameters

IP Address				
SubNetmask				
Security Interface	<input checked="" type="radio"/> Internal <input type="radio"/> External <input type="radio"/> DMZ			

IP Address: Insert the secondary IP Address

SubNetMask: Set the related SubNetMask

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

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.

3.6.3.1.4 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 fullduplex, 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.

3.6.3.1.4 DHCP Server

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

DHCP Server

Configuration

DHCP Server Mode	<input type="radio"/> Disabled
	<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"/> Disabled
Allow Unknown Clients	<input checked="" type="radio"/> Enable <input type="radio"/> Disabled
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"/>

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 possible 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	8
VCI	35
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.

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)
- **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.

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 Utagged Frames	1
<input type="button" value="Apply"/>	

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

3.6.3.2.2 DNS

DNS	
Parameters	
Obtain DNS Automatically	<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

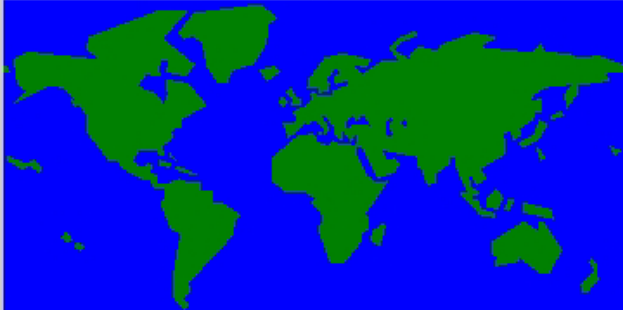
Apply Cancel

- **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

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.

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

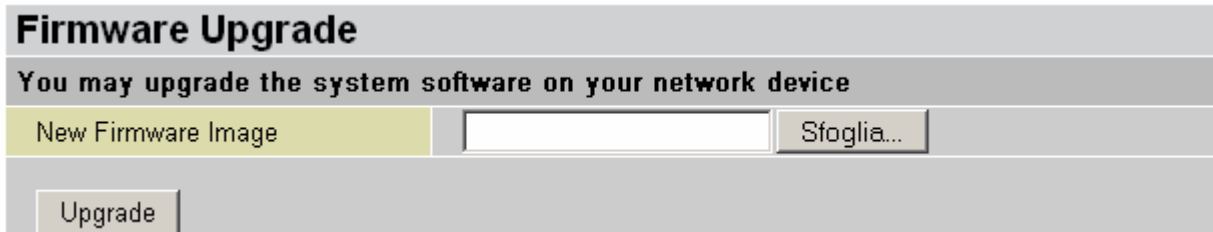
To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router permits remote access for and click Enable. You may change other configuration options for the web administration interface using Device Management options in the **Advanced** section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

3.6.3.3 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

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

Block WAN Request	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
-------------------	---

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	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	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)	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
RealAudio (7070)	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
ICMP	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	NO	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	N/A	N/A	NO	YES	NO	YES
ICQ(5190)	TCP(6)	5190	5190	N/A	N/A	N/A	N/A	YES	YES
MSNP	TCP(6)	1863	1863	N/A	N/A	N/A	N/A	YES	YES
ASF3	UDP(17)	7001	7001	N/A	N/A	N/A	N/A	YES	YES
PPTP	TCP(1723)	1723	1723	N/A	N/A	N/A	N/A	N/A	N/A
IPSEC	UDP(6)	500	500	N/A	N/A	N/A	N/A	N/A	N/A

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, stating from the first rule.

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

Packet Filter

[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	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	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	Allow ▾		
Outbound	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	Always On ▾
Protocol Number	<input type="text"/>
Inbound	Allow ▾
Outbound	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"/>	

Hacker attack types recognized by the IDS

Attack	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill	Src IP	DoS	Yes	Yes
Win Nuke	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)	Src IP	Scan	Yes	Yes
	SrcPort: 0 or 65535				
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	Src IP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort=Orifice Port (31337)	Src IP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count(Def=100 s)				Yes
ICMP Flood	Max ICMP Count (Def=100 s)				Yes
ICMP Echo	Max Ping Count (Def=15 s)				Yes

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"/>
---------	----------------------

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 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	<div style="border: 1px solid #ccc; padding: 2px;"> Forbidden Domain ▾ </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Forbidden Domain </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Trusted Domain </div>
<input type="button" value="Apply"/>	

Trusted Domain		
Name	Domain	
item1	abc	<input type="button" value="Delete"/>
Forbidden Domain		
Name	Domain	
item0	sex	<input type="button" value="Delete"/>
<input type="button" value="Return"/>		

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

3.6.3.5 VPN

Your router support 2 main types of VPN (Virtual Private Network), PPTP and IPSec, and these are the two major section choices from the menu on the left. Click **Create** to select one of applications to continually setup.

3.6.3.5.1 VPN - PPTP

The router supports PPTP VPN to establish secure, end-to-end private network connections over a public networking infrastructure. There are two kinds of PPTP VPN connections, one is remote access (dial-in & dial-out), and the other is LAN-to-LAN access.

Deploying a remote access VPN enables users to reduce the cost by leveraging the local dial-up infrastructures of the ISP, in addition, transmitting data over a secure VPN tunnel. LAN-to-LAN PPTP VPN is an alternative WAN infrastructure that is used to connect offices and home offices to share network resources with each other over a secure VPN tunnel. There are two types of PPTP VPN supported, Remote Access and LAN-to-LAN (please refer below for more information.). Click Create to configure a new VPN connection.

PPTP			
Remote Access Connection			
Connection Name	<input type="text"/>		
Type	<input checked="" type="radio"/> Dial out, <input type="radio"/> Dial in,	Server IP Address (or Domain Name)	<input type="text"/>
		Private IP Address Assigned to Dialin User	<input type="text"/>
Username	<input type="text"/>		
Password	<input type="text"/>		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 <input type="text"/> minutes		
Active as default route	<input type="checkbox"/> Enable		
Apply			

Connection Name: This allows you to identify this particular connection, e.g. “Connection to officeLAN”.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPNserver, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

PPP Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients

connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm.

Default is **Auto**, so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

Active as default route: Enables the default route.

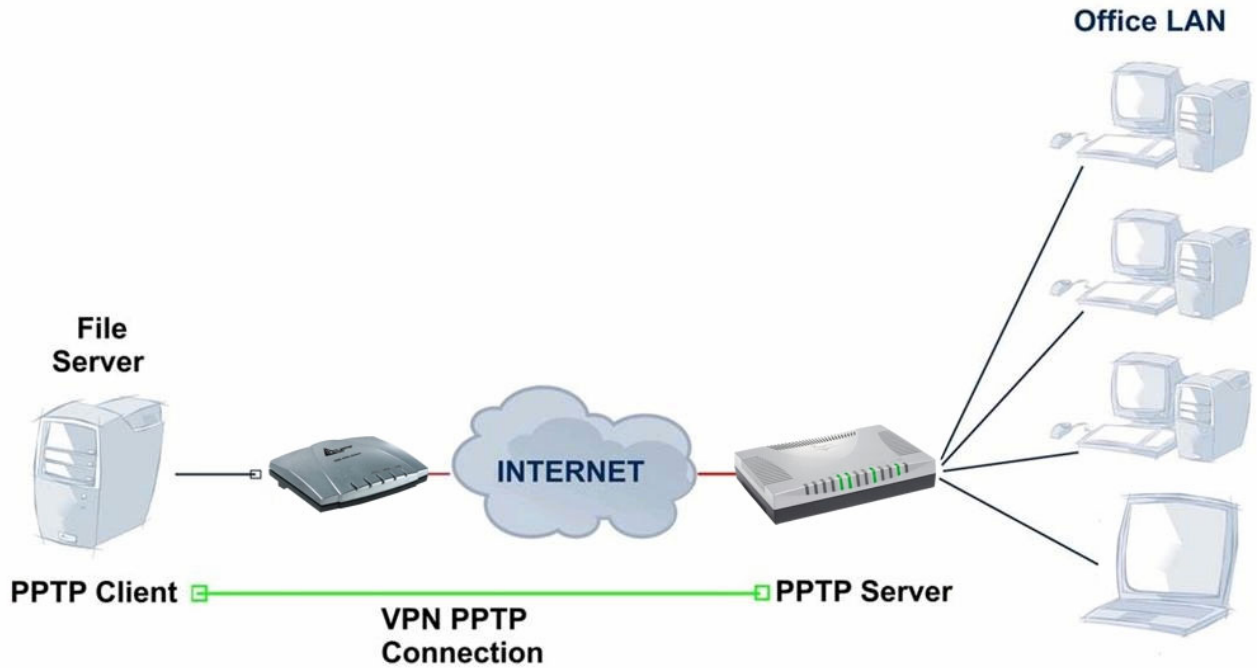
Click **Apply** button to apply your changes.

An Example of Configuring a Remote Access PPTP VPN Dial-in Connection

Background of the Example

A remote worker establishes a PPTP VPN connection with the head office using Microsoft's VPN Adapter, a piece of software included with Windows 2000/ME, etc. The Router is installed in the Office Lan, connected to a couple of PCs and Servers.

Application Diagram Configuring PPTP VPN in the Office LAN Router



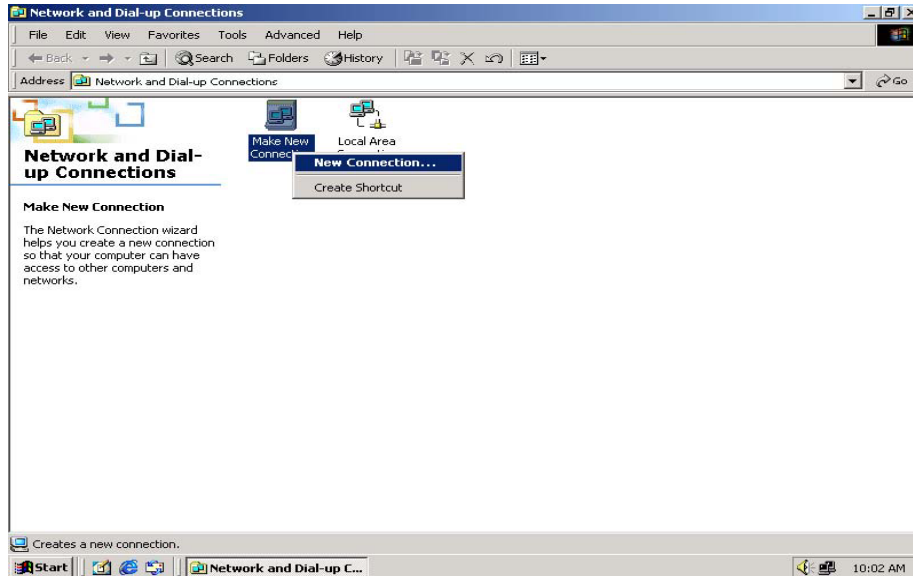
The input IP address 192.168.1.200 will be assigned to the remote worker, please make sure this IP is not used in the Office LAN.

PPTP			
Remote Access Connection			
Connection Name	Dial-IN		
Type	<input type="radio"/> Dial out,	Server IP Address (or Hostname)	
	<input checked="" type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	192.168.1.200
Username	Username		
Password	••••••••		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

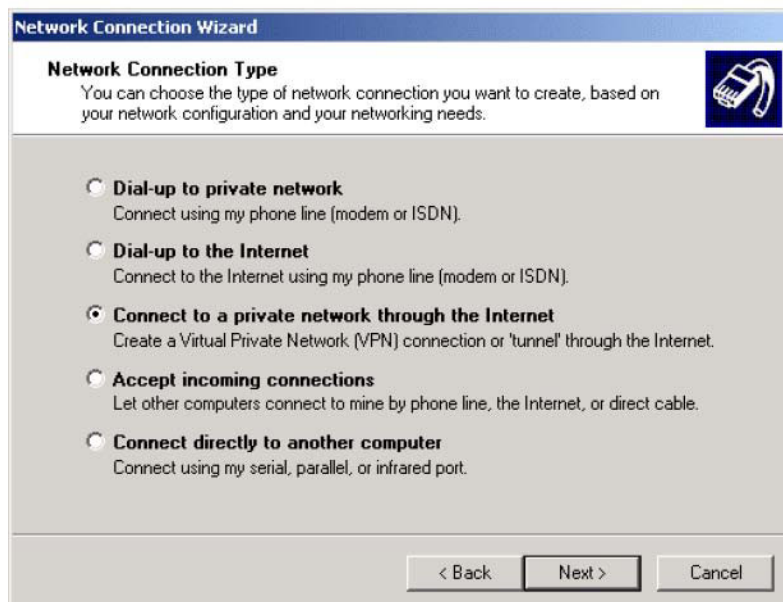
Configuring PPTP VPN in Remote Side

You can configure VPN client with commercial VPN client software package (e.g. SSH) or the Dialup Adaptor in Windows. Please follow the steps below if you are a Windows 2000/XP user.

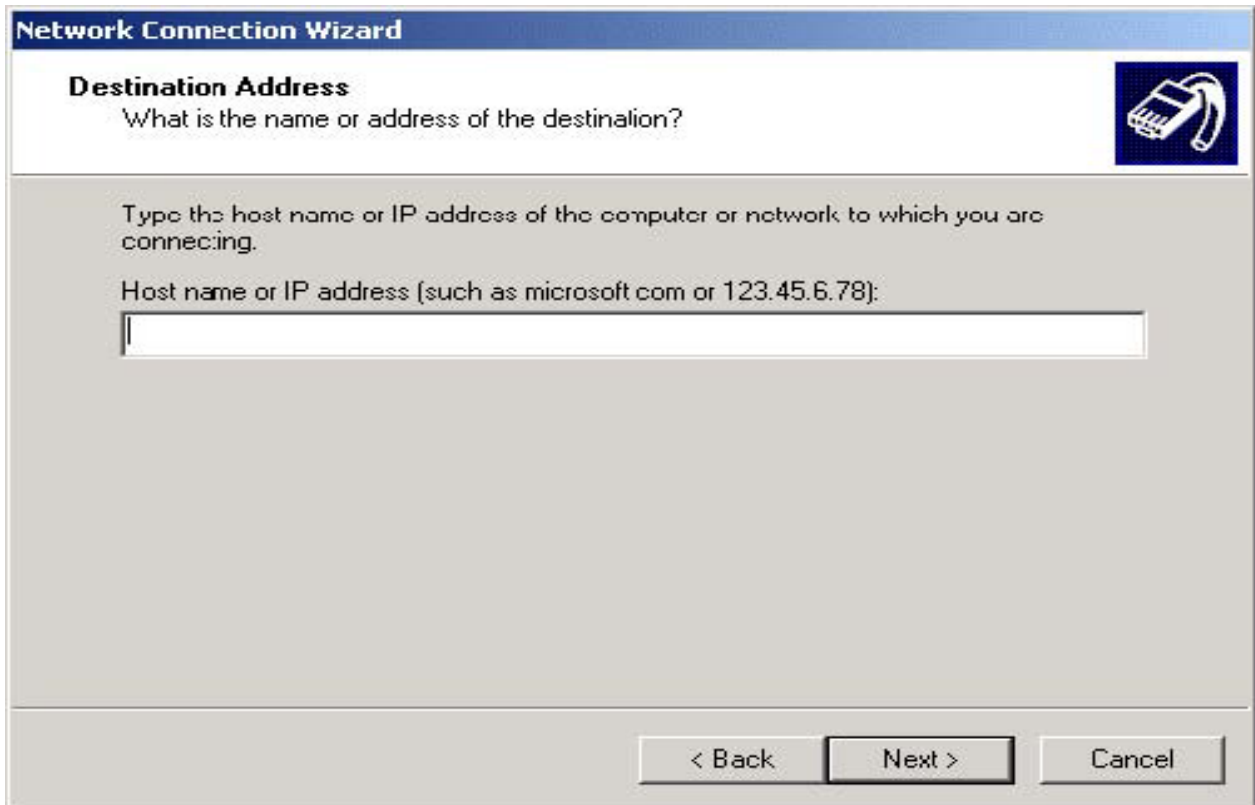
1.



2. Follow the step and select **“Connect to a private network through the Internet”**



3. Insert IP Addressor Hostname to call to establish a VPN tunnel



4. Follow the step, the following screen appears. The setup is completed.



5. To make the connection, click the Virtual Private Connection icon in Dial-up Networking Group,

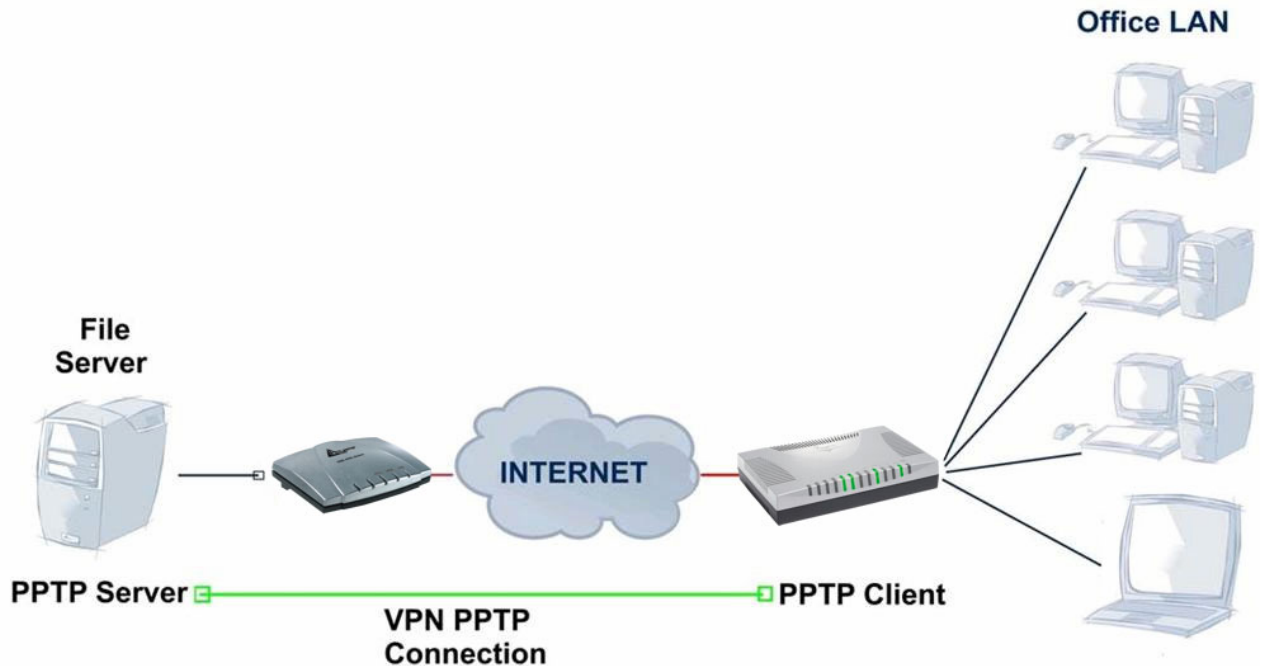


An Example of Configuring a Remote Access PPTP VPN Dial-out Connection

Background of the Example

Corporate establishes a PPTP VPN connection with the file server located in the remote side. The router is installed in the office, connected with a couple of PCs and Servers.

Application Diagram



Configuring PPTP VPN in the Office

You can either input the IP address (80.123.23.45 in this case) or hostname to reach the Server.

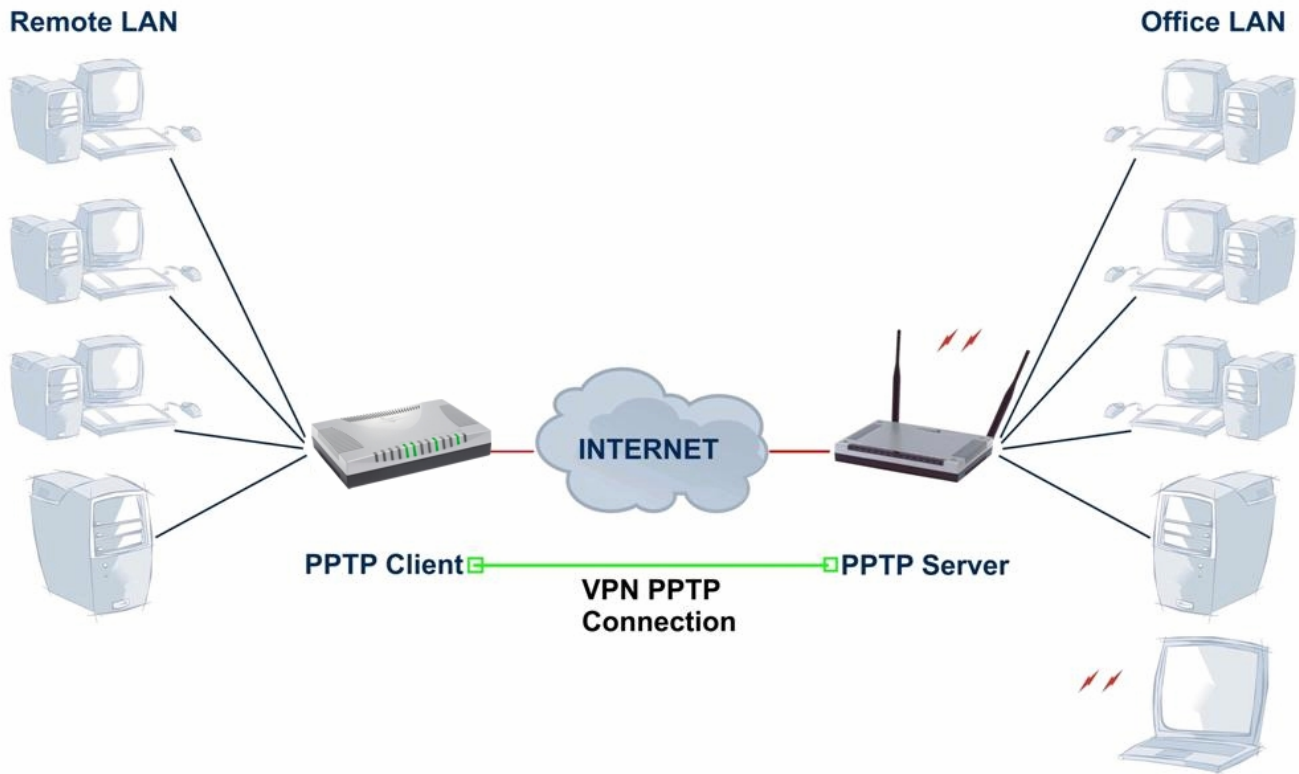
PPTP			
Remote Access Connection			
Connection Name	ToFileServer		
Type	<input checked="" type="radio"/> Dial out,	Server IP Address (or Hostname)	80.123.23.45
	<input type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	
Username	username		
Password	••••••••		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
Apply			

Refer also to **PPTP VPN – remote access (dial-in)** for the other parameters.

An Example of Configuring a LAN-to-LAN PPTP VPN Connection

Background of the Example

The Remote LAN establishes a PPTP VPN tunnel with the Office LAN to connect two private networks by leveraging the Internet infrastructure. The routers are installed in the Office Lan and Remote Lan accordingly.



	Remote LAN	Office LAN
Product Code	A02-RA440/A02-RA340	A02-WRA4-54G
Picture		
Public IP	80.17.56.78	69.121.1.32
NAT	Yes	Yes
LAN IP	192.168.1.X	192.168.2.X
Subnet Mask	255.255.255.0	255.255.255.0
PPTP	Client PPTP	Server PPTP

Configuring PPTP VPN in the Office Lan

The input IP address 192.168.2.200 will be assigned to the router located in the Remote LAN. Please make sure this IP is not used in the head office LAN.

PPTP			
LAN to LAN			
Connection Name	Lan-To-Lan		
Type	<input type="radio"/> Dial out,	Server IP Address (or Hostname)	
	<input checked="" type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	192.168.2.200
Peer Network IP	192.168.1.0	Netmask	255.255.255.0
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

Configuring PPTP VPN in the Remote Lan The input IP address 69.121.1.32 is the **Public IP** address of the router located in the Office Lan. If you have a domain name assigned to this IP address - either you registered the DDNS (please refer to the **DDNS** section), or you have a static IP with a domain name, you can also use the Hostname instead of the IP address to reach the router.

PPTP			
LAN to LAN			
Connection Name	Lan-To-Lan		
Type	<input checked="" type="radio"/> Dial out,	Server IP Address (or Hostname)	69.121.1.32
	<input type="radio"/> Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP	192.168.2.0	Netmask	255.255.255.0
Username	Username		
Password	*****		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾ Mode stateful ▾
Idle Timeout	0 minutes		
<input type="button" value="Apply"/>			

Refer also to **Configuring PPTP VPN in the Office LAN** for other parameters.

3.6.3.5.2 VPN - IPSec

The router supports IPSec VPN to establish secure, end-to-end private network connections over a public networking infrastructure.

IPSec					
Create					
Connection Name	<input type="text"/>				
Local					
Network	<input checked="" type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input 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"/>
Remote					
Secure Gateway Address(or Hostname)	<input type="text"/>				
Network	<input checked="" type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input 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"/>
Proposal					
<input checked="" type="radio"/> ESP	Authentication	None			
	Encryption	NULL			
<input type="radio"/> AH	Authentication	MD5			
Perfect Forward Secrecy	None				
Pre-shared Key	<input type="text"/>				
<input type="button" value="Apply"/>					

Connection Name: A user-defined name for the connection (e.g. “connection to office”).

Local:

Network: Set the IP address, subnet or address range of the local network.

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP:192.168.1.10

Remote:

- **Secure Gateway Address (or Domain Name):** The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.
- **Network:** Set the IP address, subnet or address range of the remote network.
- **Proposal:** Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload).
Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.
- **Authentication:** Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.
 1. **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
 2. **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Encryption: Select the encryption method from the pull-down menu. There are several

options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit,

MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy

and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic

can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

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

This function is only available after completed creating an IPSec account. Click **Advanced Optino** to change the following settings

IPSec		
IKE Mode	Main ▼	
IKE Proposal		
Hash Function	SHA1 ▼	
Encryption	3DES ▼	
Diffie-Hellman Group	MODP 1024 (Group 2) ▼	
Local ID		
Type	Default ▼	
Content	<input type="text"/>	
Remote ID		
Type	Default ▼	
Identifier	<input type="text"/>	
SA Lifetime		
Phase 1 (IKE)	240	minutes
Phase 2 (IPSec)	60	minutes
PING for keepalive		
PING to the IP	0.0.0.0	(0.0.0.0 means NEVER)
Interval	10	seconds (0-3600, 0 means NEVER)
Disconnection Time after no traffic	1200	seconds (180 at least)
Reconnection Time	15	minutes (3 at least)
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

IKE (Internet key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

IKE Proposal:

Hash Function: It is a Message Digest algorithm which coverts any length of a message into a unique set of bits. It is widely used MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm)

algorithms.

SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160-bit hash

Encryption: Select the encryption method from the pull-down menu. There are several options,

DES, 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Local ID:

- **Type:** Specify local ID type.
- **Content:** Input ID's information, like domain name www.ipsectest.com.

Remote ID:

- **Type:** Specify Remote ID type.
- **Identifier:** Input remote ID's information, like domain name www.ipsectest.com.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPsec. IKE negotiates and establishes SA on behalf of IPsec, an IKE SA is used by IKE.

Phase 1 (IKE): To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 240 minutes.

Phase 2 (IPsec): To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, everytime the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keepalive: It is used to detect IPsec tunnel connection failure. Connection failure is defined as abort or in NO response state. In such event Ping to Keepalive takes proper action to ensure the connection quality of IPsec.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function.

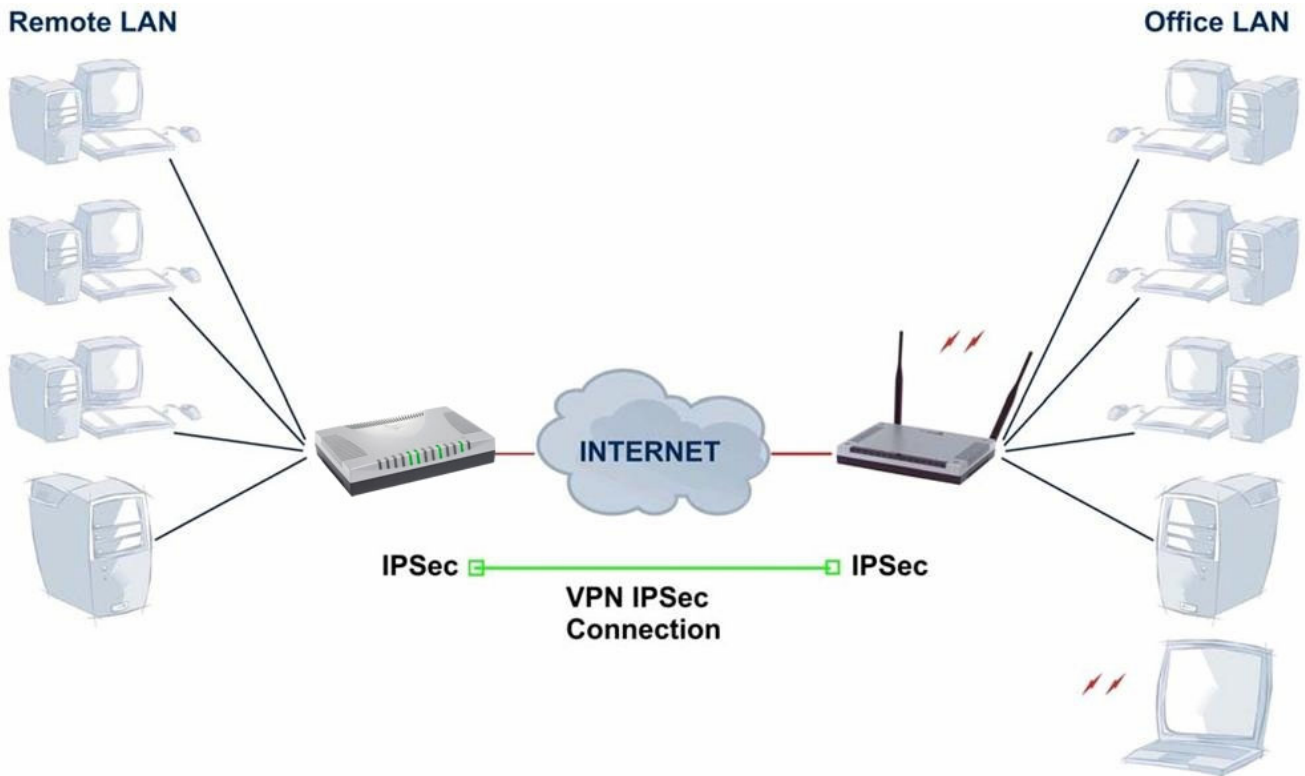
Internal: This sets the time interval between **Pings to the IP** function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the **Reconnection Time** set. Default setting is **1200 seconds; 180 seconds** is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. Default setting is **15 minutes; 3 minutes** is minimum time interval for this function.

Select the **Apply** button to update the settings.

An Example of Configuring a LAN-to-LAN IPsec VPN Connection



	Remote LAN	Office LAN
Product Code	A02-RA440/A02-RA340	A02-WRA4-54G
Picture		
Public IP	69.121.1.31	69.121.1.32
NAT	Yes	Yes
LAN IP	192.168.1.X	192.168.2.X
Subnet Mask	255.255.255.0	255.255.255.0
VPN IPsec	ESP	ESP
Encryption	DES(or 3DES/AES)	DES(or 3DES/AES)
Authentication	MD5 (or SHA1)	MD5 (or SHA1)
Perfect Forward Secrety	None	None
IKE Pre Shared Key	123456789	123456789

Configuring IPsec VPN in the Office LAN

IPSec					
Create					
Connection Name	<input type="text" value="Lan-To-Lan"/>				
Local					
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.2.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Remote					
Secure Gateway Address(or Hostname)		<input type="text" value="69.121.1.31"/>			
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.1.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Proposal					
<input checked="" type="radio"/> ESP	Authentication	<input type="text" value="MD5"/> <input type="button" value="v"/>			
	Encryption	<input type="text" value="DES"/> <input type="button" value="v"/>			
<input type="radio"/> AH	Authentication	<input type="text" value="MD5"/> <input type="button" value="v"/>			
Perfect Forward Secrecy	<input type="text" value="None"/> <input type="button" value="v"/>				
Pre-shared Key	<input type="text" value="123456789"/>				
<input type="button" value="Apply"/> Advanced Options <input type="button" value="▶"/>					

Configuring IPsec VPN in the Remote LAN

IPSec					
Create					
Connection Name	<input type="text" value="Lan-To-Lan"/>				
Local					
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.1.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Remote					
Secure Gateway Address(or Hostname)		<input type="text" value="69.121.1.32"/>			
NetWork	<input type="radio"/> Single Address	IP Address	<input type="text"/>		
	<input checked="" type="radio"/> Subnet	IP Address	<input type="text" value="192.168.2.0"/>	Netmask	<input type="text" value="255.255.255.0"/>
	<input type="radio"/> IP Range	IP Address	<input type="text"/>	End IP	<input type="text"/>
Proposal					
<input checked="" type="radio"/> ESP	Authentication	<input type="text" value="MD5"/> <input type="button" value="v"/>			
	Encryption	<input type="text" value="DES"/> <input type="button" value="v"/>			
<input type="radio"/> AH	Authentication	<input type="text" value="MD5"/> <input type="button" value="v"/>			
Perfect Forward Secrecy	<input type="text" value="None"/> <input type="button" value="v"/>				
Pre-shared Key	<input type="text" value="123456789"/>				
<input type="button" value="Apply"/> Advanced Options <input type="button" value="▶"/>					

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)
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	Time Slot1	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
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled
	Always On	High	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	Disabled

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.

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	6 *32 (kbps)
VoIP	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	4 *32 (kbps)
Restricted	TimeSlot1	any	0 ~ 0	192.168.1.100 ~ 192.168.1.100	5 *32 (kbps)
Others	TimeSlot1	any	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	1 *32 (kbps)
	Always On	any	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	1 *32 (kbps)
	Always On	any	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	0.0.0.0 ~ 192.168.1.100	64 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0	0.0.0.0 ~ 0.0.0.0	0.0.0.0 ~ 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.

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

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"/>
<input type="button" value="Apply"/> 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-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	
<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Internal IP Address Candidates ▶	<input type="text"/>
<input type="button" value="Apply"/> 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	<input checked="" type="radio"/> Disable	<input type="radio"/> Public to Private Subnet	<input type="radio"/> 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"/>
<input type="button" value="Apply"/> <input type="button" value="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 <input type="button" value="Helper"/>	<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 <input type="button" value="Candidates"/>	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="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	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"/>
Cost	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	www.dyndns.org (dynamic) ▼
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	25 <input type="text"/> 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	60 <input type="text"/> 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**

3.6.4 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.

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
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
VPN	VPN Pass Through (IPSec, L2TP, PPTP) Up to 16 VPN IPSec (A02-RA440) Up to 4 VPN IPSec(A02-RA340) Accelerator DES/3DES (A02-RA440)
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

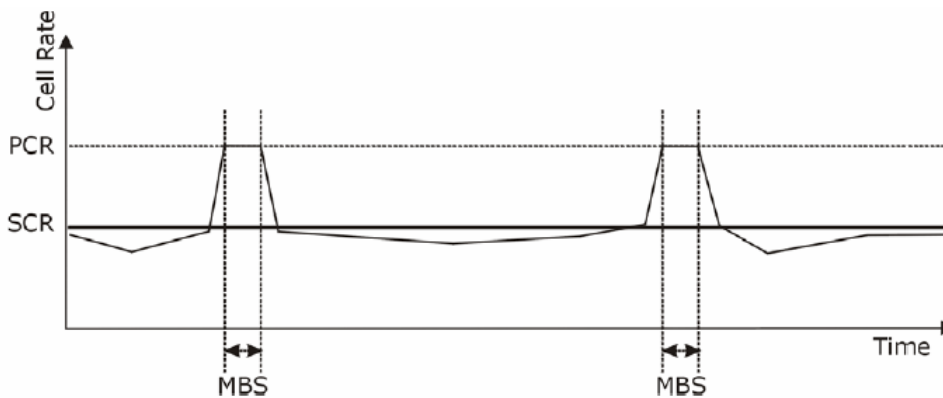
Traffic Shaping

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

Support

Support

If you have any problems with the ADSL2+ VPN 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.

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>