



## 54 Mbps Wireless G Modem Router With 4 Port Switch

HN-DR4PG

### User Manual



## **COPYRIGHT**

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

## **TRADEMARKS**

All products, company, brand names are trademarks or registered trademarks of HitekNOFAL. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

## **FCC INTERFERENCE STATEMENT**

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

## **CE DECLARATION OF CONFORMITY**

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B.



## Contents

1 Introduction.....	6
1.1 Intended Audience .....	6
1.2 Definitions Of Terms Used In This Document .....	6
1.3 Acronyms Used Throughout This Document.....	6
1.4 Usage Instructions.....	6
1.5 Questions or Comments on This Document.....	6
2 System Overview .....	7
2.1 General Description .....	7
2.2 Specifications .....	7
2.3 Hardware Description .....	9
2.3.1 Front View .....	9
2.3.2 Rear View .....	10
3 Getting Started.....	11
3.1 Package Contents.....	11
3.2 Minimum System Requirements.....	11
3.3 Hardware Installation .....	12
3.4 Software Quick Configuration.....	13
4 Graphical User Interface Pages.....	15
4.1 Status.....	15
4.1.1 Status .....	15
4.1.2 Diagnostic Test.....	16
4.1.3 Interfaces.....	17
4.1.4 ADSL.....	17
4.2 Quick Setup .....	18
4.3 LAN Interface .....	19
4.3.1 IP Address .....	19
4.3.2 DHCP Settings.....	21
4.3.2.1 DHCP Server Mode.....	21
4.3.2.2 DHCP Relay Mode .....	24
4.4 Wireless.....	25
4.4.1 Basic Setting.....	25
4.4.2 Advanced Settings.....	27
4.4.3 MBSSID.....	30
4.4.4 Security .....	31
4.4.5 Access Control .....	33
4.4.6 C2C.....	35
4.5 Internet Interface.....	37

4.5.1	WAN Configuration.....	37
4.5.1.1	PPPoE Mode.....	38
4.5.1.2	PPPoA Mode .....	39
4.5.1.3	Bridge Mode .....	39
4.5.1.4	1483 Routed Mode.....	39
4.5.1.5	MER(Mac Encapsulating Routing) Mode.....	40
4.5.2	ATM Setting .....	40
4.5.3	ADSL Setting.....	41
4.6	Firewall Configuration.....	43
4.6.1	IP/Port Filtering .....	43
4.6.2	MAC Filtering.....	44
4.6.3	Port Forwarding .....	46
4.6.4	Parental Control.....	47
4.6.5	ALG.....	50
4.6.6	NAT Forwarding.....	51
4.6.7	NAT Pool .....	52
4.6.8	DoS.....	53
4.6.9	DMZ .....	55
4.6.10	IGMP Proxy Configuration .....	56
4.6.11	UPnP Configuration.....	57
4.6.12	RIP Configuration.....	58
4.7	Advanced.....	59
4.7.1	ARP Table .....	59
4.7.2	Bridging .....	60
4.7.3	Routing.....	61
4.7.4	SNMP Configuration.....	64
4.7.5	Port Mapping .....	66
4.7.6	IP QoS.....	67
4.7.7	DNS Server.....	69
4.7.8	Dynamic DNS .....	69
4.7.9	ACL.....	71
4.7.9.1	ACL LAN .....	72
4.7.9.2	ACL WAN .....	73
4.7.10	Other .....	74
4.8	Admin .....	74
4.8.1	Save & Reboot.....	75
4.8.2	Backup/Restore.....	75
4.8.3	System Log.....	75
4.8.4	Password .....	76



4.8.5	Upgrade Firmware.....	78
4.8.6	Time Zone .....	78
4.8.7	Green AP .....	80
4.8.8	TR-069 Config (Optional) .....	80
5	Troubleshooting Guide .....	83
6	Appendix.....	85



# 1 Introduction

The 54 Mbps Wireless G Modem Router user manual contains the guidance to install and configure LogN HN-DR4PG Wireless 54 Mbps Wireless G Modem Router using the Web GUI.

## 1.1 Intended Audience

This manual is intended for end users to access ADSL broadband service.

## 1.2 Definitions Of Terms Used In This Document

None.

## 1.3 Acronyms Used Throughout This Document

None.

## 1.4 Usage Instructions

None.

## 1.5 Questions or Comments on This Document

Please contact us and visit our website at <http://www.logn.com.eg> should you have any questions or comments on this document.

## 2 System Overview

### 2.1 General Description

HN-DR4PG wireless router is a high-speed ADSL2+ Ethernet/Wireless Modem/Router that is specifically designed to connect to the Internet and to directly connect to your local area network (LAN) via high-speed 10/100 Mbps Ethernet, or wireless LAN (WLAN). The ADSL2+ modem is compatible with the latest ADSL standards, including ADSL2 and ADSL2+, and supports up to 26 Mbps downstream and 3 Mbps upstream to deliver true broadband speed and throughput. The DSL router supports wireless 802.11b/g and the following security protocols: WEP, WPA, WPA2, and 802.1x.

To ensure fully compatibility, the DSL device was tested with all major DSLAMs, and support standard 10/100 Mbps Base-T Ethernet interface Auto MDI/MDIX 10/100 Switch function allowing user easily to link to PC or other Switches/Hubs. The DSL device is an idea solution for multi-users utilizing build-in channel mode (PPPoE/A, IPoA, IPoE), IP routing, NAT functionalities sharing the ADSL link. The DSL device is also a perfect solution for the residential users, it supports the users with bridge mode in host based PPPoE Client.

### 2.2 Specifications

#### ADSL Standard

- ITU-T G.992.1(G.dmt)
- ANSI T1.413 Issue 2
- G.992.2 (G.lite)
- G.994.1 (G.hs)
- Auto-negotiating rate adaptation
- ADSL2 G.dmt.bis (G.992.3)
- ADSL2 G.lite.bis (G.992.4)
- ADSL2+ (G.992.5)

#### Wireless Features

- Compliant with IEEE 802.11 B/G
- Up to 54 Mbps wireless operation rate
- 64/128 bits WEP for security
- WPA/WPA2
- WDS
- WPS (C2C)
- ACL (MAC address Filtering)



### **Software Features**

- RFC-1483/2684 LLC/VC-Mux bridged/routed mode
- RFC-1577 Classical IP over ATM
- RFC-2516 PPPoE
- RFC-2364 PPPoA
- ITU-T 1.610 F4/F5 OAM send and receive loop-back
- 802.1d Spanning-Tree Protocol
- DHCP Client/Server/Relay
- NAT
- RIP v1/v2
- DNS Relay Agent
- DMZ support
- IGMP Proxy/Snooping
- Stateful Packet Inspection
- Protection against Denial of Service attacks
- IP Packet Filtering
- QoS
- Dynamic DNS
- UPnP support

### **Management**

- Web-based Configuration
- Menu-driven Command-line Interpreter
- Telnet Remote Management
- SNMP v1/v2/Trap
- Firmware upgrade through FTP, TFTP and HTTP
- Configuration backup/restore
- Diagnostic Tool



## 2.3 Hardware Description

### 2.3.1 Front View



LED	State	Description
Power	OFF	System is OFF
	ON-RED	System is starting up
	ON-Yellow	System is ON
WPS	OFF	WPS Disabled
	ON-Yellow	WPS stable
	Blinking-Yellow	Awaiting or communicating
WLAN	OFF	Wireless radio is disabled
	Blinking-Yellow	Wireless radio is enabled and active
LAN1-4	OFF	No Cable is connected between Device and active Client
	ON-Yellow	Cable is connected between Device and active Client
	Blinking-Yellow	Data is transferred between Device and active Client
ADSL	Blinking-Yellow	Establishing ADSL connection with ISP
	ON-Yellow	ADSL connection is established and stable
Internet	OFF	No Internet connection with ISP
	Blinking-Yellow	Internet connection is established and data is being transferred
	ON-Yellow	Internet connection is established but no data is being transferred

### 2.3.2 Rear View



## 3 Getting Started

Before you start, Please make sure you have all the contents in the package and that you meet the minimum system requirement:

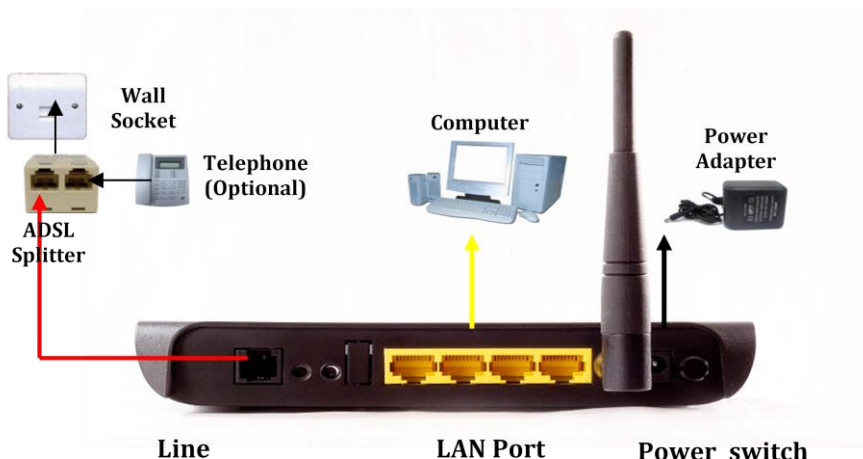
### 3.1 Package Contents

- HN-DR4PG Wireless Modem Router
- Power Adapter
- 1 x RJ-11 Telephone Cable
- 1 x RJ-45 LAN Cable
- Quick Installation Guide
- CD
- 1 x ADSL Splitter (Optional)

### 3.2 Minimum System Requirements

- ADSL Subscription
- PC with Ethernet Port and/or Wireless
- WiFi Module for non wireless-enabled PCs

### 3.3 Hardware Installation



1. Connect one end of the telephone cable to the ADSL port on the ADSL router.
2. Connect the other end of the telephone cable into the ADSL port of the ADSL splitter or directly to the wall phone socket.
3. Connect the ADSL splitter line port to the wall phone socket whereby the ADSL service is activated.
4. Connect one end of the LAN cable to the LAN port of the ADSL router.
5. Connect the other end of the LAN cable to the LAN port of your PC or laptop.
6. Connect the power adapter to the power socket.
7. Switch on your ADSL router. The "Power" LED will start in RED.
8. Wait until the "Power", "LAN" and "ADSL" LEDs are lit ON and fixed. The "WLAN" will be blinking. The "Internet" LED will depend on your ISP Internet connection settings.

**To connect to the device wirelessly, replace steps 4-5 with:**

1. Switch your PC WiFi radio on
2. Search for LogN\_HN-DR4PG, connect to it.

### 3.4 Software Quick Configuration

When you power on the device, the system will boot up and connect to ADSL automatically. The system provides a PVC for bridge test by default. The default configurations for the system are listed below:

LAN IP address: **192.168.1.1**, NetMask: **255.255.255.0**

UART setting: 115200bps, 8 bits, no parity, 1 stop bit, no flow control.

VPI/VCI for ATM: **0/35**

ADSL Line mode: Auto-detect.

This is what causes the “ADSL” LED blink first then lit ON and fixed at the end meaning the ADSL connection to the ISP is established.

**NOTE:** This does not mean that you are connected to the Internet, as this depends on your ISP Internet connection settings that your ISP should provide. In a special case of ISP Internet settings, you may get connected to Internet automatically and having the “Internet” LED lit on.

**To set the ISP connection settings via WEB browser, the following sections describe the quick set up procedures:**

1. Please set your PCs Ethernet port as follow:  
**IP address:** 192.168.1.XXX (*e.g. 192.168.1.10*)  
**NetMask:** 255.255.255.0
2. Start your web browser.
3. Type the Ethernet IP address of the modem/router on the address bar of the browser.  
**Default IP address:** 192.168.1.1.
4. Whenever the “Enter Network Password” dialog box appears, type:  
**Default Username:** admin  
**Password:** password
5. Once you are connected to the modem/router, you will see the “ADSL Router Status” page. Make sure that “DSL” status shows information for “Operational Status”, “Upstream Speed” and “Downstream Speed” like:  
**Operational Status:** G992.5, SHOWTIME.L0(Interleave)  
**Upstream Speed:** 126 kbps  
**Downstream Speed:** 511 kbps
6. Click on “Quick Setup” button. Refer to section “Quick Setup” to see description of the page.

7. Type the ISP Internet connection User Name and password provided by your ISP.
8. Save and Reboot.
9. Wait until "Internet" LED is constantly ON. The "ADSL" LED should be ON as well.
10. If the LEDs are ON, you should be connected to the internet. Start your browser and surf internet freely.

**If these quick setup procedures failed to connect you to the internet, you may have advanced ADSL connection settings that need more details:**

1. Repeat steps 1-4 of last procedure.
2. Click on "Internet Interface" and select "WAN Configuration". Refer to section "Internet Interface" to see description of the page.
3. Select one of the connections shown in the table. Modify it to exactly meet your ISP connection settings then press "Modify".
4. Press the "Save" button on the right down part of the screen.
5. Wait until "Internet" LED is constantly ON. The "ADSL" LED should be ON as well.
6. If the LEDs are ON, you should be connected to the internet. Start your browser and surf internet freely.

**To configure more features, Please refer to "Graphical User Interface pages" chapter at the section of the feature you want to configure.**

## 4 Graphical User Interface Pages

### 4.1 Status

#### 4.1.1 Status

It displays the ADSL modem/router's current status and settings. This information is read-only except for the PPPoE/PPPoA channel for which user can connect/disconnect the channel on demand. Click the "Refresh" button to update the status

### ADSL Router Status

This page shows the current status and some basic settings of the device.

---

System	
Alias Name	HN-DR4PG ADSL Wireless Modem
Uptime	0 0:22:56
Firmware Version	RTK V2.1-Log 4WG 2.5R
DSP Version	2.9.0.73
Name Servers	---
Default Gateway	0.0.0.0
DSL	
Operational Status	--, ACTIVATING(--)
Upstream Speed	--
Downstream Speed	--
LAN Configuration	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	000b2b3ed9ff

WAN Configuration						
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
pppoe1	0/33	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe2	0/35	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe3	0/100	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe4	1/33	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe5	1/35	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe6	8/33	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe7	8/35	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>
pppoe8	8/81	LLC	PPPoE	0.0.0.0	0.0.0.0	down 0:0:0 / 0:0:0 <input type="button" value="connect"/>



Function buttons in this page:

### Connect / Disconnect

The two buttons take effect only when PVC is configured as PPPoE/PPPoA mode. Click Connect/Disconnect button to connect/disconnect the PPP dial up link.

### Refresh

Click to display updated data since you opened this page.

## 4.1.2 Diagnostic Test

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

### Diagnostic Test

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

---

Select the Internet Connection:

LAN Connection Check	
Test Ethernet LAN Connection	PASS

ADSL Connection Check	
Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	FAIL
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

Internet Connection Check	
Test PPP Server Connection	PASS
Test Authentication with ISP	PASS
Test the assigned IP Address	PASS
Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS

Fields in this page:





Field	Description
Select the Internet Connection	The available WAN side interfaces are listed. You have to select one for the WAN side diagnostic.

Function buttons in this page:

**Run Diagnostic Test**

Click to run the test and see the different layer of network statistics information.

**4.1.3 Interfaces**

You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

**Statistics -- Interfaces**

This page shows the packet statistics for transmission and reception regarding to network interface.

---

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
eth0	877	0	0	793	0	0
wlan0	0	0	0	11	0	0
0_33	0	0	0	0	0	0
0_35	0	0	0	0	0	0
0_100	0	0	0	0	0	0
1_33	0	0	0	0	0	0
1_35	0	0	0	0	0	0
8_33	0	0	0	0	0	0
8_35	0	0	0	0	0	0
8_81	0	0	0	0	0	0

Function buttons in this page:

**Refresh**

Click to display updated data since you opened this page.

**4.1.4 ADSL**

This page shows the ADSL line statistic information.



## Statistics -- ADSL Line

<b>Mode</b>	
<b>Latency</b>	
<b>Trellis Coding</b>	Enable
<b>Status</b>	ACTIVATING.
<b>Power Level</b>	L0

	Downstream	Upstream
<b>SNR Margin (dB)</b>	0.0	0.0
<b>Attenuation (dB)</b>	0.0	0.0
<b>Output Power (dBm)</b>	0.0	25.5
<b>Attainable Rate (Kbps)</b>	0	0
<b>Rate (Kbps)</b>	0	0
<b>K (number of bytes in DMT frame)</b>		
<b>R (number of check bytes in RS code word)</b>		
<b>S (RS code word size in DMT frame)</b>		
<b>D (interleaver depth)</b>		
<b>Delay (msec)</b>		
<b>FEC</b>	0	0
<b>CRC</b>	0	0
<b>Total ES</b>	0	0
<b>Total SES</b>	0	0
<b>Total UAS</b>	0	0

## 4.2 Quick Setup

This page is used as a wizard to help you quickly configure the device. The page asks the user for User name and password provided by the ISP for password protected connections. Once the user types the ISP connection username and password, he can Commit and Reboot to let the device saves configuration, negotiate with ISP automatically, communicate user name and password and connect user in most cases automatically. (Internet LED is ON)

The user as well can configure the state of wireless radio, enabled or disabled, if enabled, secure or not, what the SSID is? What the Encryption format and key are?

Wireless LAN is enabled by default.


User would better consult Wireless Section to read more about the details that show here.


User may disable wireless on this page until he is back with enough information to configure wireless from its page.

### Quick Setup

#### Your Internet Login Account

Username and/or Password not correct, authentication fail. Please try again.

 Username

 Password

**Disable Wireless LAN Interface**

SSID:

Channel Number:

Encryption:

WPA Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

Pre-Shared Key Format:

Pre-Shared Key:

Authentication RADIUS Server: Port  IP address  Password

Function buttons in this page:

### **Commit and Reboot**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

## 4.3 LAN Interface

### 4.3.1 IP Address

This page shows the current setting of LAN interface. You can set IP address, subnet mask, and IGMP Snooping for LAN interface in this page.

## LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP address, subnet mask, etc..

Interface Name: **br0**

IP Address:

Subnet Mask:

Secondary IP

IGMP Snooping:  Disabled  Enabled

Apply Changes

Undo

### Fields in this page:

Field	Description
IP Address	The IP address your LAN hosts use to identify the device's LAN port.
Subnet Mask	LAN subnet mask.
Secondary IP	The second IP address your LAN hosts use to identify the device's LAN port.
IGMP Snooping	Enable/disable the IGMP snooping function for the multiple bridged LAN ports.

### Function buttons in this page:

#### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### Undo

Discard your changes.

### When **Secondary IP** is checked

## LAN Interface Setup

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP address, subnet mask, etc..

Interface Name:	br0
IP Address:	<input type="text" value="192.168.1.1"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
<input checked="" type="checkbox"/> Secondary IP	
IP Address:	<input type="text" value="0.0.0.0"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
IGMP Snooping:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
<input type="button" value="Apply Changes"/> <input type="button" value="Undo"/>	

Fields in this page:

Field	Description
IP Address	The IP address your LAN hosts use to identify the device's LAN port.
Subnet Mask	LAN subnet mask.

### 4.3.2 DHCP Settings

You can configure your network and DSL device to use the Dynamic Host Configuration Protocol (DHCP). This page provides DHCP instructions for implementing it on your network by selecting the role of DHCP protocol that this device wants to play. There are two different DHCP roles that this device can act as: DHCP Server and DHCP Relay. When acting as DHCP server, you can setup the server parameters at the **DHCP Server** page; while acting as DHCP Relay, you can setup the relay at the **DHCP Relay** page.

#### 4.3.2.1 DHCP Server Mode

By default, the device is configured as a DHCP server, with a predefined IP address pool of 192.168.1.64 through 192.168.1.253 (subnet mask 255.255.255.0).

## DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

**DHCP Mode:**  None  DHCP Relay  DHCP Server

### DHCP Server

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

**LAN IP Address:** 192.168.1.1 **Subnet Mask:** 255.255.255.0

**IP Pool Range:** 192.168.1.2 - 192.168.1.100

**Max Lease Time:** 86400 seconds (-1 indicates an infinite lease)

**Domain Name:** domain.name



### Fields in this page:

Field	Description
IP Pool Range	Specify the lowest and highest addresses in the pool.
Max Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 86400 seconds (1 day). The value -1 stands for the infinite lease.
Domain Name	A user-friendly name that refers to the group of hosts (subnet) that will be assigned addresses from this pool.

### Function buttons in this page:

#### **Show Client**

Click to see a list with the clients connected to the LAN with their assigned IPs.

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### **MAC Based Assignment**

Click to assign IP to network clients using MAC Based Assignment.

When **Show Clients** is clicked

### Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

---

Name	IP Address	MAC Address	Expiry(s)	Type
Lpt-034	192.168.1.4	00:1e:ec:88:b7:1a	In 0 days 22:31:19	Automatic

Fields in this page:

Field	Description
Name	Shows the network name of the network Client
IP Address	Shows The IP address assigned by the DHCP server to the network Client.
MAC Address	Shows the MAC address of the network Client.
Expiry	Shows the time after which the IP address assigned to the network Client will expire
Automatic	Shows how the IP was assigned to the network Client.

Function buttons in this page:

**Refresh**

Click to display updated data since you opened this page.

**Close**

Click to close the window and go back to the main menu.

When **MAC Based Assignment** is clicked

## Static IP Assignment Table

This page is used to configure the static IP base on MAC Address. You can assign/delete the static IP. The Host MAC Address, please input a string with hex number. Such as "00:d0:59:c6:12:43". The Assigned IP Address, please input a string with digit. Such as "192.168.1.100".

**Host Name:**   
**Host MAC Address:**  (XX:XX:XX:XX:XX:XX)  
**Assigned IP Address:**  (XXX.XXX.XXX.XXX)

Assign IP

Delete Assigned IP

Close

MAC-Base Assignment Table:

Select   
  Host Name   
  Host MAC Address   
  Assigned IP Address

Fields in this page:

Field	Description
Host Name	Shows the network name of the network Client
Host MAC Address	Shows The IP address assigned by the DHCP server to the network Client.
Assigned IP Address	Shows the MAC address of the network Client.

Function buttons in this page:

### Assign IP

Click to refresh the list and update its contents.

### Delete Assigned IP

Click to delete the new Client added in the table after selecting it through the check box beside it to the left.

### Close

Click to close the window and go back to the main menu.

#### 4.3.2.2 DHCP Relay Mode

Some ISPs perform the DHCP server function for their customers' home/small office network. In this case, you can configure this device to act as a DHCP relay agent. When a host on your network requests Internet access, the device contacts your ISP to obtain the IP configuration, and then forward that information to the host. You should set the DHCP



mode after you configure the DHCP relay.

## DHCP Settings

This page be used to configure DHCP Server and DHCP Relay.

---

**DHCP Mode:**  None  DHCP Relay  DHCP Server

---

### DHCP Relay Configuration

This page is used to configure the DHCP server ip addresses for DHCP Relay.

---

**DHCP Server Address:**

Fields in this page:

Field	Description
DHCP Server Address	Specify the IP address of your ISP's DHCP server. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

Function button in this page

### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

## 4.4 Wireless

This section provides the wireless network settings for your WLAN interface. The wireless interface enables the wireless AP function for ADSL modem.

### 4.4.1 Basic Setting

This page contains all of the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.

## Wireless Basic Settings

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

**Disable Wireless LAN Interface**

**Band:**

**Mode:**

**SSID:**

**Channel Number:**

**Radio Power (mW):**

**Associated Clients:**

### Fields in this page:

Field	Description
Disable Wireless LAN Interface	Check it to disable the wireless function for ADSL modem.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	The selections are: AP
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations shall select the same SSID to be able to communicate with your ADSL modem (or AP).
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You shall assign a different channel for each AP to avoid signal interference.
Radio Power (mW)	The maximum output power: 15mW, 30mW or 60mW.

### Function buttons in this page:

#### **Show Active Clients**

Click it will show the clients currently associated with the ADSL modem.

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

When Show **Active Clients** is clicked

### Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

---

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Refresh
Close

Fields in this page:

Field	Description
MAC Address	Shows the MAC address of the wireless Client.
TX Packet/ RX Packet/ Tx Rate/ Power Saving/ Expired Time	Shows some parameters of the wireless Client.

Function buttons in this page:

**Refresh**

Click to display updated data since you opened this page.

**Close**

Click to close the window and go back to the main menu.

**4.4.2 Advanced Settings**

This page allows advanced users who have sufficient knowledge of wireless LAN. These setting shall not be changed unless you know exactly what will happen for the changes you made on your DSL device.



## Wireless Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

**Authentication Type:**                     Open System    Shared Key    Auto  
**Fragment Threshold:**                 (256-2346)  
**RTS Threshold:**                         (0-2347)  
**Beacon Interval:**                       (20-1024 ms)  
**Data Rate:**                                 ▾  
**Preamble Type:**                         Long Preamble    Short Preamble  
**Broadcast SSID:**                         Enabled    Disabled  
**Relay Blocking:**                          Enabled    Disabled  
**Ethernet to Wireless Blocking:**     Enabled    Disabled  
**Wifi Multicast to Unicast:**          Enabled    Disabled  
**WMM:**                                         Enabled    Disabled

Apply Changes

### Fields in this page:

Field	Description
Authentication Type	<p><b>Open System:</b> Open System authentication is not required to be successful while a client may decline to authenticate with any particular other client.</p> <p><b>Shared Key:</b> Shared Key is only available if the WEP option is implemented. Shared Key authentication supports authentication of clients as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in clear. Requiring the use of the WEP privacy mechanism.</p> <p><b>Auto:</b> Auto is the default authentication algorithm. It will change its authentication type automatically to fulfill client's requirement.</p>
Fragment Threshold	<p>This value should remain at its default setting of 2346. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increases the "Fragment Threshold" value within the value range of 256 to 2346. Setting this value too low may result in poor network performance. Only minor modifications of this value are recommended.</p>
RTS Threshold	<p>This value should remain at its default setting of 2347. Should you encounter</p>

	inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset "RTS threshold" size, the RTS/CTS mechanism will not be enabled. The ADSL modem (or AP) sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.
Beacon Interval	The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1024. A beacon is a packet broadcast by the ADSL modem (or AP) to synchronize the wireless network. The default is 100.
Data Rate	The rate of data transmission should be set depending on the speed of your wireless network. You should select from a range of transmission speeds, or you can select <i>Auto</i> to have the ADSL modem (or AP) automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the AP and a wireless client. The default setting is <i>Auto</i> .
Preamble Type	The Preamble Type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and mobile wireless stations. Make sure to select the appropriate preamble type. Note that high network traffic areas should use the <i>short preamble</i> type. CRC is a common technique for detecting data transmission errors.
Broadcast SSID	If this option is enabled, the device will automatically transmit their network name (SSID) into open air at regular interval. This feature is intended to allow clients to dynamically discover and roam between WLANs; if this option is disabled, the device will hide its SSID. When this is done, the station cannot directly discover its WLAN and MUST be configure with the SSID. Note that in a home Wi-Fi network, roaming is largely unnecessary and the SSID broadcast feature serves no useful purpose. You should disable this feature to improve the security of your WLAN.
Relay Blocking	When <b>Relay Blocking</b> is enabled, wireless clients will not be able to directly access other wireless clients.
Ethernet to Wireless Blocking	When enabled, traffic between Ethernet and wireless interfaces are not allowed.
WiFi Muticast to Unicast	Router receives Multicast streams from the network backbone, converts them to Unicast format, and routes them to the end-users over the last mile infrastructure (e.g. DSL, Ethernet, WiFi).
WMM	Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia

(WMM) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones (VoWLAN).

Function buttons in this page:

### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

### 4.4.3 MBSSID

Multiple BSSID allows user to configure more than one virtual access point (VAP), each virtual interface is assigned to its own basic service set identifier (BSSID), or MAC address, which provides a better user experience. This is implemented in most off-the-shelf APs equipped with the multiple SSID feature.

## Wireless Multiple BSSID Setup

This page allows you to set virtual access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

---

Enable VAP0

SSID:

broadcast SSID:  Enable  Disable

Authentication Type:  Open System  Shared Key  Auto

---

Enable VAP1

SSID:

Broadcast SSID:  Enable  Disable

Authentication Type:  Open System  Shared Key  Auto

**Enable VAP2**

SSID:

Broadcast SSID:  Enable  Disable

Authentication Type:  Open System  Shared Key  Auto

---

**Enable VAP3**

SSID:

Broadcast SSID:  Enable  Disable

Authentication Type:  Open System  Shared Key  Auto

Fields in this page:

Field	Description
Enable VAP1-3	To enable Virtual Access Point 1 to 3.
SSID	Service set identifier, or SSID, is a name that identifies a particular 802.11 wireless LAN.
Broadcast SSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Authentication Type	Authentication protocol available for MBSSID.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.4.4 Security**

This screen allows you to setup the wireless security. Turn on WEP or WPA by using encryption keys could prevent any unauthorized access to your WLAN.

## Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE:  Root  VAP0  VAP1  VAP2  VAP3

Encryption:

Use 802.1x Authentication  WEP 64bits  WEP 128bits

WPA Authentication Mode:  Enterprise (RADIUS)  Personal (Pre-Shared Key)

Pre-Shared Key Format:

Pre-Shared Key:

Authentication RADIUS Server: Port  IP address  Password

*Note: When encryption WEP is selected, you must set WEP key value.*

### Fields in this page:

Field	Description
SSID Type	Choose the SSID type where wireless security to be configured with.
Encryption	<p>There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature.</p> <p><b>WEP:</b> Make sure that all wireless devices on your network are using the same encryption level and key. Click <i>Set WEP Key</i> button to set the encryption key.</p> <p><b>WPA (TKIP):</b> WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.</p> <p><b>WPA2 (AES):</b> WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption.</p> <p><b>WAP2 Mixed:</b> The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.</p>
Use 802.1x	Check it to enable 802.1x authentication. This option is selectable only



Authentication	when the “Encryption” is choose to either <i>None</i> or <i>WEP</i> . If the “Encryption” is <i>WEP</i> , you need to further select the WEP key length to be either <i>WEP 64bits</i> or <i>WEP 128bits</i> .
WPA Authentication Mode	There are 2 types of authentication mode for WPA. <b>WPA-RADIUS:</b> WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to “Authentication RADIUS Server” setting below for RADIUS setting. The WPA algorithm is selected between TKIP and AES, please refer to “WPA cipher Suite” below. <b>Pre-Shared Key:</b> Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the “Pre-Shared Key Format” and “Pre-Shared Key” setting respectively. Please refer to “Pre-Shared Key Format” and “Pre-Shared Key” setting below.
Pre-Shared Key Format	<b>PassPhrase:</b> Select this to enter the Pre-Shared Key secret as user-friendly textual secret. <b>Hex (64 characters):</b> Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the “Pre-Shared Key Format” is specified as <i>PassPhrase</i> , then it indicates a passphrase of 8 to 63 bytes long; or if the “Pre-Shared Key Format” is specified as <i>PassPhrase</i> , then it indicates a 64-hexadecimal number.
Authentication RADIUS Server	If the <i>WPA-RADIUS</i> is selected at “WPA Authentication Mode”, the port (default is 1812), IP address and password of external RADIUS server are specified here.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.4.5 Access Control**

This page allows administrator to have access control by enter MAC address of client stations. When Enable this function, MAC address can be added into access control list and only those clients whose wireless MAC address are in the access control list will be able to connect to your DSL device (or AP).



## Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

**Wireless Access Control Mode:**

**MAC Address:**  (ex. 000B2B710302)

### Current Access Control List:

MAC Address	Select
00:0b:23:e3:22:ac	<input type="checkbox"/>

### Fields in this page:

Field	Description
Wireless Access Control Mode	<p>The Selections are:</p> <ul style="list-style-type: none"> <li>Disable</li> <li>Disable the wireless ACL feature.</li> <li>Allow Listed</li> </ul> <p>When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device).</p> <ul style="list-style-type: none"> <li>Deny Listed</li> </ul> <p>When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device).</p>
MAC Address	Enter client MAC address and press "Apply Changes" button to add client MAC address into current access control list.

### Function buttons for the setting block:

#### Apply Changes

Click to add this entry into the **Current Access Control List**.

#### Reset

Discard your changes.

The **Current Access Control List** lists the client MAC addresses. Any wireless client with its

MAC address listed in this access control list will be able to connect to the device. You can select the entries at the Select column and apply to the following function buttons.

Function buttons for the Current Access Control List:

**Delete Selected**

Delete the selected entries from the list.

**Delete All**

Flush the list.

**Reset**

Discard your changes.

#### 4.4.6 C2C

Although home Wi-Fi networks have become more and more popular, users still have trouble with the initial set up of network. This obstacle forces users to use the open security and increases the risk of eavesdropping. Therefore, The Wi-Fi Protected Setup (WPS) is designed to ease set up of security-enabled Wi-Fi networks and subsequently network management (Wi-Fi Protected Setup Specification 1.0h.pdf, p. 8).

The largest difference between WPS-enabled devices and legacy devices is that users do not need the knowledge about SSID, channel and security settings, but they could still surf in a security-enabled Wi-Fi network.

This device supports Push Button method and PIN method for WPS. The following sub-paragraphs will describe the function of each item. The webpage is as below.

## Wi-Fi Protected Setup

This page allows you to change the setting for C2C (Click To Connect). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

Disable C2C

C2C Status:

Configured  UnConfigured

Self-PIN Number:

12345670

Regenerate PIN

Push Button Configuration:

Start PBC

Apply Changes

Reset

Client PIN Number:

Start PIN

### Fields in this page:

Field	Description
Disable C2C	Check to disable the Click to Connect Setup.
C2C Status	When AP's settings are factory default (out of box), it is set to open security and un-configured state. "C2C Status" will display it as "UnConfigured". If it already shows "Configured", some registrars such as Vista WCN will not configure AP. Users will need to go to the "Backup/Restore" page and click "Reset" to reload factory default settings.
Self-PIN Number	"Self-PIN Number" is AP's PIN. Whenever users want to change AP's PIN, they could click "Regenerate PIN" and then click "Apply Changes". Moreover, if users want to make their own PIN, they could enter four-digit PIN without checksum and then click "Apply Changes". However, this would not be recommended since the registrar side needs to be supported with four-digit PIN.
Push Button Configuration	Clicking this button will invoke the PBC method of C2C. It is only used when AP acts as a registrar.
Client PIN Number	It is only used when users want their station to join AP's network. The length of PIN is limited to four or eight numeric digits. If users enter eight-digit PIN with checksum error, there will be a warning message

popping up. If users insist on this PIN, AP will take it.

Function buttons in this page:

**Regenerate PIN**

Click to regenerate the Self-PIN Number.

**Start PBC**

Click to start the Push Button method of WPS.

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Reset**

Discard your changes.

**Start PIN**

Click to start the PIN method of WPS.

## 4.5 Internet Interface

There are three sub-menus for WAN configuration: [Channel Config], [ATM Settings], and [ADSL Settings].

### 4.5.1 WAN Configuration

ADSL modem/router comes with 8 ATM Permanent Virtual Channels (PVCs) at the most. There are mainly three operations for each of the PVC channels: add, delete and modify. And there are several channel modes to be selected for each PVC channel. For each of the channel modes, the setting is quite different accordingly.

**WAN Configuration**

This page is used to configure the parameters for the channel operation modes of your ADSL Modem/Router.

---

Current ATM VC Table:

Select	Inf	Mode	VPI	VCI	Encap	NAPT	IP Addr	Remote IP	Subnet Mask	User Name	Status	Actions
<input type="radio"/>	pppoe1	PPPoE	0	33	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe2	PPPoE	0	35	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe3	PPPoE	0	100	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe4	PPPoE	1	33	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe5	PPPoE	1	35	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe6	PPPoE	8	33	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe7	PPPoE	8	35	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	
<input type="radio"/>	pppoe8	PPPoE	8	81	LLC	On	0.0.0.0	0.0.0.0	0.0.0.0		Enable	



VPI: <input type="text" value="0"/>	VCI: <input type="text"/>	Encapsulation: <input checked="" type="radio"/> LLC <input type="radio"/> VC-Mux	Channel Mode: <input type="text" value="1483 Bridged"/>
Enable NAPT: <input type="checkbox"/>	Admin Status: <input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<hr/>			
PPP Settings:	User Name: <input type="text"/>	Password: <input type="text"/>	
	Type: <input type="text" value="Continuous"/>	Idle Time (min): <input type="text"/>	
<hr/>			
WAN IP Settings:	Type: <input checked="" type="radio"/> Fixed IP <input type="radio"/> DHCP		
	Local IP Address: <input type="text"/>	Remote IP Address: <input type="text"/>	
	Subnet Mask: <input type="text"/>	Unnumbered <input type="checkbox"/>	
<input type="button" value="Add"/> <input type="button" value="Modify"/>			

### Function buttons in this page:

#### **NEW PVC**

Click to add a New PVC, It will add new PVC when the available PVCs shown in the table are less than 8.

#### **Delete Selected**

Select an existing PVC channel to be deleted by clicking the radio button at the **Select** column of the **Current ATM VC Table**. Click **Delete** to delete this PVC channel from configuration.

#### **ADD**

Click **Add** to complete the channel setup and add this PVC channel into configuration.

#### **Modify**

Select an existing PVC channel by clicking the radio button at the **Select** column of the **Current ATM VC Table** before we can modify the PVC channel. After selecting an PVC channel, we can modify the channel configuration at this page. Click **Modify** to complete the channel modification and apply to the configuration.

ADSL router supports multiple channel operation modes. This section will show procedures to configure the router.

#### 4.5.1.1 PPPoE Mode

1. Select the Channel Mode to "PPPoE". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
2. Enter user/password from your ISP.
3. Click "Add" button to add this channel.
4. Enable DHCP server to allow the local PCs share the PPP connection. Reference to

section DHCP Settings.

5. Set DNS address from your ISP. Reference to section DNS.
6. Open the WEB page at "Admin/Commit/Reboot". Press "Commit" to save the settings into flash memory.
7. The new settings will take effect after reboot the system.

#### 4.5.1.2 PPPoA Mode

1. Select the Channel Mode to "PPPoA". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
2. Enter user/password from your ISP.
3. Click "Add" button to add this channel.
4. Enable DHCP server to allow the local PCs share the PPP connection. Reference to section DHCP Settings.
5. Set DNS address from your ISP. Reference to section DNS.
6. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
7. The new settings will take effect after reboot the system.

#### 4.5.1.3 Bridge Mode

1. Select your VPI/VCI under ATM VC table
2. Change the Channel Mode to "1483 Bridged". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
3. Click "Add" button to add this channel into VC table.
4. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
5. The new settings will take effect after reboot the system.

#### 4.5.1.4 1483 Routed Mode

1. Select the Channel Mode to "1483 Routed". Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM's setting.
2. In WAN IP settings, give the local and remote IP address from your ISP or use DHCP to get them automatically if your ISP support it. Local IP is the address of ADSL router. Remote IP is the ISP's gateway address.
3. Click "Add" button to add this channel.
4. Open the WEB page at "Admin/ Commit/Reboot". Press "Commit" to save the settings into flash memory.
5. The new settings will take effect after reboot the system.

#### 4.5.1.5 MER(Mac Encapsulating Routing) Mode

1. Select the Channel Mode to “1483 MER”. Set the parameters VPI/VCI and Encapsulation mode according to the CO DSLAM’s setting.
2. Set “Local IP Address:” according to the IP that ISP assign for your router. Set “Remote IP Address” to the ISP’s gateway.
3. Click “Add” button to add this channel into VC table.
4. Open the WEB page at “Admin/ Commit/Reboot”. Press “Commit” to save the settings into flash memory.
5. The new settings will take effect after reboot the system.

#### 4.5.2 ATM Setting

The page is for ATM PVC QoS parameters setting. The DSL device support 4 QoS mode —CBR/rt-VBR/nrt-VBR/UBR.

### ATM Settings

This page is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for VPI, VCI, QoS etc ...

---

VPI:  VCI:  QoS:  ▾

PCR:  CDVT:  SCR:  MBS:

**Current ATM VC Table:**

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	0	33	UBR	6000	0	---	---

#### Fields in this page:

Field	Description
VPI	Virtual Path Identifier. This is read-only field and is selected on the <b>Select</b> column in the Current ATM VC Table.
VCI	Virtual Channel Identifier. This is read-only field and is selected on the <b>Select</b> column in the Current ATM VC Table. The VCI, together with VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.
QoS	Quality of Server, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The four QoS options are:



	UBR (Unspecified Bit Rate): When UBR is selected, the SCR and MBS fields are disabled. CBR (Constant Bit Rate): When CBR is selected, the SCR and MBS fields are disabled. nrt-VBR (non-real-time Variable Bit Rate): When nrt-VBR is selected, the SCR and MBS fields are enabled. rt-VBR (real-time Variable Bit Rate): When rt-VBR is selected, the SCR and MBS fields are enabled.
PCR	Peak Cell Rate, measured in cells/sec., is the cell rate which the source may never exceed.
CDVT	Cell Delay Variation Tolerance (CDVT) is a QoS parameter in ATM network for managing traffic that is specified when a connection is set up. In CBR transmissions, CDVT determines the level of jitter that is tolerable for the data samples taken by the PCR.
SCR	Sustained Cell Rate, measured in cells/sec., is the average cell rate over the duration of the connection.
MBS	Maximum Burst Size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the peak cell rate.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Undo**

Discard your settings.

### 4.5.3 ADSL Setting

The ADSL setting page allows you to select any combination of DSL training modes.

## ADSL Settings

Adsl Settings.

---

**ADSL modulation:**

- G.Lite
- G.Dmt
- T1.413
- ADSL2
- ADSL2+

**AnnexB Option:**

- Enabled

**AnnexL Option:**

- Enabled

**AnnexM Option:**

- Enabled

**ADSL Capability:**

- Bitswap Enable
- SRA Enable

Apply Changes

Fields in this page:

Field	Description
ADSL modulation	Choose preferred xdsl standard protocols. G.lite : G.992.2 Annex A G.dmt : G.992.1 Annex A T1.413 : T1.413 issue #2 ADSL2 : G.992.3 Annex A ADSL2+ : G.992.5 Annex A
AnnexB Option	Enable/Disable ADSL2/ADSL2+ Annex B capability.
AnnexL Option	Enable/Disable ADSL2/ADSL2+ Annex L capability.
AnnexM Option	Enable/Disable ADSL2/ADSL2+ Annex M capability.
ADSL Capability	“Bitswap Enable” : Enable/Disable bitswap capability. “SRA Enable” : Enable/Disable SRA (seamless rate adaptation) capability.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

## 4.6 Firewall Configuration

Firewall contains several features that are used to deny or allow traffic from passing through the device.

### 4.6.1 IP/Port Filtering

The IP/Port filtering feature allows you to deny/allow specific services or applications in the forwarding path.

### IP/Port Filtering

Entries in this table are used to restrict certain types of data packets through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

---

**Outgoing Default Action**    Deny    Allow  
**Incoming Default Action**    Deny    Allow  

**Direction:**    **Protocol:**    **Rule Action**    Deny    Allow

**Source IP Address:**    **Subnet Mask:**    **Port:**  -

**Destination IP Address:**    **Subnet Mask:**    **Port:**  -

**Current Filter Table:**

Select	Direction	Protocol	Src Address	Src Port	Dst Address	Dst Port	Rule Action
<input type="checkbox"/>	Outgoing	TCP	192.168.1.2/24	21	192.168.1.3/24	21	Deny

#### Fields on the first setting block:

Field	Description
Outgoing Default Action	Specify the default action on the LAN to WAN forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN forwarding path.

#### Function button for first setting block:

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and

reboot the system. See section “Admin” for save details.

Fields on the second setting block:

Field	Description
Direction	Traffic forwarding direction.
Protocol	There are 3 options available: TCP, UDP and ICMP.
Rule Action	Deny or allow traffic when matching this rule.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Source Subnet Mask	Subnet-mask of the source IP.
Source Port	Starting and ending source port numbers.
Destination IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Destination Subnet Mask	Subnet-mask of the destination IP.
Destination Port	Starting and ending destination port numbers.

Function buttons for second setting block:

**ADD**

Click to save the rule entry to the configuration.

Function buttons for the **Current Filter Table:**

**Delete Selected**

Delete selected filtering rules from the filter table. You can click the checkbox at the **Select** column to select the filtering rule.

**Delete All**

Delete all filtering rules from the filter table.

**4.6.2 MAC Filtering**

The MAC filtering feature allows you to define rules to allow or deny frames through the device based on source MAC address, destination MAC address, and traffic direction.

## MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Outgoing Default Action**  Deny  Allow

**Incoming Default Action**  Deny  Allow

Apply Changes

**Direction:**  **Rule Action**  Deny  Allow

**Source MAC Address:**

**Destination MAC Address:**

Add

**Current Filter Table:**

Select	Direction	Src MAC Address	Dst MAC Address	Rule Action
<input type="checkbox"/>	Outgoing	00-09-5b-a0-17-ff	00-09-5b-a0-17-ff	Deny

Delete Selected

Delete All

Fields on the first setting block:

Field	Description
Outgoing Default Action	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Action	Specify the default action on the WAN to LAN bridging/forwarding path.

Function button for first setting block:

### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Fields on the second setting block:

Field	Description
Direction	Traffic bridging/forwarding direction.
Rule Action	Deny or allow traffic when matching this rule.
Source MAC Address	he source MAC address. It must be xxxxxxxxxxxx format. Blanks can be used in the MAC address space and are considered as don't care.
Destination MAC	The destination MAC address. It must be xxxxxxxxxxxx format. Blanks

Address can be used in the MAC address space and are considered as don't care.

Function buttons for second setting block:

**ADD**

Click to save the rule entry to the configuration.

Function buttons for the **Current Filter Table**:

**Delete Selected**

Delete selected filtering rules from the filter table. You can click the checkbox at the **Select** column to select the filtering rule.

**Delete All**

Delete all filtering rules from the filter table.

**4.6.3 Port Forwarding**

Firewall keeps unwanted traffic from the Internet away from your LAN computers. Add a Port Forwarding entry will create a tunnel through your firewall so that the computers on the Internet can communicate to one of the computers on your LAN on a single port.

### Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

---

Port Forwarding:  Disable  Enable

---

Protocol:  Comment:   Enable

Local IP Address:  Local Port:  -

Setting:  Public Port:  -

Interface:

**Current Port Forwarding Table:**

Select	Local IP Address	Protocol	Local Port	Comment	Enable	Global IP Address /If	Public Port
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>							

Fields in this page:

Field	Description
Port Forwarding	Check this item to enable the port-forwarding feature.
Protocol	There are 3 options available: TCP, UDP and Both.
Comment	To provide any remarkable notes for ease identification.
Enable	Check this item to enable this entry.
Local IP Address	IP address of your local server that will be accessed by Internet.
Local Port	The destination port number that is made open for this application on the LAN-side.
Settings	Selects between Interface and IP address
Interface	Select the WAN interface on which the port-forwarding rule is to be applied.
Remote IP Address	The source IP address from which the incoming traffic is allowed. Leave blank for all.
Public Port	The destination port number that is made open for this application on the WAN-side

Function buttons for the setting block:

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### **ADD**

Click to save the rule entry to the configuration.

Function buttons for the Current Port Forwarding Table:

#### **Delete Selected**

Delete the selected port forwarding rules from the forwarding table. You can click the checkbox at the **Select** column to select the forwarding rule.

#### **Delete All**

Delete all forwarding rules from the forwarding table

### **4.6.4 Parental Control**

Parental controls provide parents with automated tools to help protect their children and set restrictions while using devices and services. The control includes: URL blocking and Domain blocking.

#### URL Blocking

In URL (Uniform Resource Locator) blocking, requests to a network are examined to decide if a specific URL is to be allowed or denied access.

### Domain Blocking

Provides the ability to block/filter web sites visited based upon categories. This provides for corporate, educational and parental control over the type of sites that are deemed appropriate by the networks owner.

## Parental Control

This page is used to configure the filtered URL and domain. Here you can add/delete filtered URL and domain, and you can also add/delete excluded IP from which packets free from these URL filtering rules.

URL Blocking Capability:  Disable  Enable

Domain Blocking Capability:  Disable  Enable

Apply Changes

Block Any URL

URL  Domain Blocking:

Days:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time: From : to : (e.g. From 09:21 to 18:30)

Add Filter



**URL Blocking Table:**

Select	Filtered URL	Days	Time
Delete Selected URL			

**Domain Blocking Table:**

Select	Blocked Domain	Days	Time
Delete Selected Domain			

---

**Excluded IP:**

**Excluded IP Table:**

Select	Excluded IP
--------	-------------

Fields on the first setting block:

Field	Description
URL Blocking Capability	To enable filtering based on URL. Default value is "disabled".
Domain Blocking Capabilities	To enable filtering based on Domain. Default value is "disabled".

Function button for first setting block:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Fields on the second setting block:

Field	Description
Block any URL	Basically ALL URL is to be blocked. Default value is "unchecked".
URL	To block only URL
Domain Blocking	To block only Domain, provide domain, if selected.
Days	Check days which to comply with the filtering.
Time	Provide time from and time to which to comply with the filtering.

Function buttons for second setting block:

**ADD Filter**

Click to save the rule entry to the **URL Blocking Table**.

**Delete Selected URL**

Click to delete the entry from the **URL Blocking Table**.

**Delete Selected Domain**

Click to delete the entry from the **Domain Blocking Table**.

Fields on the third setting block:

Field	Description
Excluded IP	IP address provided will be excluded from all filter settings.

Function buttons for third setting block:

**ADD IP**

Click to save the rule entry to the **Excluded IP Table**.

**Delete Selected IP**

Click to delete the entry from the **Excluded IP Table**.

#### 4.6.5 ALG

An application-level gateway (also known as ALG or application layer gateway) consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, BitTorrent, SIP, RTSP, file transfer in IM applications etc. In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the control traffic and open up port mappings (firewall pinhole) dynamically as required.

## NAT ALG and Pass-Through

Setup NAT ALG and Pass-Through configuration

IPSec Pass-Through:	<input checked="" type="checkbox"/> Enable
L2TP Pass-Through:	<input checked="" type="checkbox"/> Enable
PPTP Pass-Through:	<input checked="" type="checkbox"/> Enable
FTP:	<input checked="" type="checkbox"/> Enable
H.323:	<input checked="" type="checkbox"/> Enable
SIP:	<input checked="" type="checkbox"/> Enable
RTSP:	<input checked="" type="checkbox"/> Enable
ICQ:	<input checked="" type="checkbox"/> Enable
MSN:	<input checked="" type="checkbox"/> Enable

Fields in this page:

Field	Description
IPSec pass-Through	Default Value is "Enabled"
L2TP Pass-Through	Default Value is "Enabled"
PPTP Pass-Through	Default Value is "Enabled"
FTP	Default Value is "Enabled"
H.323	Default Value is "Enabled"
SIP	Default Value is "Enabled"
RTSP	Default Value is "Enabled"
ICQ	Default Value is "Enabled"
MSN	Default Value is "Enabled"

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

**Reset**

Discard your settings.

**4.6.6 NAT Forwarding**

Network address translation only allows requests coming from the internal network to the external network, which means that it is impossible as such for an external machine to send

a packet to a machine on the internal network. In other words, the internal network machines cannot operate as a server with regards the external network.

## NAT Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

---

Local IP Address:

Remote IP Address:

Enable:

Current NAT Port Forwarding Table:

Local IP Address	Remote IP Address	State	Action

Fields in this page:

Field	Description
Local IP address	The target local host IP Address, eg: 192.168.1.123 is web server.
Remote IP address	The address known by the outside world (Wider Area Network, or WAN) is the IP address of your router.
Enable	To enable the settings

Function buttons in this page:

### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

### **Reset**

Discard your settings.

## **4.6.7 NAT Pool**

Creates an address pool from which the NAT router obtains an address when performing a dynamic translation. You can create address pools with either a single range or multiple, non-overlapping ranges. The no version removes the NAT pool.

## NAT IP POOL

Entries in this table allow you to config one IP pool for any WAN Router pvc interface,so one packet through the interface will select one IP address from pool for NAT.

---

interface:

IP Range:  -

netmask:

**Current NAT Pool Table:**

WAN Interface	Low IP	High IP	Netmask	Action

Fields in this page:

Field	Description
Interface	The WAN interface available.
IP Range	First IP address to last IP address in the NAT pool range you are creating; omitting this value in the command launches the IP NAT Pool configuration mode, in which you can enter multiple, discontinuous ranges.
Netmask	Subnet mask for any NAT pool range specified.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Reset**

Discard your settings.

**4.6.8 DoS**

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Default, the DoS is disabled.

## DoS Setting

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

- Enable DoS Prevention**
- Whole System Flood: SYN  Packets/Second
  - Whole System Flood: FIN  Packets/Second
  - Whole System Flood: UDP  Packets/Second
  - Whole System Flood: ICMP  Packets/Second
  - Per-Source IP Flood: SYN  Packets/Second
  - Per-Source IP Flood: FIN  Packets/Second
  - Per-Source IP Flood: UDP  Packets/Second
  - Per-Source IP Flood: ICMP  Packets/Second
  - TCP/UDP PortScan  Sensitivity
  - ICMP Smurf
  - IP Land
  - IP Spoof
  - IP TearDrop
  - PingOfDeath
  - TCP Scan
  - TCP SynWithData
  - UDP Bomb
  - UDP EchoChargen

Select ALL

Clear ALL

**Enable Source IP Blocking**

**Block time (sec)**

Apply Changes

Fields in this page:

Field	Description
Enable DoS prevention	To enable the feature of DoS
Enable Source IP Blocking	To enable the Source IP to be blocked.

Block Time	The duration that Source IP blocking should carry.
------------	--

Function buttons in this page:

**Select All**

Click to select all entries

**Clear All**

Click to de-select all entries

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.6.9 DMZ**

A DMZ (Demilitarized Zone) allows a single computer on your LAN to expose ALL of its ports to the Internet. Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. When doing this, the DMZ host is no longer behind the firewall.

**DMZ**

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP ) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

---

**DMZ Host:**  Disable  Enable

**DMZ Host IP Address:**

Fields in this page:

Field	Description
DMZ Host	Check this item to enable the DMZ feature.
DMZ Host IP Address	IP address of the local host. This feature sets a local host to be exposed to the Internet.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.



### 4.6.10 IGMP Proxy Configuration

Multicasting is useful when the same data needs to be sent to more than one hosts. Using multicasting as opposed to sending the same data to the individual hosts uses less network bandwidth. The multicast feature also enables you to receive multicast video stream from multicast servers.

IP hosts use Internet Group Management Protocol (IGMP) to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. This device supports IGMP proxy that handles IGMP messages. When enabled, this device acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast group on the WAN side.

When a host wishes to join a multicast group, it sends IGMP REPORT message to the device's IGMP downstream interface. The proxy sets up a multicast route for the interface and host requesting the video content. It then forwards the Join to the upstream multicast router. The multicast IP traffic will then be forwarded to the requesting host. On a leave, the proxy removes the route and then forwards the leave to the upstream multicast router.

The IGMP Proxy page allows you to enable multicast on WAN and LAN interfaces. The LAN interface is always served as downstream IGMP proxy, and you can configure one of the available WAN interfaces as the upstream IGMP proxy.

**Upstream:** The interface that IGMP requests from hosts is sent to the multicast router.

**Downstream:** The interface data from the multicast router are sent to hosts in the multicast group database.

### IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

- . Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.
- . Enable IGMP on LAN interface (downstream), which connects to its hosts.

---

**IGMP Proxy:**       Disable     Enable

**Proxy Interface:**

Fields in this page:

Field	Description
IGMP Proxy	Enable/disable IGMP proxy feature





Proxy Interface	The upstream WAN interface is selected here.
-----------------	--

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.6.11 UPnP Configuration**

The DSL device supports a control point for Universal Plug and Play (UPnP) version 1.0, and supports two key features: **NAT Traversal** and **Device Identification**. This feature requires one active WAN interface. In addition, the host should support this feature. In the presence of multiple WAN interfaces, select an interface on which the incoming traffic is present.

With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into system commands to open the ports in NAT and the firewall. The interface to open the ports on is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the DSL device as a control point back to the host making the request.

### UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable it and select WAN interface (upstream) that will use UPnP.

---

**UPnP:**     
  Disable   
  Enable

**WAN Interface:**

Fields in this page:

Field	Description
UPnP	Enable/disable UPnP feature.
WAN Interface	Select WAN interface that will use UPnP from the drop-down lists.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.



### 4.6.12 RIP Configuration

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

Most small home or office networks do not need to use RIP; they have only one router, such as the ADSL Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the ADSL Router). The ADSL Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

### RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol. This page is used to select the interfaces on your devices that use RIP, and the version of the protocol used.

RIP:  Disable  Enable

Interface:

Receive Mode:

Send Mode:

**RIP Config Table:**

Select	Interface	Receive Mode	Send Mode
<input type="checkbox"/>	br0	RIP1	RIP1
<input type="checkbox"/>	ppp0	Both	RIP2

Fields on the first setting block:

Field	Description
RIP	Enable/disable RIP feature.

Function buttons for first setting block:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

Fields on the second setting block:

Field	Description
Interface	The name of the interface on which you want to enable RIP.
Receive Mode	Indicate the RIP version in which information must be passed to the DSL device in order for it to be accepted into its routing table.
Send Mode	Indicate the RIP version this interface will use when it sends its route information to other devices.

Function buttons for second setting block:

**Add**

Add a RIP entry and the new RIP entry will be display in the table

**Delete Selected**

Delete a selected RIP entry. The RIP entry can be selected on the **Select** column of the **RIP Config Table**.

**Delete All**

Click to delete all entries

## 4.7 Advanced

### 4.7.1 ARP Table

The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known. This function is critical in local area networking as well as for routing internetworking traffic across gateways (routers) based on IP addresses when the next-hop router must be determined.

## ARP Table

This table shows a list of learned MAC addresses.

IP Address	MAC Address
192.168.1.1	00:0B:2B:3E:D9:FF
192.168.1.3	00:1E:EC:88:B7:1A

Refresh

Function buttons in this page:

### Refresh

Click to display updated data since you opened this page.

## 4.7.2 Bridging

You can enable/disable Spanning Tree Protocol and set MAC address aging time in this page.

## Bridge Configuration

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Aging Time:  (seconds)

Apply Changes

Undo

Show MACs

Fields in this page:

Field	Description
Ageing Time	Set the Ethernet address ageing time, in seconds. After [Ageing Time] seconds of not having seen a frame coming from a certain address, the bridge will time out (delete) that address from Forwarding DataBase (fdb).

Function buttons in this page:

### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

**Undo**

Discard your changes

**Show MACs**

List MAC address in forwarding table.

When **Show MACs** is clicked

**Bridge Forwarding Database Table**

This table shows a list of learned MAC addresses for this bridge.

Port No	MAC Address	Is Local?	Ageing Timer
01:80:c2:00:00:00	0	Static	300
01:00:5e:00:00:09	0	Static	300
00:1e:ec:88:b7:1a	1	Dynamic	300
00:0b:2b:3e:d9:ff	0	Static	300
ff:ff:ff:ff:ff:ff	0	Static	300

Fields in this page:

Field	Description
Port No	The Port No which the bridge forwarding to attached.
MAC Address	The MAC address of the device.
Is Local?	To indicate Static or Dynamic.
Aging Timer	To indicate Aging Timer configured.

Function buttons in this page:

**Refresh**

Click to display updated data since you opened this page.

**Close**

Click to close the window and go back to the main menu.

**4.7.3 Routing**

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing



routes that set up the default gateways for your LAN hosts and for the DSL device provide the most appropriate path for all your Internet traffic.

On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the DSL device. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.

On the DSL device itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to setup through the configuration.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

### Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

---

**Default Gateway:** Auto ▼

Apply Changes

---

**Enable:**

**Destination:**

**Subnet Mask:**

**Next Hop:**

**Metric:**

**Interface:** any ▼

Add Route
Update
Delete Selected
Show Routes

---

**Static Route Table:**

Select	State	Destination	Subnet Mask	NextHop	Metric	IF
--------	-------	-------------	-------------	---------	--------	----

Fields in first section of the page:

Field	Description
Default Gateway	Select your default gateway

Function buttons for first section:

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and



reboot the system. See section “Admin” for save details.

Fields in the second section of the page:

Field	Description
Enable	Check to enable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.
Interface	The WAN interface to which a static routing subnet is to be applied.

Function buttons for second section:

**Add Route**

Add a user-defined destination route.

**Update**

Update the selected destination route on the **Static Route Table**.

**Delete Selected**

Delete a selected destination route on the **Static Route Table**.

**Show Routes**

Click this button to view the DSL device’s routing table.

When **Show Routes** is clicked



## IP Route Table

This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	NextHop	Metric	Iface
192.168.1.0	255.255.255.0	*	0	br0
127.0.0.0	255.255.255.0	*	0	lo

Refresh

Close

### Fields in this page:

Field	Description
Destination	The IP Address of the destination.
Subnet Mask	The Subnet Mask address of the destination.
Next Hop	The Next Hop IP address.
Metric	Defines the number of hops between network nodes that data packets travel.
Interface	The WAN interface to which a static routing subnet is to be applied.

### Function buttons in this page:

#### Refresh

Click to display updated data since you opened this page.

#### Close

Click to close the window and go back to the main menu.

## 4.7.4 SNMP Configuration

Simple Network Management Protocol (SNMP) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The DSL device can be managed locally or remotely by SNMP protocol.



## SNMP Protocol Configuration

This page is used to configure the SNMP protocol. Here you may change the setting for system description, trap ip address, community name, etc..

<b>System Description</b>	<input type="text" value="System Description"/>
<b>System Contact</b>	<input type="text" value="System Contact"/>
<b>System Name</b>	<input type="text" value="ADSL Modem/Router"/>
<b>System Location</b>	<input type="text" value="System Location"/>
<b>System Object ID</b>	<input type="text" value="1.3.6.1.4.1.16972"/>
<b>Trap IP Address</b>	<input type="text" value="192.168.1.254"/>
<b>Community name (read-only)</b>	<input type="text" value="public"/>
<b>Community name (write-only)</b>	<input type="text" value="public"/>

### Fields in this page:

Field	Description
System Description	System description of the DSL device.
System Contact	Contact person and/or contact information for the DSL device.
System Name	An administratively assigned name for the DSL device.
System Location	The physical location of the DSL device.
System Object ID	Vendor object identifier. The vendor's authoritative identification of the network management subsystem contained in the entity.
Trap IP Address	Destination IP address of the SNMP trap.
Community name (read-only)	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
Community name (write-only)	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

### Function buttons in this page:

#### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### Undo

Discard your changes



### 4.7.5 Port Mapping

The DSL device provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the DSL device can isolate traffic from group to group for some application. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.

#### Port Mapping Configuration

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

**Note that the selected interfaces will be removed from their existing groups and added to the new group.**

Disabled    Enabled

**Grouped Interfaces**

->

<-

**Available Interfaces**

LAN1  
 LAN2  
 LAN3  
 LAN4  
 LAN5  
 wlan0  
 ppp0  
 ppp1

Select	Interfaces
<input checked="" type="radio"/>	Default LAN1,LAN2,LAN3,LAN4,LAN5,wlan0,ppp0,ppp1,ppp2,ppp3,ppp4,ppp5,ppp6,ppp7
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

#### Fields in this page:

Field	Description
Enabled/Disabled	Radio buttons to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
"Interface groups"	<p>To manipulate a mapping group:</p> <p>Select a group from the table.</p> <p>Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.</p> <p>Click "Apply Changes" button to save the changes.</p>

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.7.6 IP QoS**

The DSL device provides a control mechanism that can provide different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: **Traffic Classification** and **Action**. The **Traffic Classification** enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The **Action** enables you to assign the strictly priority level for and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all field as needed in these two QoS blocks for a QoS rule.

## IP QoS

Entries in this table are used to assign the precedence for each incoming packet based on physical LAN port, TCP/UDP port number, and source/destination IP address/subnet masks.

---

**IP QoS:**  Disabled  Enabled     
 **Default QoS:** IP Pred     
 Apply Changes

**Specify Traffic Classification Rules**

**Source IP:**      
 **Netmask:**      
 **Port:**   
**Destination IP:**      
 **Netmask:**      
 **Port:**   
**Protocol:** ▼     
 **Physical Port:** ▼

**Assign Priority and/or IP Precedence and/or Type of Service**

**Outbound Priority:** p3(lowest) ▼     
 **802.1p:** ▼  
**Precedence:** ▼     
 **TOS:** ▼

Add

**IP QoS Rules:**

		Traffic Classification Rules						Mark			
Select	Status	Src IP	Src Port	Dst IP	Dst Port	Protocol	Lan Port	Priority	IP Preced	IP ToS	Wan 802.1p
<input type="checkbox"/>	Enable					TCP	LAN1	p3			

Delete Selected     
 Delete All



Fields on the first setting block of this page:

Field	Description
IP QoS	Enable/disable the IP QoS function.
Default QoS	The default QoS standard to be applied.
Source IP	The IP address of the traffic source.
Source Netmask	The source IP netmask. This field is required if the source IP has been entered.
Source Port	The source port of the selected protocol. You cannot configure this field without entering the protocol first.
Destination IP	The IP address of the traffic destination.
Destination Netmask	The destination IP netmask. This field is required if the destination IP has been entered.
Destination Port	The destination port of the selected protocol. You cannot configure this field without entering the protocol first.
Protocol	The selections are TCP, UDP, ICMP and the blank for none. This field is required if the source port or destination port has been entered.
Physical Port	The incoming ports. The selections include LAN ports, wireless port, and the blank for not applicable.

Function buttons for first setting block:

### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

Fields on the second setting block of this page:

Field	Description
Outbound Priority	The priority level for the traffic that matches this classification rule. The possible selections are (in the descending priority): p0, p1, p2, p3.
802.1p	Select this field to mark the 3-bit user-priority field in the 802.1p header of the packet that match this classification rule. Note that this 802.1p marking is workable on a given PVC channel only if the VLAN tag is enabled in this PVC channel.
Precedence	Select this field to mark the IP precedence bits in the packet that match this classification rule.
TOS	Select this field to mark the IP Type Of Service bits in the packet that match this classification rule.

Function buttons for second setting block:

**Delete Selected**

Delete a selected IP QoS Rule entry. The IP QoS Rule entry can be selected on the **Select** column of the **IP QoS Rules Table**.

**Delete All**

Click to delete all entries

**4.7.7 DNS Server**

This page is used to select the way to obtain the IP addresses of the DNS servers.

Fields in this page:

Field	Description
Attain DNS Automatically	Select this item if you want to use the DNS servers obtained by the WAN interface via the auto-configuration mechanism.
Set DNS Manually	Select this item to configure up to three DNS IP addresses.
DNS1,2,3	Type the IP of the DNS servers

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Reset Selected**

Discard your changes.

**4.7.8 Dynamic DNS**

Each time your device connects to the Internet, your ISP assigns a different IP address to your device. In order for you or other users to access your device from the WAN-side, you



need to manually track the IP that is currently used. The Dynamic DNS feature allow you to register your device with a DNS server and access your device each time using the same host name. The **Dynamic DNS** page allows you to enable/disable the Dynamic DNS feature.

## Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org or TZO. Here you can Add/Remove to configure Dynamic DNS.

### Dynamic DDNS Table:

Select	State	Hostname	Username	Service
--------	-------	----------	----------	---------

Enable:

DDNS provider:

Hostname:

### DynDns Settings:

Username:

Password:

### TZO Settings:

Email:

Key:

On the **Dynamic DNS** page, configure the following fields:

Field	Description
Enable	Check this item to enable this registration account for the DNS server.
DDNS provider	There are two DDNS providers to be selected in order to register your device with: DynDNS and TZO. A charge may occurs depends on the service you select.
Hostname	Domain name to be registered with the DDNS server.
Username	User-name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.

Function buttons in this page:

**Add**

Click Add to add this registration into the configuration.

**Modify**

Select an existing DDNS registration by clicking the radio button at the **Select** column of the **Dynamic DNS Table**. Click **Modify** button to modify the selected registration with the new configuration.

**Remove**

Select an existing DDNS registration by clicking the radio button at the **Select** column of the **Dynamic DNS Table**. Click **Remove** button to remove the selected registration from the configuration.

#### 4.7.9 ACL

The Access Control List (ACL) is a list of permissions attached to the DSL device. The list specifies who is allowed to access this device. If ACL is enabled, all hosts cannot access this device except for the hosts with IP address in the ACL table. It has two directions; LAN and WAN

4.7.9.1 ACL LAN

## ACL Configuration

You can specify what services are accessible form LAN or WAN parts.  
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.  
Using of such access control can be helpful in securing or restricting the Gateway management.

---

Direction Select:  LAN  WAN

---

LAN ACL Switch:  Enable  Disable

---

IP Address:

Services Allowed:

- Any
- web
- telnet
- ftp
- tftp
- snmp
- ping

Fields in this page:

Field	Description
LAN ACL Switch	Select to Enable or Disable the LAN ACL Switch then Press Apply
IP address	Select the LAN IP address that you want to control his access
Services Allowed	Select the type of Service the LAN user can access the device through

Function buttons in this page:

**Apply**

Save configuration to system.

**Add**

Click Add to add this registration into the **Current ACL Table**.

**Reset**

Click to discard your changes





4.7.9.2 ACL WAN

### ACL Configuration

You can specify what services are accessible from LAN or WAN parts.  
 Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.  
 Using of such access control can be helpful in securing or restricting the Gateway management.

---

Direction Select:    LAN    WAN

---

WAN Setting:                     

WAN Interface:                  

Services Allowed:

web

telnet

ftp

tftp

snmp

ping

Fields in this page:

Field	Description
WAN Settings	Select Between filtering by Interface or IP address
WAN Interface	Select your Interface, If the services is filtered by Interface
WAN IP Address	Type your IP, If the services is filtered by IP
Services Allowed	Select the type of Service the LAN user can access the device through

Function buttons in this page:

**Add**

Click Add to add this registration into the **Current ACL Table**.

**Reset**

Click to discard your changes

Current ACL Table shows the summary of the ACL for both LAN and WAN users.



**Current ACL Table:**

Select	Direction	IP Address/Interface	Service	Port	Action
--------	-----------	----------------------	---------	------	--------

#### 4.7.10 Other

### Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to Continuous.

---

Half Bridge:     Disable     Enable

Interface:       ▼

Fields in this page:

Field	Description
Half bridge	To enable or disable Half Bridge mode.
Interface	The WAN interface available to be selected.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Undo**

Discard your changes

## 4.8 Admin

### 4.8.1 Save & Reboot

#### Commit/Reboot

This page is used to commit changes to system No-volatile Memory and reboot your system with different configurations.

Save Current Configuration

- Save Current Configuration >> **Apply** ... apply the current configuration
- Factory Default Configuration >> **Apply** ...apply the factory default configuration
- **Reset** >> discard your changes
- **Reboot** >> restart the modem

### 4.8.2 Backup/Restore

This page allows you to backup and restore your configuration into and from file in your host.

#### Backup/Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current configuration to factory default.

Save Settings to File:

Load Settings from File:

- Save Settings to File >> **Save**...select where in PC to save the file
- Load Settings from File >> **Browse**...select where in PC to take the file >> **Upload**...to apply the setting in the file

### 4.8.3 System Log

This page shows the system log.

**System Log**

System Log       Disable     Enable     

Save Log to File:   

Clear Log:           

```
<46> Jan 1 08:00:15 1970 syslogd started
<8> Jan 1 08:00:24 1970 boa[192]: Boa/0.93.15 started
<14> Jan 1 08:00:37 1970 udhcpd: sending OFFER of 192.168.1.100
<14> Jan 1 08:00:37 1970 udhcpd: sending ACK to 192.168.1.100
<80> Jan 1 08:31:32 1970 boa[192]: Authentication successful for admin from
192.168.1.100
```

- System Log ...select to enable or disable >>**Apply Changes...**to apply your selection
- Save Log to File >> **Save...**select where in PC to save the file
- Clear Log >> **Reset** ...click to clear the log
- **Refresh** >> click to update the log with latest information

#### 4.8.4 Password

The first time you log into the system, you use the default password. There are two-level logins: **admin** and **user**. The **admin** and **user** password configuration allows you to change the password for administrator and user.

## Password Setup

This page is used to set the account to access the web server of ADSL Router. Empty user name and password will disable the protection.

<b>User Name:</b>	<input type="text" value="admin"/>
<b>Old Password:</b>	<input type="text"/>
<b>New Password:</b>	<input type="text"/>
<b>Confirmed Password:</b>	<input type="text"/>

### Fields in this page:

Field	Description
User Name	Selection of user levels are: admin and user.
Old Password	Enter the old password for this selected login.
New Password	Enter the new password here.
Confirmed Password	Enter the new password here again to confirm.

### Function buttons in this page:

#### **Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### **Reset**

Discard your changes

### 4.8.5 Upgrade Firmware

## Upgrade Firmware

This page allows you upgrade the ADSL Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

---

**Select File:**

To upgrade the firmware for the DSL device:

- Click the **Browse** button to select the firmware file.
- Confirm your selection.
- Click the **Upload** button to start upgrading.

**IMPORTANT!** Do not turn off your DSL device or press the Reset button while this procedure is in progress.

### 4.8.6 Time Zone

Simple Network Timing Protocol (SNTP) is a protocol used to synchronize the system time to the public SNTP servers. The DSL device supports SNTP client functionality in compliance with IETF RFC2030. SNTP client functioning in daemon mode which issues sending client requests to the configured SNTP server addresses periodically can configure the system clock in the DSL device

## System Time Configuration

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time:  year  month  day  hour  min  sec

Apply Changes

Reset

### NTP Configuration:

State:  Disable  Enable

NTP Server1:

NTP Server2:

Interval: Every  hours

Time Zone:

GMT time: Thu Jan 1 11:46:43 1970

Apply Changes

Reset

NTP Start:

Get GMT Time

### Fields in first section in this page:

Field	Description
System Time	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP.

### Function buttons for first section:

#### Apply Changes

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

#### Reset

Discard your changes

### Fields in second section in this page:

Field	Description
State	Enable or Disable mode
NTP Server	Network Time Protocol servers available as preset.
Interval	Grasp period for next synchronize of time with NTP server.
Time Zone	User local time zone.
GMT time	Greenwich Mean Time

Function buttons for second section:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**Reset**

Discard your changes

**Get GMT Time**

Greenwich Mean Time

**4.8.7 Green AP**

**GREEN AP**

This page is used to configure the Green ap time.e.g. (From 09:21 to 18:30,action txPower 25%)

Green AP rule list:

Duration	Action
:00 :00 -- :00 :00	Disable <input type="button" value="v"/>
:00 :00 -- :00 :00	Disable <input type="button" value="v"/>
:00 :00 -- :00 :00	Disable <input type="button" value="v"/>
:00 :00 -- :00 :00	Disable <input type="button" value="v"/>

Function buttons for second section:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section “Admin” for save details.

**4.8.8 TR-069 Config (Optional)**

TR-069 is a protocol for communication between a CPE and Auto-Configuration Server (ACS). The CPE TR-069 configuration should be well defined to be able to communicate with





the remote ACS.

## TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

### ACS:

URL:

User Name:

Password:

Periodic Inform Enable:  Disabled  Enabled

Periodic Inform Interval:

### Connection Request:

User Name:

Password:

Path:

Port:

### Debug:

ACS Certificates CPE:  No  Yes

Show Message:  Disabled  Enabled

CPE Sends GetRPC:  Disabled  Enabled

Skip MReboot:  Disabled  Enabled

Delay:  Disabled  Enabled

Auto-Execution:  Disabled  Enabled

CT Inform Extension:  Disabled  Enabled

Apply Changes

Undo

Fields in this page:

ACS Field	Description
URL	ACS URL. For example, <a href="http://10.0.0.1:80">http://10.0.0.1:80</a> <a href="https://10.0.0.1:443">https://10.0.0.1:443</a>
User Name	The username the DSL device should use when connecting to the ACS.
Password	The password the DSL device should use when connecting to the

	ACS.
Periodic Inform Enable	When this field is enabled, the DSL device will send an Inform RPC to the ACS server at the system startup, and will continue to send it periodically at an interval defined in <b>Periodic Inform Interval</b> field; When this field is disabled, the DSL device will only send Inform RPC to the ACS server once at the system startup.
Periodic Inform Interval	Time interval in second to send Inform RPC.
Connection Request Field	Description
User Name	The username the remote ACS should use when connecting to this device.
Password	The password the remote ACS should use when connecting to this device.
Path	The path of the device Connection Request URL. The device Connection Request URL should be configured based on the Device_IP, Path and Port as follows: http://Device_IP:Port/Path
Port	The port of the device Connection Request URL.
ACS Certificate CPE	Specify whether to check the ACS certification of the router.
Show Message	Select Enable to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select Enable, the CPE contact the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto Execution	Specify whether to automatically start the TR-069 after the router is powered on.
CT Inform Extension	Specify whether to support China Telecom extension inform type.

Function buttons in this page:

**Apply Changes**

Set new configuration. New parameters will take effect after save into flash memory and reboot the system. See section "Admin" for save details.

**Undo**

Discard your changes

## 5 Troubleshooting Guide

### Q1 Why all LED indicators are off?

- A1
- Check the connection between the power adaptor and the power socket.
  - Check the power switch is on or not.

### Q2 Why LAN LED is not lighting?

- A2
- Check the connection between the ADSL modem and your computer, hub, or switch.
  - Check the running status of your PC, hub, or switch, and ensure that they are working normally.

### Q3 Why ADSL LED is not lighting?

- A3 Check the connection between the ADSL “DSL” port and the wall jack.

### Q4 Why cannot visit Internet with ADSL LED is on?

- A4 Ensure that the following information is correctly entered.
- VPI/VCI
  - Username/password.

### Q5 Why cannot open the Modem Web configuration page?

- A5 Follow below steps to check the communication between the computer and modem.
- Choose **Start ► Run** from the desktop, and ping 192.168.1.1 (the IP address of the modem).
  - If the modem cannot be reached, please check following configuration:
    - Type of the network cable
    - Connection between the modem and computer
    - TCP/IP configuration of you computer

**Q6 How to load the default setting after incorrect configuration?**

- A6
- To restore the factory default, keep the device powered on and push a needle into the hole.  
Press down the button about one second and then release.
  - The default IP address and subnet mask of the modem are 192.168.1.1 and 255.255.255.0 respectively.
  - User/password of super user: admin/admin
  - User/password of common user: user/user

## 6 Appendix

### PRODUCT SUPPORT AND CONTACT INFORMATION

At LogN, we are committed to provide you with the best quality of products as well as the best technical support. While if your computer is infected by virus, we may suggest you to find a solution in order to remove the virus, because we are unable to assist you until the virus is eradicated.

#### Technical Support

Hotline Inside Egypt: 19906

Outside Egypt: +202 275 49607

E-mail: [support@logn.com.eg](mailto:support@logn.com.eg)

[www.logn.com.eg](http://www.logn.com.eg)