

# Robustel GoFixed W800

3G ADSL Wireless VoIP Gateway

for WCDMA/HSUPA Networks

## User Guide

Document Name:	<b>User Guide</b>
Version:	<b>02.00</b>
Date:	<b>2011-11-04</b>
Status:	<b>Confidential</b>
DocID:	<b>RT_W800_v02.00</b>



***Robustel***

[www.robustel.com](http://www.robustel.com)

## About This Document

This document describes the hardware and software of the *Robustel W800 3G ADSL Wireless VoIP Gateway*.

**Copyright© Guangzhou Robustel Technologies Co., Limited  
All Rights Reserved.**

## Trademarks and Permissions

Robustel are trademark of Guangzhou Robustel Technologies Co. Limited.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

## Technical Support Contact Information

Tel: +86-2023354618

Fax: +86-2032016426

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

Web: [www.robustel.com](http://www.robustel.com)

## Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the gateway are used in a normal manner with a well-constructed network, the gateway should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the gateway, or for failure of the gateway to transmit or receive such data.

## Safety Precautions

### General

- The gateway generates radio frequency (RF) power. When using the gateway care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your gateway in aircraft, hospitals, petrol stations or in places where using GSM products are prohibited.
- Be sure that the gateway will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the gateway should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the gateway for proper operation. Only using approved antenna with the gateway. Please contact authorized distributor to find an approved antenna.
- Always keep the antenna with minimum safety distance of 26.6 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.

**Note:** *Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Gateway may be used at this time.*

### Using the gateway in vehicle

- Check for any regulation or law authorizing the use of GSM in vehicle in your country before installing the gateway.
- The driver or operator of any vehicle should not operate the gateway while is in control of a vehicle.
- Install the gateway by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the gateway.
- The gateway should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the gateway is powered by the vehicle's main battery. The battery may be drained after extended period.

### Protecting your gateway

- To ensure error-free usage, please install and operate your gateway with care. Do remember the follow:
- Do not expose the gateway to extreme conditions such as high humidity / rain, high temperatures, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the gateway. There is no user serviceable part inside and the warranty would be void.

- Do not drop, hit or shake the gateway. Do not use the gateway under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the gateway only according to the instruction manual. Fail to do it will void the warranty.
- In case of problems, please contact authorized distributor.

## Regulatory and Type Approval Information

**Table 1:** Directives

2002/95/EC	Directive of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)	
2002/96/EC	Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)	
2003/108/EC	Directive of the European Parliament and of the Council of 8 December 2003 amending directive 2002/96/ec on waste electrical and electronic equipment (WEEE)	

**Table 2:** Standards of the Ministry of Information Industry of the People’s Republic of China

SJ/T 11363-2006	“Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products” (2006-06).	
SJ/T 11364-2006	<p>“Marking for Control of Pollution Caused by Electronic Information Products” (2006-06).</p> <p>According to the “Chinese Administration on the Control of Pollution caused by Electronic Information Products” (AGATEWAYIP) the EPUP, i.e., Environmental Protection Use Period, of this product is 20 years as per the symbol shown here, unless otherwise marked. The EPUP is valid only as long as the product is operated within the operating limits described in the Hardware Interface Description.</p> <p>Please see <a href="#">Table 3</a> for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.</p>	

**Table 3:** Toxic or hazardous substances or elements with defined concentration limits

Name of the part	Hazardous substances					
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)
Metal Parts	o	o	o	o	o	o
Circuit Modules	x	o	o	o	o	o
Cables and Cable Assemblies	o	o	o	o	o	o
Plastic and Polymeric parts	o	o	o	o	o	o

**O:**  
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

**X:**  
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.

### Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	Firmware Version	Details
2011-05-09	01.00	First Release
2011-11-04	02.00	Add WCDMA voice

## Contents

Chapter 1.	Product Concept.....	8
1.1	Overview .....	8
1.2	Packing List.....	8
1.3	Specifications .....	9
1.4	Application Cases .....	12
Chapter 2.	Installation.....	13
2.1	Interface .....	13
2.2	LED Indicators.....	13
2.3	Install the Bracket.....	14
2.4	Installation the SIM Card.....	15
2.5	Hardware Connection .....	15
Chapter 3.	Operate the Gateway .....	17
3.1	Default Configuration.....	17
3.2	Configuration .....	17
3.3	Log In the Gateway .....	17
3.4	Status .....	18
3.5	Quick Setup.....	19
3.6	Network .....	25
3.6.1	3G Configuration (WAN Device/WAN Service).....	25
3.6.2	ADSL Configuration (WAN Service) .....	27
3.6.3	SIM PIN (3G Settings) .....	28
3.6.4	Advanced ADSL Settings.....	29
3.6.5	DMZ Host.....	30
3.6.6	Port Forwarding (Virtual Servers) .....	31
3.6.7	Advanced IP Routing (Static Route).....	32
3.6.8	QoS Configuration .....	33
3.7	Application .....	34
3.7.1	UPnP Settings .....	34
3.7.2	Dynamic DNS.....	34
3.7.3	VPN (IPSec VPN) .....	35
3.7.4	VPN (PPTP Config) .....	36
3.8	Wireless Configuration (WLAN) .....	38
3.8.1	WLAN Basic .....	38
3.8.2	WLAN Security .....	38
3.8.3	Advanced Settings .....	39
3.8.4	WLAN MAC Filters.....	39
3.8.5	WLAN Bridge .....	40
3.9	LAN Configuration (DHCP) .....	41
3.10	Firewall.....	42
3.10.1	Firewall Settings .....	42
3.10.2	IP Filters.....	42
3.10.3	Domain Filters .....	44

- 3.10.4 MAC Filters ..... 45
- 3.10.5 Access Control (Remote Access)..... 45
- 3.11 Voice..... 46
  - 3.11.1 Voice Configuration ..... 46
  - 3.11.2 Basic Settings..... 46
  - 3.11.3 Advanced Settings ..... 48
- 3.12 Tools ..... 51
  - 3.12.1 Account Settings (Users) ..... 51
  - 3.12.2 Time Settings..... 51
  - 3.12.3 Backup Settings ..... 52
  - 3.12.4 Update (Restore) Settings ..... 52
  - 3.12.5 Update Software ..... 53
  - 3.12.6 Factory Settings..... 53
  - 3.12.7 Reboot Router ..... 54
  - 3.12.8 TR-069 Client ..... 54
  - 3.12.9 Ping Reboot ..... 54
  - 3.12.10 3G Link Notice ..... 55
- Chapter 4. Troubleshooting ..... 56
  - 4.1 Factory Settings..... 56
  - 4.2 Troubleshooting ..... 56
    - 4.2.1 Unable to Access Internet..... 56
  - 4.3 Terms and Abbreviations ..... 58

# Chapter 1. Product Concept

## 1.1 Overview

- Robustel GoFixed W800 3G ADSL Wireless VoIP Gateway is a Dual-WAN 3G / ADSL2+ (VPN) firewall router integrated 3G HSUPA, ADSL / ADSL2+, 802.11b/g/n ,**WCDMA/GSM voice** and SIP VoIP/FoIP.
- 3G HSUPA works as a backup WAN, functioning as an automatic fail-over when an ADSL2+ connection breaks down.
- With one RJ-11 FXS interface, users could enjoy excellent VoIP and T.38 FoIP service over ADSL or 3G. Also supports WCDMA/GSM voice over this RJ-11 interface based on circuit switch.
- 3G ADSL Wireless Gateway also provides IPsec VPN and PPTP VPN, users can access corporate intranet and transmit sensitive data between branch offices and remote sites anytime and anyplace.

## 1.2 Packing List

Check your package to make certain it contains the following items:

- Robustel GoFixed W800 gateway x1



- AC/DC Power Supply Adapter (12VDC, 1A) x1



- Desktop bracket x1



- ADSL splitter x1



- Ethernet cable RJ45 x1



- Phone cable RJ11 x2



- CD with user guide and configuration utility x1

**Note:** Please notify your sales representative if any of the above items are missing or damaged.

### 1.3 Specifications

<b>3G</b>	HSUPA	WCDMA / HSUPA Quad Band 850 / 900 / 1900 / 2100 MHz HSUPA DL / UL 7.2 / 5.76 Mbps HSDPA DL 7.2 Mbps, UL 384 Kbps UMTS DL / UL 384 / 384 Kbps GSM / GPRS / EDGE Quad Band 850 / 900 / 1800 / 1900 MHz GPRS, multi-slot class 10 (4+1, 3+2) up to 86.2 kbps (downlink) EDGE, multi-slot class 10 (4+1, 3+2) up to 237 kbps (downlink)
	Authentication	PAP/CHAP/MS-CHAP
	Always Online	PPP LCP Echo/Reply and ICMP keep alive for link inspection
	Dial On Demand	Always online or triggered by local data flow and auto disconnect
	Number of SIMs	1
	SIM Control	3V, standard SIM or USIM

<b>DSL</b>	Interface	One RJ-11
	ADSL Standard	Full-rate ANSI T1.413 Issue 2 G.dmt (ITU G.992.1) G.lite (ITU G.992.2)
	ADSL2 Standard	G.dmt.bis (ITU G.992.3) ADSL2 Annex L (ITU G.992.3 Annex L)
	ADSL2+ Standard	G.dmt.bis plus (ITU-T G.992.5) ADSL2+ Annex M (ITU G.992.5 Annex M)
<b>ATM and PPP Protocols</b>	AAL5	ATM Adaptation Layer Type 5 (AAL5)
	Multiple Protocol over AAL5	Multiple Protocol over AAL5 (RFC 2684, formerly RFC 1483)
	Encapsulation	Bridged or routed Ethernet encapsulation
	Multiplexing	VC and LLC based multiplexing
	PPPoE	PPP over Ethernet (PPPoE, RFC 2516)
	PPPoA	PPP over ATM (PPPoA, RFC 2364)
	IP over ATM	Classical IP over ATM (RFC 1577)
	Mac Encapsulated Routing	MAC Encapsulated Routing (RFC 1483 MER)
<b>Wireless LAN</b>	OAM F4 / F5	OAM F4 / F5
	Standards	Compliant with IEEE 802.11b/g/n
	Data Rates	Up to 300 Mbps wireless data transfer rates
	Mode	Access Point (AP) or AP Bridge (WDS)
	WPS	Wi-Fi Protected Setup (WPS) for easy setup
	Encryption	WEP 64/128 bits
	Security	WPA, WPA-PSK, WPA2, WPA2-PSK
	Mac Filter	Black list and white list filter
	QoS	WMM
	ACS	Automatic channel selection
	Antenna	2T2R MIMO mode (2 transmitter, 2 receiver) One external antenna with 2dBi gain; one internal antenna with 4dBi gain
	Transmission Power	802.11b: 16+/-1.5dBm 802.11g: 14+/-1.5dBm 802.11n: HT20 16+/-1.5dBm; HT40 14+/-1.5dBm
	Reception Sensibility	802.11b: -82dBm, ±2dB 802.11g: -68dBm, ±2dB 802.11n: HT20 -64dBm, ±2dB; HT40 -60dBm, ±2dB
RF Selection	On/Off	
<b>Ethernet Interface</b>	Interface	8-pin RJ-45, auto MDI-X
	Number of Ports	4-port fast Ethernet switch
	Speed	10/100 Mbps
<b>VoIP</b>	Interface	RJ-11
	Number of Ports	One FXS port for connecting to analog telephone
	Protocol	Compliant with SIP standard (RFC3261)
	Audio Codec	G.711 A/μ law, G.729a, G.723.1, G.726_24, G.726_32, GSM_ARM_12k / 10

		/ 795 / 740 / 670 / 590 / 515 / 475
	Telephone Features	Call waiting, Call forwarding, Call barring, Call blocking, Silence suppression, Voice activity detection (VAD), Comfort noise generation (CNG), G.168 line echo cancellation, Caller ID
	Fax	T.38
	DTMP	Supports DTMF tone detection and generation
	Dial Plan	Flexible dial plan customization
<b>WCDMA/GSM Voice</b>	Interface	RJ - 11(the same as VoIP RJ - 11)
<b>Protocols and Firewall</b>	Network Protocols	NAT, NATP, DMZ, DHCP, SNTP, DNS Relay, IGMP Proxy / Snooping, Static Routing, ALG, UPnP
	Firewall	SPI (Stateful Packet Inspection), IP / Domain / MAC filters
<b>QoS</b>	IP QoS	Base on source IP address, source and destination port, protocol and DSCP
	ATM QoS	Support CBR, UBR, nrt-VBR, rt-VBR
	Features	Support for extended Impulse Noise Protection (INP) for better IPTV quality
<b>Operation and Management</b>	Configuration	Web, Telnet, SSH
	Firmware Upgrade	HTTP / TFTP / FTP
	Management	TR069
<b>VPN</b>	PPTP	Client, maximum 6 tunnels Encryption: MPPE
	IPSec	Client, maximum 5 tunnels IKE key management Encryption: DES, 3DES, AES-128 / 192 / 256 Integrity: MD5 and SHA-1 Authentication: pre-shared key
	VPN Passthrough	PPTP / L2TP / IPsec Passthrough
<b>Others</b>	LED Indicators	Power, LAN1, LAN2, LAN3, LAN4, Internet, DSL, WiFi, WPS, 3G
	Buttons	Power On/Off, 3G, WPS, Reset
<b>Physical Characteristics</b>	Color	White
	Housing	Plastic
	Weight	1500g
	Dimensions	Gateway without bracket (L x W x H): 170 x 140 x 35 mm Gateway with bracket (L x W x H): 160 x 75 x 20 mm Giftbox including gateway and accessories (L x W x H): 265 x 210 x 75 mm
	Installation Method	Desktop with bracket
<b>Environmental Limits</b>	Operating Temperature	0°C to 50°C
	Storage Temperature	-20°C to 70°C
	Operating Humidity	20 to 95% non-condensing
<b>Power Supply</b>	Power Supply Adapter	Input AC 100-240 V, 50 / 60 Hz, 0.5 A Output DC 12 V, 1.5 A
<b>Regulatory and Type Approvals</b>	Directives	RoHS and WEEE compliant
	CE and R&TTE Approval	To be determined
	FCC Approval	To be determined

---

	PTCRB Approval	To be determined
<b>Warranty</b>	Warranty Period	1 year

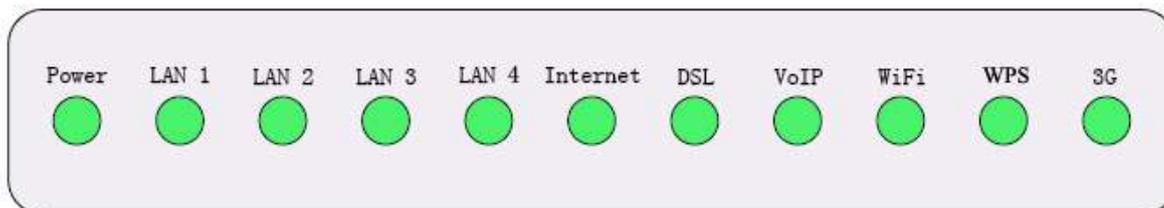
## 1.4 Application Cases

- **Office in a Box:** provides an office solution to sectors such as mining, construction and emergency services where fixed infrastructure is costly and time prohibitive
- **Data backup and redundancy:** ensure business continuity to retail, banking and emergency services by providing a wireless voice and data redundancy path to guard against fixed line outages
- **Fixed line alternative:** a cost and time efficient solution for broadband and fixed phone services where POTS infrastructure is unavailable
- **Mobile workforce:** event management, consulting and auditing sectors can bring their own wireless branch office (VPN) to a temporary work location

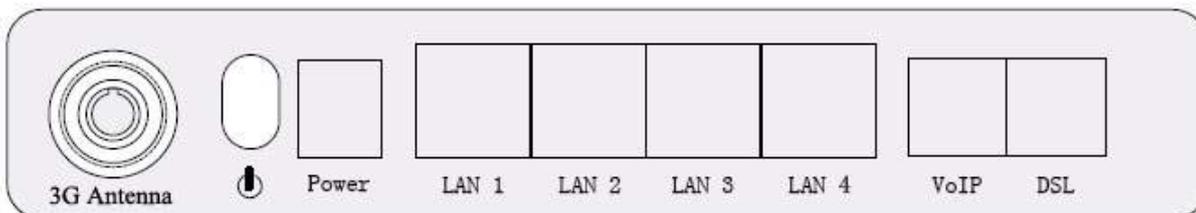
## Chapter 2. Installation

### 2.1 Interface

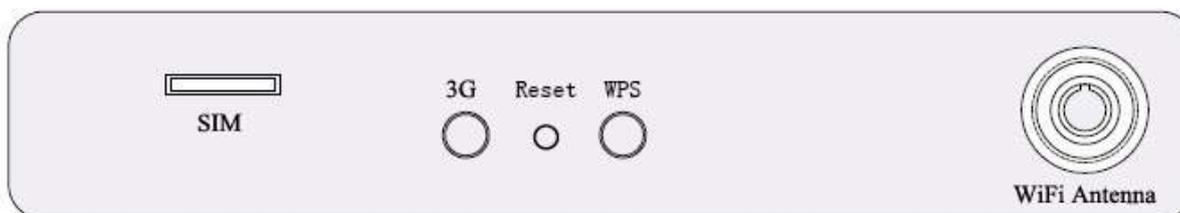
Front Panel Indicators:



Right Side Interfaces:



Left Side Interfaces:



### 2.2 LED Indicators

Item	Name	Function
Indicators	Power	On: Modem power up
		Off: Modem power off
	LAN 1-4	On: Ethernet is connected
		Blinking green: Ethernet traffics flow
	Off: Ethernet is disconnected	
	Internet	Blinking green: PPP/DHCP

		negotiation
		Solid green: PPP/DHCP up
		Quick blinking green: Tx/Rx traffic on line
	DSL	On: Modem synchronized to the DSLAM
		Quick blinking green: Modem training, but not synchronized
		Slow blinking green: Modem Idle
	VoIP	On: The analog phone connected to VoIP off-hook
		Off: The analog phone connected to VoIP on-hook
	WiFi	On: Wi-Fi connection is available
		Blinking green: Negotiation or traffic on line
		Off: Wi-Fi connection is not available
	WPS	Indicate the status of WPS authenticator
	3G	Blinking green: Negotiation or traffic on line
		Solid green: Up
		Quick blinking green: Tx/Rx traffic on line
Solid red: Authentication failed		
Off: Traffic through DSL interface		
Interface 1		Power switch
	Power	For 12V DC power adapter
	LAN 1-4	LAN interface for connecting to computers
	VoIP	Connecting to analog telephones
	DSL	Connecting to ADSL enabled telephone line
Interface 2	SIM	SIM Card slot
	3G	3G Switch
	Reset	Restore to factory default settings
	WPS	WPS Switch

## 2.3 Install the Bracket

Mount the bracket on the bottom of the gateway.

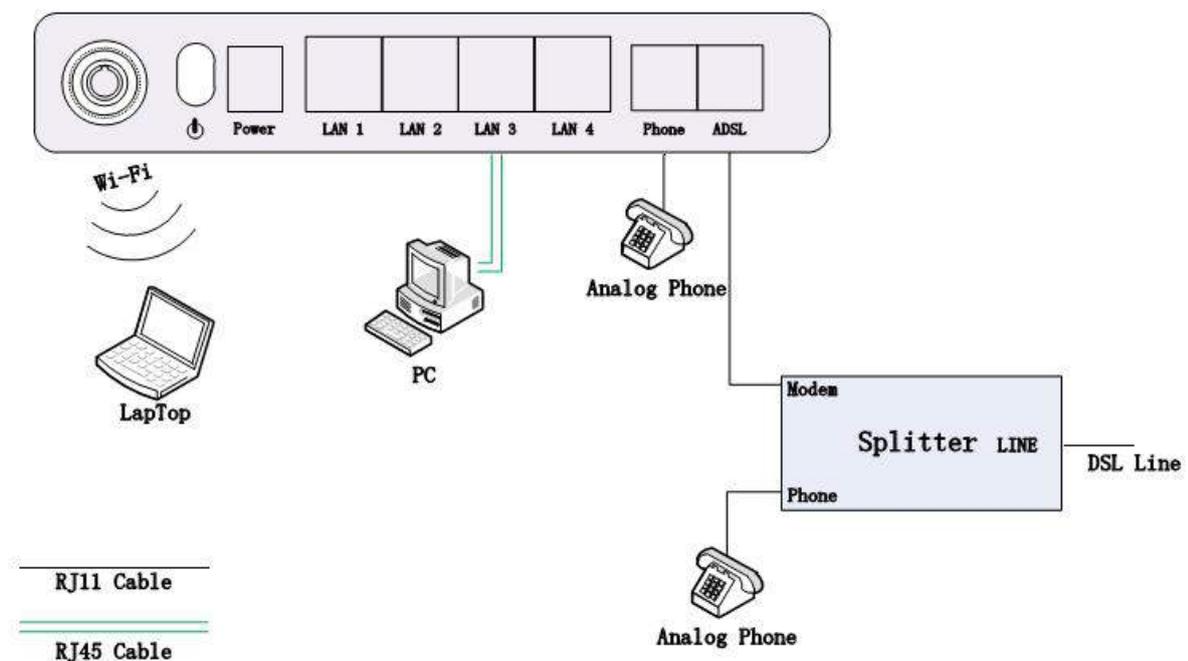


## 2.4 Installation the SIM Card

Be sure to insert a SIM card before you use the gateway.

**Note:** Make sure to disconnect the charger and switch off your gateway before inserting or removing your SIM/USIM card.

## 2.5 Hardware Connection



1. Use a telephone cord to connect the LINE port of the splitter with the phone socket on the wall (only if using ADSL).
2. Use another telephone cord to connect the MODEM port of the splitter with the ADSL port of the GATEWAY (only if using ADSL).
3. Connect Ethernet port of the GATEWAY with 10/100BASE-T port of the computer by using the network cable that comes with the unit.
4. Plug in the power cord, and turn on the power.

## Chapter 3. Operate the Gateway

### 3.1 Default Configuration

The Gateway has pre-configured with the VCI/VPI which is in common use. The default dial-up mode is bridge encapsulation. For bridge mode, no need to configure any more parameter. However, the third party dial-up software is needed for connection with the Internet.

### 3.2 Configuration

The default IP address for Gateway is: **192.168.1.1**; the Subnet Mask is: **255.255.255.0**.

Users can configure the Gateway through an Internet browser. The Gateway can be used as gateway and DNS server; users need to set the PC's TCP/IP protocol as follow:

1. Set the PC IP address at same segment of the Gateway such as set the IP address of the network card to one of the "192.168.1.2" to "192.168.1.254" excluding "192.168.1.1".
2. Set the PC's gateway the same IP address as the Gateway's.
3. Set PC's DNS server the same as Gateway's IP address or that of an effective DNS server.

### 3.3 Log In the Gateway

Power on to start the Gateway, making sure your PC can PING via LAN port of Gateway (the factory default IP is **192.168.1.1**), then run IE. Inputting **http://192.168.1.1** in the address column, press ENTER, and authentication interface will pop up as below:



Default User Name: **admin**

Default Password: **admin**

Press ENTER or click on 'OK' to enter into Gateway main page to perform configuration after entering the accurate user name and password in the dialog box.

If log on successfully, the main page will be displayed as follows:



### 3.4 Status

Click on the **Status** menu in the web interface

The following status information is available by clicking the links on the left of the webpage:

### Basic Info

Include hardware and software versions, system time info and basic IP information.

### Network Status

Include basic 3G status (SIM card details, network and signal strength) and basic ADSL status.

### WAN Info

Lists the configured WAN (3G and ADSL) interfaces and shows type, connection status and basic IP information.

### WLAN Status

Include basic Wireless information and a list of clients connected wirelessly.

### Connected Devices

Show a full list of connected clients, both wired and wireless.

### Routing Table

Displays the current IP routing table

### Statistics

Displays a list of configured WAN (3G and ADSL) interfaces and shows the amount of traffic sent and received on each interface.

### VoIP Status

Show the current registration status of a configured VoIP provider.

## 3.5 Quick Setup

Click on the **Quick** menu in the web interface.

This will show a quick setup wizard that allows the user to configure the most commonly used options:

### Step 1: Access Account

Username:	<input type="text"/>
New Name:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

This sets the username and password to access the web interface.

The default username to access the GATEWAY is **admin**.

The default password is **admin**.

To change the password:

1. Select **admin** from the **Username** drop-down box
2. Enter the password **admin** in the **Old Password** box
3. Enter a new password in both the **New Password** and **Confirm Password** boxes
4. Click the **Next** button
5. Login with the new password
6. Click on the **Quick** menu to continue the wizard

To continue to the next step without changing the password and click the **Skip** button.

### Step 2: Time Settings

Current Time: Thu Jan 1 00:24:29 1970

Set Time Mode:  Time Server  Manual Setting

Time:  year  month  day  
 hour  minute

Time Zone Offset:

From this page the current time can be set manually or the GATEWAY can be set to obtain the correct time from an internet time server.

**Note:** it is recommended that an internet time server is used when available if the time is set manually it will be lost in the event of a power cut or if the unit is restarted.

To set the time manually:

1. Select **Manual Setting**
2. Enter the current time
3. Select the correct Time Zone
4. Click **Next**

To use an internet time server:

1. Select **Time Server**
2. Enter the time server domain name e.g **time.nist.gov** or **pool.ntp.org**
3. Select the correct Time Zone
4. Click **Next**

### Step 3: Wireless Settings

Enable WLAN  
 Disable SSID broadcast

SSID:

BSSID:

Country:

Max client number:

Channel:

Auto Channel Timer(min):

By default the Wireless (Wi-Fi) access point is enabled and the SSID (the name that is displayed when users search for Wi-Fi networks) is set to "gateway". To keep the default settings click **Next** to go to the next step.

To change the SSID:

1. Enter the new SSID in the **SSID** box
2. Select the correct Country
3. Click the **Next** button

#### Step 4: Local Area Network Setup

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server  
 Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static DNS Server:   
 Get DNS Server From WAN

Configure the second IP Address and Subnet Mask for LAN interface

By default the gateway has an IP Address of 192.168.1.1 and the DHCP server is enabled so that IP addresses will be

automatically assigned to clients connecting to either the wired Ethernet ports or via Wi-Fi. To keep the default settings click **Next** to go to the next step.

A new IP address can be assigned to the gateway and the DHCP options can be changed from this screen--- for more details on available options refer to section 10.

Enable Automatic 3G backup

Time out all dsl linkdown to run 3G(seconds)  seconds

WAN Device Select:

When both ADSL and 3G connections are available the GATEWAY can failover to the 3G connection when the ADSL connection is unavailable. To use the feature to check the **Enable Automatic 3G backup** box and enter the amount of time (in seconds) that the ADSL link must be unavailable before switching to 3G then click **Next**.

**Step 6: Configure 3G and ADSL connections**

*To setup the 3G connection:*

**3G Network (WAN) Service Setup**

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Connected		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

Click the **Edit** button for the 3G service

**3G network settings**

PPP Connect Mode

PPP author

PPP Username

PPP Password

APN

Dial Number

Auto reconnect interval time

Service Mode

Port Bind  LAN1  LAN2  LAN3  LAN4  SSID1

Enable LAN DHCP (?)

For most networks it is only required to set the correct **APN** value (this should be provided by your network operator) leave the other settings on default values.

If your network requires logging the valid **PPP Username** and **PPP Password**.

Fill in the required information and click the **Apply/Save** button.

**To setup the ADSL connection:**

**ADSL Network (WAN) Service Setup**

Interface	Vpi	Vci	Category	QoS	Description
atm0_1	0	35	UBR	Disabled	2_INTERNET_B_0_35
atm1_1	8	35	UBR	Disabled	3_INTERNET_B_8_35

Click the **Add** button to start the ADSL network wizard.

VPI: [0-255]

VCI: [32-65535]

Enter the values for VPI and VCI supplied by the ADSL Service Provider and click **Next**.

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Service Mode:

Port Bind (?):  LAN1  LAN2  LAN3  LAN4  SSID1

Enable LAN DHCP (?)

If EoA link type was selected, choose the WAN service type, normally PPP over Ethernet (PPPoE).

Click **Next**.

PPP Username:   
PPP Password:   
PPPoE Service Name:   
Authentication Method:

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

Enable IGMP Multicast Proxy

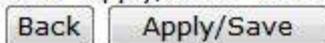
Enter the username and password provided by the ADSL service provider; select any other options required and click **Next**.

## WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

<b>PORT / VPI / VCI:</b>	0 / 0 / 35
<b>Connection Type:</b>	PPPoE
<b>Service Name:</b>	pppoe_0_0_35
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Automatically Assigned
<b>Service State:</b>	Enabled
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Enabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.



Check the Summary screen and then click **Apply/Save** to enable the connection.

The Quick Setup wizard is now complete. Refer to the following sections for a complete description of all of the available options.

## 3.6 Network

### 3.6.1 3G Configuration (WAN Device/WAN Service)

Please go to **Network** interface to select the **WAN Service**. Users can either edit a 3G network or an ADSL network.

**Note:** please power off the Gateway before inserting the SIM card.

Please go to path: Network -> WAN Device page. Check the **Enable Automatic 3G backup**, and configure the **time out all DSL link down to run 3G** – the value here is used to determine the time interval for using 3G after DSL link is down. Then click **Apply/Save**.

### WAN Device Settings

Please click Apply/Save to save you configure

Enable Automatic 3G backup

Time out all dsl linkdown to run 3G(seconds)  seconds

WAN Device Select:

Then go to path: **Network -> WAN Service** to check the status. Please refer to the following figure.

#### WAN Service

Choose Add, Edit or Remove to configure a WAN service over a selected interface.  
 If Ports Binding is enable,only the binding port can access to the internet.  
 If Ports Binding is disable,all of the ports can access to the internet.

Enable Ports Binding

#### 3G Network (WAN) Service Setup

Interface	Description	Connect Mode	binding ports	APN	Dial Number	Igmp	NAT	Firewall	Status	Edit	Action
ppptd3g0	ppptd3g	AlwaysOn	none	3gnet	(null)	Disabled	Enabled	Enabled	Connected		<input type="button" value="Connect"/> <input type="button" value="Disconnect"/>

Click the **Edit** button for the 3G service

#### 3G network settings

PPP Connect Mode   
 PPP author   
 PPP Username   
 PPP Password   
 APN   
 Dial Number   
 Auto reconnect interval time   
 Service Mode

Port Bind  LAN1  LAN2  LAN3  LAN4  
 SSID1  SSID2  SSID3  SSID4

Enable LAN DHCP (?)

Fill in the required information and click the Apply/Save button. For most networks it is only required to set the correct APN value. Leave the other settings on default values.

If your network requires logging the valid PPP Username and PPP Password.

## 3.6.2 ADSL Configuration (WAN Service)

Please go to path: Network -> WAN Service page. Then do the following to setup an ADSL connection.

1. Click **Add** button to configure an ATM PVC identifier;

### ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI).

**Notice: If the link type is EoA, it can use the PVC repeatedly though it is existent. But the PPPoA or IPoA can't.**

VPI: [0-255]

VCI: [32-65535]

2. Click **Next** to select a service category; (here please choose EoA for PPPoE connection);

### ATM PVC Configuration

Select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA  
 PPPoA  
 IPoA

Encapsulation Mode:

Service Category:

Enable VLAN

### Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service

3. Click **Next** to select WAN service type; (here please choose PPP over Ethernet);

### WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)  
 IP over Ethernet  
 Bridging

Enter Service Description:

Port Bind:  LAN1  LAN2  LAN3  LAN4  
 SSID1  SSID2  SSID3  SSID4

4. Click **Next** to input the username and password authorized by your ISP; (here please make Enable **Fullcone NAT** checked);

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

- Enable Fullcone NAT
- Enable Firewall
- Dial on demand (with idle timeout timer)
- Use Static IPv4 Address
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

**Multicast Proxy**

- Enable IGMP Multicast Proxy

5. Click Next to check the Summary of this connection;

**WAN Setup - Summary**

Make sure that the settings below match the settings provided by your ISP.

<b>PORT / VPI / VCI:</b>	0 / 0 / 35
<b>Connection Type:</b>	PPPoE
<b>Service Name:</b>	pppoe_0_0_35
<b>Service Category:</b>	UBR
<b>IP Address:</b>	Automatically Assigned
<b>Service State:</b>	Enabled
<b>NAT:</b>	Enabled
<b>Full Cone NAT:</b>	Enabled
<b>Firewall:</b>	Enabled
<b>IGMP Multicast:</b>	Disabled
<b>Quality Of Service:</b>	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

6. Click **Apply/Save** to enable the connection.

### 3.6.3 SIM PIN (3G Settings)

Go to path **Network -> 3G Settings**

### PIN Settings

#### PIN code operation

Disable--When PIN lock disabled, SIM card can be activated without PIN auth.

Enable--When PIN lock disabled, SIM card should be activated after PIN auth successfully.

Modify--Set PIN code as a new one.

PIN code: 4~8 decimal digits.

PUK code: 8 decimal digits. When SIM card is PIN locked, it should be unlocked with correct PUK code.

Residual allowed try time After these times, SIM card will be locked.

PIN State:	Disabled
PIN code operation:	Enable <input type="button" value="v"/>
PIN code:	<input type="text" value="••••"/>
Residual allowed try time:	3

This page allows the user to enable or disable the SIM PIN function. Select whether the SIM Pin should be enabled or disabled, enter the current SIM pin and click the Apply/Save button.

The "PIN State" shows whether the SIM PIN function is currently enable or disable.

The "Residual allowed try time" shows how many attempts to enter a correct PIN remain, if the incorrect PIN is entered too many times a PUK code will then be required for the SIM before it can be used again.

## 3.6.4 Advanced ADSL Settings

Go to page **Network -> ADSL Settings**

### DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Apply/Save

This page allows advanced settings for the ADSL interface to be adjusted. It is recommended that these settings are unchanged from their default values unless instructed by the ISP.

### 3.6.5 DMZ Host

Go to page **Network -> DMZ Host**

#### NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

This page allows an IP Address to be entered where all incoming traffic from the WAN interfaces will be routed. Noted that the "Virtual Servers" options take precedence--all traffic that do not match any application configured in Virtual Servers will be forwarded to the DMZ Host IP Address.

Enter the required IP Address and click the **Save/Apply** button.

### 3.6.6 Port Forwarding (Virtual Servers)

Go to path **Network -> Virtual Servers**

#### NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

This page allows the user to forward incoming traffic of selected ports on the WAN interfaces to internal hosts. This can be used to make internal applications available to the internet (e.g. a web server). Click the Add button to add a new forward:

#### NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".** Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

- Use Interface to select the WAN interface to forward from.
- Service Name either selects from the list of predefined services (e.g. Web Server (HTTP)) or enters a name for a custom service.
- Server IP Address enter the local IP Address to forward network traffic to.
- Ports Table if a predefined service is selected the table will be completed automatically. If a custom service is entered the table must be filled in manually.
  - ✧ Enter the range of IP addresses to match from the external (WAN) interface (start and end ports can be the same to match a single IP Address).
  - ✧ Select the Protocol (TCP, UDP or both TCP/UDP).
  - ✧ Enter the range of IP addresses to forward to the internal host. These can be the same as the external ports or the traffic can be forwarded to a different port on the internal host.

Enter the required values and then click the **Apply/Save** button.

### 3.6.7 Advanced IP Routing (Static Route)

Go to page **Network -> Static Route**

#### Routing -- Static Route (A maximum 32 entries can be configured)

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove
------------	---------------------	---------	-----------	--------	--------

This page allows the user to manually edit the routing table and create Static IP Routes. Note that in normal operation this is not required.

Click the Add button to add a new static route:

#### Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version:

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

- Destination IP address/prefix length ---- enter the destination in the format IP address/network prefix e.g. 124.80.0.0/16.
- Interface selects the network interface to route to.
- Gateway IP address specify the IP address for the gateway (if required).
- Metric (optional) specify the route metric.

Enter the required values and then click the **Apply/Save** button.

### 3.6.8 QoS Configuration

Please go to path: **Network -> QoS Configuration** page to enable Queue Management Configuration. If Enable QoS checkbox is selected, a default DSCP mark should be chosen to automatically mark incoming traffic without reference to a particular classifier. Click **Apply/Save** button to save.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces; The default DSCP mark is used to mark all egress packets that do not match any classification rules.

#### QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

**Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.**

**Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.**

Enable QoS

Select Default DSCP Mark

Please click **QoS QUEUE** button to enter the QoS Queue setup page, then click **Add** button. This screen allows you to configure a QoS queue and assign it to a specific layer 2 interface. The scheduler algorithm is defined by the layer 2 interface. Click **Apply/Save** to save and activate the queue.

#### QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

**Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others**

Click 'Apply/Save' to save and activate the queue.

Name:

Enable:

Interface:

Please click **QoS Class** button to enter QoS Classification Setup page, then click **Add** button to configure network traffic classes. This screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the rule.

### Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

### Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

## 3.7 Application

### 3.7.1 UPnP Settings

Go to path **Application -> UPnP**

#### UPnP Settings

Enable UPnP.

Use this page to enable or disable Universal Plug and Play (UPnP) functionality. UPnP allows networked devices to automatically discover each other.

By default UPnP is enabled -- it is recommended that this setting be left unchanged.

### 3.7.2 Dynamic DNS

Go to path **Application -> Dynamic DNS**

### Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
<input type="button" value="Add"/>	<input type="button" value="Remove"/>			

Dynamic DNS allows a static hostname to be assigned to a connection which is not assigned a static IP address. A subscription to a Dynamic DNS provider is required to maintain the mapping between the hostname and the currently assigned IP address.

Gateway can work with either the DynDNS or TZO dynamic DNS services.

Click the **Add** button and then enter the details provided by the dynamic DNS service provider

### 3.7.3 VPN (IPSec VPN)

Go to path **Application -> IPSec VPN**

#### IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove	Edit
<input type="button" value="Add New Connection"/>	<input type="button" value="Remove"/>				

Click the **Add New Connection** button to display the IPSec Settings:

**IPSec Settings**

IPSec Connection Name	<input type="text" value="new connection"/>
Remote IPSec Gateway Address (IP or Domain Name)	<input type="text" value="0.0.0.0"/>
Tunnel access from local IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Tunnel access from remote IP addresses	<input type="text" value="Subnet"/>
IP Address for VPN	<input type="text" value="0.0.0.0"/>
IP Subnetmask	<input type="text" value="255.255.255.0"/>
Key Exchange Method	<input type="text" value="Auto(IKE)"/>
Authentication Method	<input type="text" value="Pre-Shared Key"/>
Pre-Shared Key	<input type="text" value="key"/>
Perfect Forward Secrecy	<input type="text" value="Disable"/>
Advanced IKE Settings	<input type="button" value="Show Advanced Settings"/>

- IPSec Connection Name---- specify a name to identify the tunnel.
- Remote IPSec Gateway Address---- specify the IP address or FQDN for the remote end of the tunnel, this should be the internet IP address for the remote gateway.
- Tunnel access from local IP addresses ---- specify the IP address or subnet for the local side of the IPSec tunnel.
- Tunnel access from remote IP addresses---specify the IP address or subnet for the remote side of the IPSec tunnel.
- Key Exchange Method--select Auto to use the standard Internet Key Exchange (IKE) method or Manual to specify the encryption and authentication keys manually.
- Authentication Method--only Pre-Shared Key is supported.
- Pre-Shared Key -- enter the Pre-Shared Key.
- Perfect Forward Secrecy---- select whether to use the Perfect Forward Secrecy (PFS) method.

Fill in the required options and then click the **Apply/Save** button.

**3.7.4 VPN (PPTP Config)**

Go to path **Application -> PPTP Config**

**PPTP Config**

Choose Edit to modify information over PPTP WAN Service.

**Note:**If the table below is empty, please add WAN Service first! [Click Here](#)

Tunnel Name	Ip Address/Domain Name	WAN Interface	Enable	Default Gateway	Use Default Gateway	Status	Edit	Action
1_VOIP_INTERNET_R_orangeinternet	(null)	ppp3g0	NO	(null)	NO	Unconfigured		<input type="button" value="Connect"/>

A default PPTP tunnel is automatically created for each available WAN interface. Click the Edit button to configure the tunnel:

**PPTP Edit**

Tunnel Name:

Ip Address or Domain Name:

WAN Interface:

PNS Username:

PNS Password:

Enable:

Use Default Gateway On The Remote Network:

Authentication Method:

Use Static IP Address

- Tunnel Name-- specify a name to identify the tunnel.
- Ip Address or Domain Name --- specify the IP Address or FQDN for the remote PPTP Network Server.
- PNS Username - -specify the username required to login to the remote PPTP Network Server.
- PNS Password - -specify the password required to login to the remote PPTP Network Server.
- Enable--- set to use to start using the PPTP tunnel.
- Use Default Gateway on the Remote Network--- set to yes to forward traffic to the remote gateway.
- Authentication Method ---select the authentication method required to login to the PNS (PAP/CHAP/MSCHAP) or set to AUTO for the authentication method to be determined automatically.
- Use Static IP Address---select to specify the IP Address manually.

Set the required options and then click the **Apply** button

## 3.8 Wireless Configuration (WLAN)

### 3.8.1 WLAN Basic

Click **WLAN** to configure the wireless feature of the Gateway.

Go to path: WLAN -> WLAN Basic page to enable/disable WLAN feature. Then click **Apply/Save** button;

#### WLAN Basic Settings

Enable WLAN  
 Disable SSID broadcast

SSID:

BSSID: 00:05:b5:00:00:00

Country:

Max client number:

Channel:  Current channel: 1

Auto Channel Timer(min):

- Enable WLAN – select to enable the built-in WiFi access point.
- Disable SSID broadcast – select to prevent the Access Point from discovering. Users will need to manually specify the SSID to connect.
- SSID – enter the SSID to identify the WiFi access point, this is the name that will be displayed when users search for WiFi networks.
- Country – select the country where the CPE is installed
- Max client number – specify the maximum number of wireless clients that will be allowed. The CPE supports up to 16 simultaneous WiFi connections.
- Channel – select the Wireless channel to use. The channel number can be changed if interference is experienced.

After entering the required settings click the **Apply/Save** button.

### 3.8.2 WLAN Security

Go to path: WLAN -> WLAN Security page to set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click **Apply/Save** when done.

### WLAN Security Settings

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Enable WLAN security

Network Authentication:

WPA Pre-Shared Key:  [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

### 3.8.3 Advanced Settings

Go to path **WLAN -> Advanced Settings**

This page contains advanced parameters for the Wireless LAN interface.

It is strongly recommended that these settings be left unchanged unless there is a specific requirement for different settings in the environment where the GATEWAY is installed.

Altering these parameters may result in a reduction in Wireless performance.

### 3.8.4 WLAN MAC Filters

Go to path WLAN -> WLAN MAC Filters

#### Wireless -- MAC Filter

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address	Remove
-------------	--------

This page can be used to restrict the clients that are permitted to connect Wirelessly to the CPE.

**WARNING:** Changing the mode takes immediate effect and so may disconnect any connected Wireless clients.  
MAC Restrict Mode – select from the following:

- Disabled – all MAC Addresses will be allowed to connect.
- Allow – only MAC addresses listed below will be allowed to connect.
- Deny – all MAC Addresses will be allowed to connect EXCEPT those listed below.

Use the **Add** button to add MAC addresses to the list.

### 3.8.5 WLAN Bridge

Go to path WLAN -> WLAN Bridge

AP Mode:	<input type="text" value="Access Point"/>	
Bridge Restrict:	<input type="text" value="Enabled"/>	
Remote Bridges MAC Address:	<input type="text"/>	<input type="text"/>
	<input type="text"/>	<input type="text"/>

Use this page to configure Wireless Bridging functionality. Wireless Bridging allows a Wi-Fi network to be extended to cover a larger area through the use of multiple Wi-Fi bridge devices.

AP Mode:

- Access Point - The gateway can be used as both a Wireless Access Point and a Wireless Bridge (default).
- Wireless Bridge – The gateway can be used as a Wireless Bridge only.

Bridge Restrict:

- Enabled - only Wireless Bridges whose MAC Addresses are entered below may connect.
- Disabled - any Wireless Bridge may connect.

Remote Bridges MAC Address – enter MAC Addresses for remote bridges which are permitted to connect when “Bridge Restrict” option is enabled.

Enter the required settings and then click the **Apply/Save** button.

## 3.9 LAN Configuration (DHCP)

Configure the Gateway's IP address and DHCP options.

Go to path **DHCP -> LAN Setup**

### Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static DNS Server:

Get DNS Server From WAN

Configure the second IP Address and Subnet Mask for LAN interface

Set the required options then click the **Apply/Save** button

**Note:** changes will take effect immediately and if the IP Address of the gateway is changed the connection to the web interface will be lost. The new IP address will need to be entered into the web browser (The PC must be in the same subnet as the new IP address to view the webpage).

**IP Address** - enter the IP address that the gateway will be available on. The default IP address is 192.168.1.1.

**Subnet Mask** - enter the Subnet Mask. The default subnet mask is 255.255.255.0.

**Enable IGMP Snooping** - select to have the gateway monitor all IGMP network traffic for the purpose of reducing the multicast overhead (Advanced option)

**Disable DHCP Server** - turn off the built-in DHCP server. If the DHCP server is disabled all clients will need to have manually assigned IP addresses in order to connect.

**Enable DHCP Server** - turn on the built-in DHCP server

**Start/End IP Address** - enter the range of IP addresses that the DHCP server can assign to clients. These IP addresses must be in the same subnet as the IP address assigned to the gateway.

**Leased Time** - enter the duration for the lease of DHCP IP addresses (default is 24 hours)

**Static DNS Server** - enter an IP address for a DNS server to pass to DHCP clients. By default this is set to the IP address

of the GATEWAY to use the built-in DNS server (recommended).

**Get DNS Server from WAN** - select to pass the DNS server addresses obtained automatically from the WAN interface to the DHCP clients.

**Configure the second IP address** - select to assign an additional IP address to the gateway (advanced option).

**Note:**

1. When using the DHCP Servers, please make sure you don't have multiple DHCP Servers in one LAN.
2. To view a list of clients that have been assigned addresses by the DHCP server go to the path DHCP -> Assigned Leases
3. To reserve an IP address within the DHCP range for a client so that the client always receives the same IP address go to the path DHCP -> Static Leases. Click the Add Static Lease button and enter the MAC address and required IP Address for the client. Make sure that the IP address chosen is within the range entered on the LAN Setup page.

## 3.10 Firewall

### 3.10.1 Firewall Settings

Please go to path: **Firewall** -> **Firewall Settings** page, check **Enable** to activate **Global firewall settings**, then click **Apply/SAVE**.

**Note:** three Firewall levels are supported in the Gateway, they are:

- **Low:** enable basic firewall feature - prevent port from scanning; allow PING from WAN side; allow ICMP redirect messages from WAN side.
- **Middle:** based on low level, prevent ICMP redirect messages.
- **High:** based on middle level, prevent SYN Flood attack; against PING from WAN side.

#### Firewall Settings

Global firewall settings:  Enable

Firewall level Low ▼

Low

Middle

High

Apply/Save

**Note:** by default the Firewall is enabled and set to the "High" setting – it is recommended that to maintain maximum security this setting is not changed.

### 3.10.2 IP Filters

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic

can be **ACCEPTED** by setting up filters. Please go to path: **Firewall -> IP Filters -> Incoming IP Filtering Setup.**

**Incoming IP Filtering Setup**

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is **BLOCKED**. However, some IP traffic can be **ACCEPTED** by setting up filters. Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	------------	----------	---------------------	---------	---------------------	---------	--------

Click **Add** button to configure incoming IP filters. The following interface allows user to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

**Add IP Filter -- Incoming**

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

**WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces**

Select one or more WAN/LAN interfaces displayed below to apply this rule.

- Select All
- ppptd3g/ppptd3g0
- br0/br0

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Please go to path: **Firewall -> IP Filters -> Outgoing IP Filtering Setup.**

**Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose Add or Remove to configure outgoing IP filters.

Filter Name	IP Version	Protocol	SrcIP/ PrefixLength	SrcPort	DstIP/ PrefixLength	DstPort	Remove
-------------	------------	----------	---------------------	---------	---------------------	---------	--------

Click **Add** button to configure outgoing IP filters. The following interface allow user to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All of the specify conditions in this filter rule must be satisfied for the rule to take effect. Click **Apply/Save** to save and activate the filter.

### Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Apply/Save

### 3.10.3 Domain Filters

Please go to path: **Firewall -> Domain Filters** page. Please select the list type first and then configure the list entries.

List type:

**Exclude:** default accepts all the DNS except the list;

**Include:** default drop all the DNS except the list.

**domain Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.**

**Exclude: default accept all the DNS expect the list**

**Include: default drop all the DNS expect the list**

domain List Type:  Exclude  Include

Address	Port	Remove
---------	------	--------

Click **Add** to do the configuration after choosing a domain list type. Then set the domain address and port number in the coming interface. Click **Apply/Save** to add the entry to the domain filter.

#### Parental Control -- domain Add

Enter the domain address and port number then click "Apply/Save" to add the entry to the domain filter.

domain Address:

Apply/Save

### 3.10.4 MAC Filters

Please go to path: **Firewall -> MAC Filters** page to setup MAC filtering. All MAC layer frames will be forwarded except those matching with any of the specified rules in the settings.

#### MAC Filtering Setup

All MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. Choose Add or Remove to configure MAC filtering rules.

Protocol	MAC address	Remove
----------	-------------	--------

Please click **Add** to create a filter to identify the MAC layer frames by specifying at least one condition. If multiple conditions are specified, all of them will take effect. Click **Apply** to save and activate the filter.

#### Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type: 
  
 Source MAC Address: 
  
(eg: 00:90:96:01:2A:3B)

### 3.10.5 Access Control (Remote Access)

The Access Control feature allows ports to be opened to the internet (WAN) connections so that it is possible to connect remotely to the gateway.

Go to path **Firewall -> Access Control**

#### Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used. Only the service of WAN is Enabled, the WAN Port can be configured effectively.

Services	LAN	WAN	WAN Port
HTTP	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable	<input type="text" value="80"/>
ICMP	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="text" value="23"/>
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="text" value="69"/>

To enable remote access to the GATEWAY web interface and check the Enable box under WAN for the HTTP service. The default port is the standard web port 80 which can be changed by entering a new value under WAN Port.

Once enabled, it will be possible to access the web interface by browsing to the Internet IP Address assigned to the GATEWAY. For example, if the IP address assigned by the ISP is 80.70.60.50 and the WAN Port is set to 8080 the following would be entered into the web browser: `http://80.70.60.50:8080`

**Note:** *It is strongly recommended that the web interface password be changed (go to path Tools -> Access Control) before enabling the Access Control feature.*

This feature can be used via an ADSL or 3G connection. Note that some 3G networks have internal NAT and Firewall systems which do not allow remote access.

## 3.11 Voice

### 3.11.1 Voice Configuration

Connect a normal analogue telephone to the Phone port.

Phone calls can be made over the GSM/3G network (when a valid SIM is inserted) and using Voice over IP (when there is an active connection to the internet).

By default, all calls are dialed over the GSM/3G network. To make calls via VoIP (SIP) it is necessary to configure a connection to a SIP Service Provider:

### 3.11.2 Basic Settings

Go to path: **VoIP -> Basic Settings** page, then click on the Service Provider 0 tab.

Enter SIP parameters and click Apply to save the parameters.

Global Parameters	Service Provider 0
<b>Voice -- SIP Configuration</b>	
Enter the SIP parameters and click Start/Stop to save the parameters and start/stop the voice application.	
Locale Selection*:	USA - NORTHAMERICA <input type="button" value="v"/> <b>(Note: Requires vodsl restart to take affect)</b>
SIP Domain Name*:	<input type="text"/>
Voip Dialplan Setting:	9x.T 9x.#
<input checked="" type="checkbox"/> Use SIP Proxy.	
SIP Proxy:	<input type="text"/>
SIP Proxy Port:	5060
<input checked="" type="checkbox"/> Use SIP Outbound Proxy.	
SIP Outbound Proxy:	<input type="text"/>
SIP Outbound Proxy Port:	5060
<input checked="" type="checkbox"/> Use SIP Registrar.	
SIP Registrar:	<input type="text"/>
SIP Registrar Port:	5060

**Locale selection:** choose the Location---this will set the local tones etc. heard on the phone.

**SIP Domain Name:** enter the SIP Domain provided by the SIP Provider

**Voip Dialplan Setting:** specify the dial strings to be matched for VoIP calls. All numbers dialed which match one of the dial strings will be dialed via the SIP Service Provider; all numbers dialed which do not match any of the dial strings will be dialed via the GSM/3G network.

Key: x = any digit

. = 1 or more digits

T = dial after timeout

# = dial immediately when # terminator dialed

| = separator between dial strings

e.g. 9x.T|9x.# = all numbers starting with a 9 will be dialed via SIP (numbers will be dialed after a timeout or after a # is dialed)

012x.T|013x.T = all numbers starting with 012 or 013 will be dialed via SIP (numbers will be dialed after a timeout)

**Use SIP Proxy:** enable to allow using SIP Proxy. Enter the SIP proxy address (IP address or FQDN) and port

**Use SIP Outbound Proxy:** enable to allow using SIP Outbound Proxy. Enter the SIP Outbound Proxy address (IP address or FQDN) and port

**Use SIP Registrar:** enable to register to a SIP server. Enter the SIP Registrar address (IP address or FQDN) and port.

<b>SIP Account</b>	0
<b>Account Enabled</b>	<input checked="" type="checkbox"/>
<b>Physical Endpt Id</b>	0
<b>Authentication Name</b>	1001
<b>Password</b>	1001
<b>Preferred Ptime</b>	20 ▾
<b>Preferred Codec 1</b>	G.711ALaw ▾
<b>Preferred Codec 2</b>	G.729a ▾
<b>Preferred Codec 3</b>	G.723.1 ▾
<b>Preferred Codec 4</b>	G.726_24 ▾
<b>Preferred Codec 5</b>	G.726_32 ▾
<b>Preferred Codec 6</b>	GSM_AMR_12K ▾

**Authentication Name** - the username which is provided by the SIP provider.

**Password** - the password which is provided by the SIP provider.

**Preferred codec list** - select the order of the audio codecs to be used.

Once the configuration is completed, click the **Apply** button to save changes. Click **Stop SIP client**, and then click **Start SIP client** to enable the configuration.

### 3.11.3 Advanced Settings

Go to path: **VoIP -> Advanced Settings** page, to configure the advanced VoIP features.

Voice -- SIP Advanced Configuration	
Line	1
Echo Cancellation	<input checked="" type="checkbox"/>
Call Waiting	<input type="checkbox"/>
Call Forwarding Number	
Forward Unconditionally	<input type="checkbox"/>
Forward on "Busy"	<input type="checkbox"/>
Forward on "No Answer"	<input type="checkbox"/>
MWI	<input type="checkbox"/>
Call Barring	<input checked="" type="checkbox"/>
Call Barring Pin	9999
Call Barring Digit Map	
Anonymous Call Blocking	<input type="checkbox"/>
Anonymous Calling	<input type="checkbox"/>
DND	<input type="checkbox"/>
Silence Suppression	<input checked="" type="checkbox"/>
CNG	<input checked="" type="checkbox"/>
Ingress Gain	0 ▾
Egress Gain	0 ▾

**Echo Cancellation** - select to enable the built-in echo canceller

**Call forwarding Number:** set a number to use call-forwarding. Select the conditions to use call forwarding by ticking the required boxes.

**MWI** - select to enable MWI (Message Waiting Indicator) support

**Call Barring** - select to enable Call Barring

**Anonymous Call Blocking** - select to disallow incoming calls with no CLI

**Anonymous Calling** - select to withhold CLI on outgoing calls

**DND** - select to enable DND (Do Not Disturb) support

**Silence Suppression** - when selected audio packets will not be transmitted to the network if no audio is detected to reduce bandwidth usage

**CNG** - select to enable detection of CNG (Fax) tones

**Ingress Gain** - used to increase or decrease the volume of the incoming audio

**Egress Gain** - used to increase or decrease the volume of the outgoing audio

<input type="checkbox"/> Enable T38 Support	
<input checked="" type="checkbox"/> Enable V18 Support	
Registration Expire Timeout*	0
Registration Retry Interval	0
DSCP for SIP*	EF (101110) ▼
DSCP for RTP*	EF (101110) ▼
Dtmf Relay Setting*	InBand ▼
Hook Flash Relay Setting*	None ▼
SIP Transport Protocol*	UDP ▼
<input checked="" type="checkbox"/> Enable SIP Tag Matching* (Uncheck for Vonage Interop).	
<input type="checkbox"/> SIP Prack	
Music Server*:	
Music Server Port*:	0

**Enable T38 Support** - enable support for T.38 fax compatible devices

**Enable V18 Support** - enable support for V.18 Textphone compatible devices

**Registration Expire Timeout** - enter the timeout length for the registration

**Registration Retry Interval** - enter the retry interval for the registration

**DSCP for SIP/RTP** - select the codepoint to use when connecting via QoS compatible systems

**Dtmf Relay Setting** - select the format to transmit DTMF tones to the network. Tones can be transmitted In-Band or Out-Of-Band (SIP INFO or RFC2833)

**Hook Flash Relay Setting** - select whether local Hook Flash should be ignored or sent as SIP INFO packet

**SIP Transport Protocol** - select the protocol (UDP or TCP) to use for SIP packets. Most systems use UDP.

**Enable SIP Tag Matching** - uncheck when using with Vonage

**SIP Prack** - use the SIP Prack method instead of ACK

**Music Server** - enter an address and port for an external music server to provide music on hold.

## 3.12 Tools

### 3.12.1 Account Settings (Users)

When you configure the GATEWAY through an Internet browser, the system requires user name and password to validate access permission. The factory sets the default username of "admin" and the password of "admin". Go to path **Tools -> Account Settings**, you can choose the username and change the password.

#### Access Account

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:	<input type="text"/>
new name:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

**Note:** please remember the password after change, otherwise you will need to reset the device and will lose all configuration settings.

### 3.12.2 Time Settings

Go to path **Tools -> Time Settings**

From this page the current time can be set manually or the GATEWAY can be set to obtain the correct time from an internet time server.

**Note:** it is recommended that an internet time server is used when available if the time is set manually it will be lost in the event of a power cut or if the unit is restarted.

Current Time: Thu Jan 1 10:46:42 1970

Set Time Mode:  Time Server  Manual Setting

Time Server:

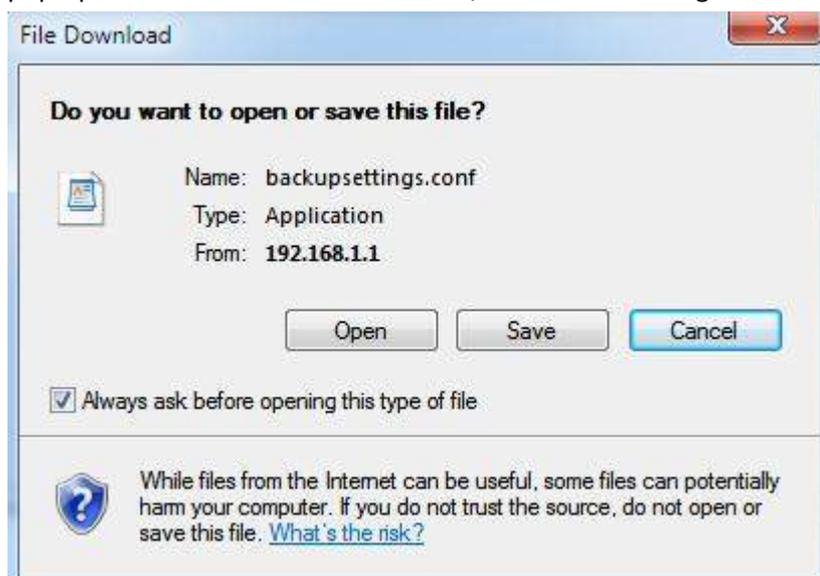
Time Zone Offset: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Enter the required options and click the **Apply/Save** button.

### 3.12.3 Backup Settings

To backup the current configuration to a file:

Please go to path: **Tools -> Backup Settings** page. Click Backup Settings button, then a File download window will pop-up. Click **Save** button to download/save current configuration of the device to the PC.



### 3.12.4 Update (Restore) Settings

Please go to path: **Tools -> Update Settings** page. Click **Browse** button to choose a configuration file, then click **Update Settings** to restore configuration.

## Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

## 3.12.5 Update Software

Please go to path: **Tools -> Update Software** page. Click **Browse** to choose the right software. Then click **Update Software** to update.

The power LED will go **red** to indicate that the software upgrade is in progress. Once complete the unit will automatically restart with the new software. The current software version can be viewed by going to path **Status -> Basic Info**

**Attention:** please make sure the power to the device is not interrupted during the software updating process. Also, the RJ45 cable should be connected tightly between the PC and device during the software uploading process.

Once updated, please press the reset button or go to path: **Tools -> Factory Settings** to restore the device to the new factory default settings if necessary.

### Update Software

**Step 1:** Obtain an updated software image file from your ISP.

**Step 2:** Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

**Step 3:** Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

## 3.12.6 Factory Settings

To restore the GATEWAY to the factory default configuration either press the **Reset** button on the side of the unit or go to path **Tools -> Factory Settings** and click the **Restore Default Settings** button.

**Note:** all user entered configuration options will be lost.

### 3.12.7 Reboot Router

To perform a soft restart of the GATEWAY go to path **Tools -> Reboot Router** and click the **Reboot** button. A restart takes approximately 2 minutes.

### 3.12.8 TR-069 Client

The GATEWAY can be provisioned remotely via the use of a TR-069 remote management server.

Please go to path: **Tools -> TR-069 Client** page to setup an auto-configuration server to perform auto-configuration, provision, collection and diagnostics to this device. Select the desired values and click **Apply/Save** to configure the TR-069 client options.

Note: all the parameters in the screenshot should be matched with the TR-069 Server.

#### TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Safe Link:	<input type="button" value="Cert Import"/>
Inform Interval:	<input type="text" value="300"/>
ACS URL:	<input type="text" value="http://200.48.229.23:70"/>
ACS User Name:	<input type="text" value="001aa92e202d"/>
ACS Password:	<input type="password" value="....."/>
WAN Interface used by TR-069 client:	<input type="text" value="Any_WAN"/>
Display SOAP messages on serial console	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	<input type="text" value="admin"/>
Connection Request Password:	<input type="password" value="....."/>
Connection Request URL:	<input type="text" value="(null)"/>

### 3.12.9 Ping Reboot

The "Ping Reboot" feature can be used to monitor the status of the internet connection and to automatically restart the GATEWAY when the internet connection is unavailable.

Go to path **Tools -> Ping Reboot**

### Ping Reboot Settings

Disable Ping Reboot

Enable Ping Reboot

Ping IP Address:

Ping Interval(range:10min~3600min):

Enter an IP Address to ping in order to test the internet connection and a ping interval of how often to check the connection.

### 3.12.10 3G Link Notice

The 3G Link Notice feature can be used to send an SMS to inform the user when the 3G data connection is unavailable.

#### 3G Link Notice

3G Link UP Notice:  Enable

Mobile Number

Enter the Mobile Number to send the SMS to and click the **Apply/Save** button.

## Chapter 4. Troubleshooting

### 4.1 Factory Settings

**IP:** 192.168.1.1

**DHCP Server:** Enable

**User name:** admin

**Password:** admin

### 4.2 Troubleshooting

This section of the document describes possible problems encountered when using the Robustel W800 Gateway and their solutions.

#### 4.2.1 Unable to Access Internet

##### 4.2.1.1 Check the Line and the Device

1. Check the indicator of power supply is on, if not, make sure the connection of power supply is correct; make sure the output of power supply is correct; make sure the switch of power supply is turned on;
2. Check the indicator of PC is on, if not, Make sure the connection of cable and network adapter; Make sure that the correct cable is used;
3. Check the DSL LED to see if it is twinkling. If no fast twinkling is observed within 3 minutes, please check whether phone line has been correctly placed; whether ADSL separator is correctly used. If multiple extensions have been installed, make sure that the separator is installed prior to the junction box of phone line. If the above items are confirmed and still no fast twinkling of DSL LED is observed, call the ISP to query whether ADSL service has been provided on your line;
4. Check the DSL LED to see whether it is unable to change status from fast twinkling to always light, or whether it changes status to fast twinkling after sometime of always light. If these phenomena occur constantly, please contact your ISP with a demand to check lines and signal quality;

If there is no problem in the above items, the line and the device shall be working. Problems may come from your computer configuration or device configuration.

## 4.2.1.2 Check Your Configuration

We explain here the configuration of PPPOE using Windows XP operation system as an example. For other operation systems the process is similar.

1. Enter the device manager to check if Ethernet adapter is correctly installed. If any problem exists, please re-installed it;
2. Check the configuration of Ethernet adapter in PC. Try to manually set IP address that is in band 192.168.1.X without conflict;
3. Try to run command “ping 192.168.1.1” on command line mode. If the response returns “time out”, please check Ethernet connection and IP settings;
4. If this Gateway is reachable, try to run ping with a known outer IP, e.g. the DNS server IP of Google: “ping 8.8.8.8”.
  - If ping is reachable, there shall be no problems in the Gateway. Please see step 5;
  - If ping is not reachable, see step 6 and check if the configuration is correct.
5. Please try to ping a certain outer URL, e.g. “ping www.google.com”.
  - If ping is reachable, there shall be no problems in the network settings. Please check the settings of the PC terminal, e.g. whether the security level is too high, or whether anti-virus firewall is installed;
  - If ping is not reachable, check the DNS setting of Ethernet adapter.

**Note:**

1. The precondition is that LAN settings in the Gateway have not been modified.
2. We usually start command line mode in Windows XP as follows: click on the “RUN” item of Windows Start Menu, input characters “cmd” in the input box popped up with an “Enter”. The window subsequently popped up is the command line window.
3. The returned values of ping command in the following format show the standard of “reachable”.

```
C:\Users\Pretender>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. If ping of the Gateway is reachable but ping of the outer fixed IP is unreachable, attention should be concentrated upon device settings. Please enter the configuring interface and follow the instructions in this manual.
  - a. Check first the number of connections. If more than one connection exists, for troubleshooting, delete unused connections and remain the one connection you are using.
  - b. Check the connection to see whether correct “type” is selected. It’s normal to choose login type of PPPoE. When you use PPPoE to login, the following information should be provided: VPI and VCI, which can be queried from your ISP, user name and password.
  - c. Then make sure that “using NAT” and “default gateway” have been selected with a tick. Check whether “connect

on demand” has been selected with a tick. If it is selected, the connection is activated only when traffic to outer networks arrives. If not selected, check “keep connection”, which should be set to 0 if you demand to keep connection

Make sure that the above parameters are saved after configuration. Internet is now available since the configuration is properly done.

### 4.3 Terms and Abbreviations

Abbreviations	Description
802.11b	An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 11Mbps
802.11g	An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 54Mbps
802.11n	An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 600Mbps
AC	Alternating Current
ADSL	Asymmetric Digital Subscriber Line
AP	Access Point
APN	Access Point Name of GPRS Service Provider Network
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCS 1800	Digital Cellular System, also referred to as PCN
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
FoIP	Fax over IP
Gateway	A network point that acts as an entrance to another network
GND	Ground
GPRS	General Package Radio Service
GSM	Global Standard for Mobile Communications
HSDPA	High Speed Download Packet Access
HSUPA	High Speed Upload Packet Access
IMEI	International Mobile Equipment Identification
IP	Internet Protocol

LAN	Local Area Network
kbps	kbits per second
LED	Light Emitting Diode
MAC	Media Access Control
MAX	Maximum
Min	Minimum
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PPP	Point-to-point Protocol
PIN	Personal Identity Number
PSU	Power Supply Unit
PSTN	Public Switched Telephone Network
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
SIM	Subscriber Identification Module
SMA	Subminiature Version A RF Connector
SSID	Service Set Identifier
T.38	An ITU standard for sending FAX accross IP networks in a real-time mode
TCP/IP	Transmission Control Protocol / Internet Protocol
UMTS	Universal Mobile Telecommunications Service
URL	Uniform Resource Locator
VoIP	Voice over IP
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network
WCDMA	Wideband CDMA
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2