

User Manual

BDE761AM-001

WiFi Broadband BG



TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 6

1.1 CONTENTS LIST 6

1.2 HARDWARE INSTALLATION 7

 1.2.1 WARNING 7

 1.2.2 SYSTEM REQUIREMENTS..... 7

 1.2.3 Hardware Configuration 9

 1.2.4 LED Indicators..... 10

CHAPTER 2 GETTING STARTED 11

2.1 EASY SETUP BY WINDOWS UTILITY 11

2.2 EASY SETUP BY CONFIGURING WEB UI 14

CHAPTER 3 MAKING CONFIGURATIONS..... 19

3.1 BASIC NETWORK 22

 3.1.1 WAN Setup..... 22

 3.1.1.1 Physical Interface..... 23

 3.1.1.2 Network Setup 24

 3.1.1.2.1 Wireless WAN – 3G/4G24

 3.1.1.2.2 Ethernet WAN27

 3.1.2 LAN & VLAN Setup 36

 3.1.2.1 Network Setting..... 36

 3.1.2.2 LAN & VLAN 37

 3.1.2.2.1 Port-Based VLAN.....37

 3.1.2.2.2 Tag-Based VLAN.....38

 3.1.2.3 DHCP Server 39

 3.1.3 Wireless Setup 42

 3.1.3.1 Wireless Setup..... 42

 3.1.3.1.1 AP Router Mode.....42

 3.1.3.1.2 WDS Hybrid Mode46

 3.1.3.1.3 WDS Only Mode.....48

 3.1.3.2 Advanced Wireless Setup 49

 3.1.4 IPv6 Setup..... 51

 3.1.4.1 Static IPv6..... 51

 3.1.4.2 DHCP v6 53

 3.1.4.3 PPPoE 54

 3.1.4.4 6 to 4 55

 3.1.4.5 IPv6 in IPv4 Tunnel..... 56

3.1.5	NAT Setup.....	57
3.1.5.1	Virtual Server	57
3.1.5.2	Virtual Computers	58
3.1.5.3	Special AP	58
3.1.5.4	NAT Loopback	59
3.1.5.5	DMZ	60
3.1.6	Routing Setup.....	61
3.1.6.1	Static Routing.....	61
3.1.6.2	Dynamic Routing.....	61
3.1.6.3	Routing Information.....	63
3.1.7	Client/Server/Proxy	64
3.1.7.1	Dynamic DNS	64
3.2	ADVANCED NETWORK.....	65
3.2.1	Firewall	65
3.2.1.1	Packet Filters	65
3.2.1.2	URL Blocking	67
3.2.1.3	Web Content Filter	67
3.2.1.4	L7 Application Filter.....	68
3.2.1.5	IPS	69
3.2.1.6	MAC Address Control	70
3.2.1.7	Others	72
3.2.2	QoS (Quality of Service).....	72
3.2.2.1	Rule-based QoS	73
3.2.3	VPN Setup.....	77
3.2.3.1	VPN-IPSec.....	77
3.2.3.1.1	Dynamic IP VPN.....	78
3.2.3.1.2	IPSec-IKE Setting	81
3.2.3.1.3	IPSec-Manual Setting	84
3.2.3.1.4	XAUTH Account.....	85
3.2.3.2	VPN-PPTP Server.....	86
3.2.3.3	VPN-PPTP Client.....	87
3.2.3.4	VPN-L2TP Server	89
3.2.3.5	VPN-L2TP Client.....	90
3.2.3.6	GRE Tunnel	92
3.2.4	Redundancy	93
3.2.4.1	VRRP.....	93
3.2.5	Management.....	94
3.2.5.1	UPnP.....	94
3.2.5.2	SNMP.....	95

3.3	SYSTEM	97
3.3.1	System Information	97
3.3.2	System Status	98
3.3.2.1	Web Log	98
3.3.2.2	Syslog	98
3.3.2.3	Email Alert	98
3.3.3	System Tools	99
3.3.3.1	Change Password	99
3.3.3.2	FW Upgrade	100
3.3.3.3	System Time	101
3.3.3.4	Others	102
3.3.4	Scheduling	103
3.3.5	MMI	104
3.3.5.1	Web UI	104
CHAPTER 4	TROUBLESHOOTING	105
CHAPTER 5	APPLICATION DESCRIPTION	109
5.1	VLAN APPLICATION	109
5.2	VPN SETUP	112
5.3	REDUNDANCY	116
APPENDIX A	LICENSING INFORMATION	117

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 their respective companies. 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.

Chapter 1 Introduction

Congratulations on your purchase of this outstanding product: BDE761-001 WiFi 2.4G Business Gateway. This device is specifically designed for those who need to have the data, voice, video and file sharing services beyond his home and office. It provides a complete solution for Internet surfing and broadband sharing. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Contents List

Items	Description	Contents	Quantity
1	WiFi 2.4G Business Gateway		1pce
2	WiFi Antenna		2pce
3	Power Adapter		1pce
4	RJ45 Cable		1pce
5	CD		1pce

1.2 Hardware Installation

1.2.1 WARNING



Attention

- Do not use the product in high humidity or high temperatures.
- Do not use the same power source for the Product as other equipment. Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.
- Do not open or repair the case yourself. If the Product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the Product on a stable surface and avoid using this product and all accessories outdoors.

1.2.2 SYSTEM REQUIREMENTS

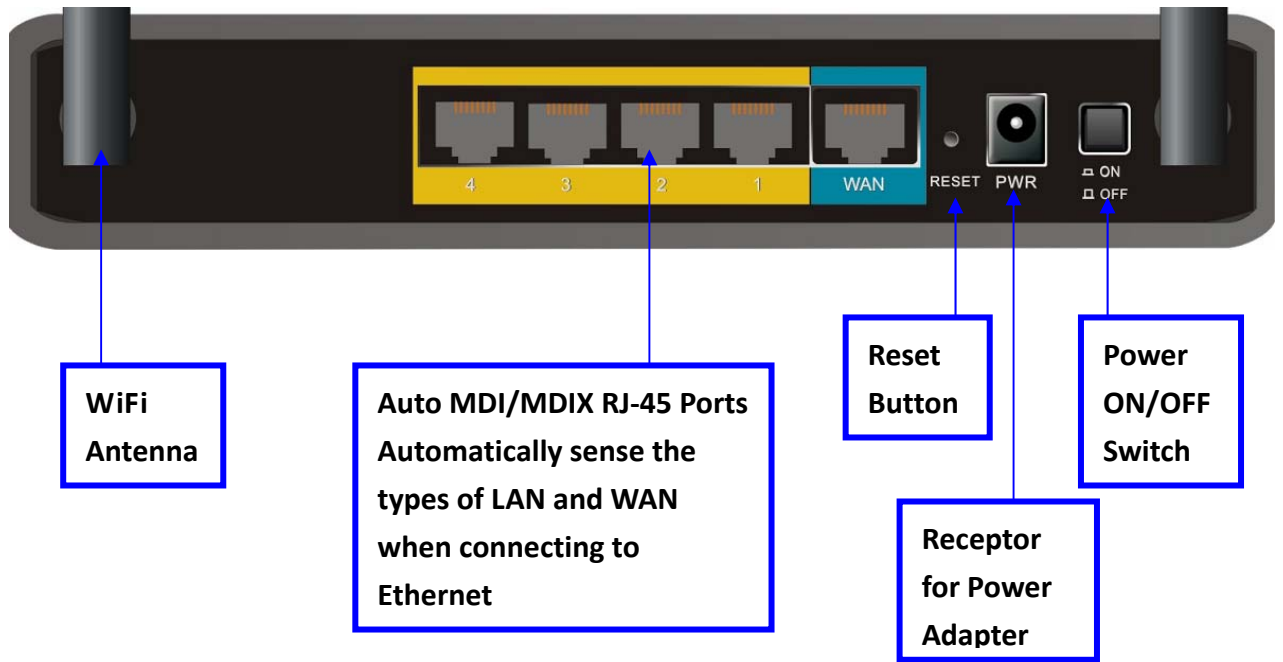
Network Requirements	<ul style="list-style-type: none">● An Ethernet-based Cable or DSL modem● 3G/4G cellular service subscription● IEEE 802.11n or 802.11b, g wireless clients● 10/100 Ethernet
Web-based Configuration Utility Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">● Windows®, Macintosh, or Linux-based operating system● An installed Ethernet adapter <p>Browser Requirements:</p> <ul style="list-style-type: none">● Internet Explorer 6.0 or higher● Chrome 2.0 or higher● Firefox 3.0 or higher● Safari 3.0 or higher (with Java 1.3.1 or higher)

WiFi Broadband BG

	Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	Computer with the following: <ul style="list-style-type: none">• Windows® 7, Vista®, or XP with Service Pack 2• An installed Ethernet adapter• CD-ROM drive

1.2.3 Hardware Configuration

Rear View:








Front View:



1.2.4 LED Indicators



LED		Description
Power/Status		Orange: ON during power on (@bootloader) Green: Normal flash per second Orange in flash: The device is in recovery mode or abnormal.
WAN		Green: Ethernet connection is established Green in flash: data packet transferred via Ethernet
Wi-Fi		Green in flash: data packet transferred. Green in flash per second during 2min:WPS PBC status Dark: Wireless Radio is disable
LAN1 ~ LAN4		Green: Ethernet connection is established Green in flash: data packet transferred via Ethernet
USB		Green: USB connection is established Green in flash: data packet transferred through USB

Chapter 2 Getting Started

Please use windows EZ setup utility or Web UI wizard to enter the setup process.

2.1 Easy Setup by Windows Utility

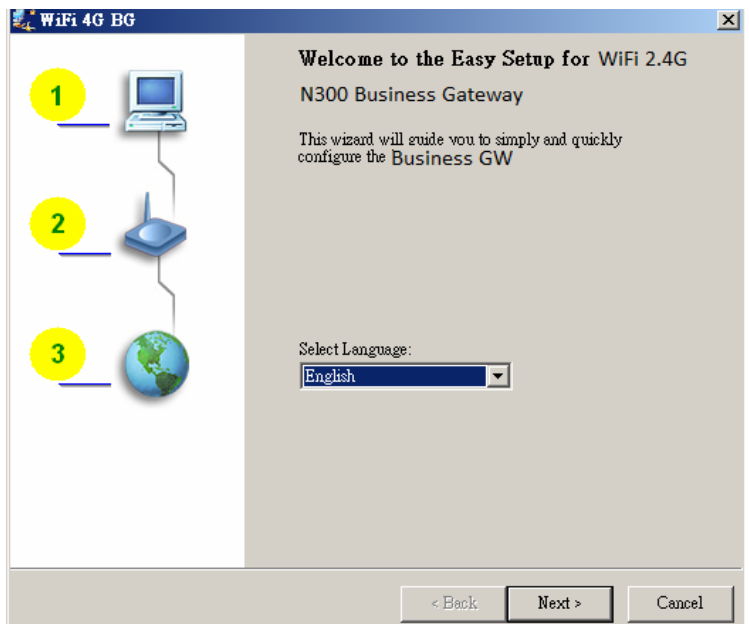
Step 1.

Install the Easy Setup Utility from the provided CD then follow the steps to configure the device.



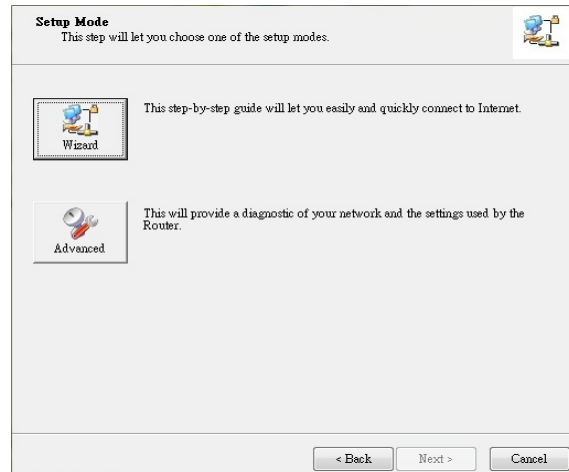
Step 2.

Select Language then click “Next” to continue.



Step 3.

Then click the **“Wizard”** to continue.



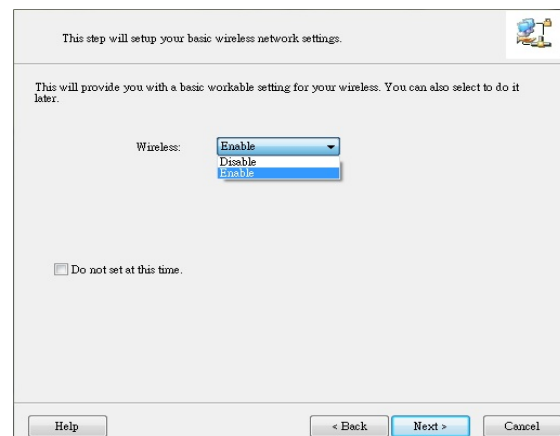
Step 4.

Click **“Next”** to continue.



Step 5.

Select Wireless Enable, and then click **“Next”** to continue.



Step 6.

Enter SSID, Channel and Security options, and then click “Next” to continue.

This step will setup your basic wireless network settings.

Please assign the parameters to your wireless networking. If you need more settings, please login to the Router's configuration page.

SSID: default
Channel: 6
Security: WEP
Key: ●●●●●●●●

Buttons: Help, < Back, Next >, Cancel

Step 7.

Select Auto Detect WAN service.

Auto Detect WAN Service
This step will automatically detect one suitable WAN service for Router.

Please make sure the WAN cable connection is working between your Router and broadband modem.
You can ignore the WAN cable connection, but the WAN service will not be checked later.
You can set it manually if you know your WAN service type.

Let me select WAN service by myself

Buttons: Help, < Back, Next >, Cancel

Step 8.

Save the setting.

Save Settings

The settings will be saved to the Router and reboot at the next step.

Wireless Setting
Wireless Mode: AP Only Mode
SSID: default
Channel: 6
Security: Disable

WAN Setting (Dynamic IP Service)

Modify Settings

Buttons: Help, < Back, Next >, Cancel

Step 9.

Congratulations! Setup is completed.
Now you have already connected to Internet successfully.



2.2 Easy Setup by Configuring Web UI

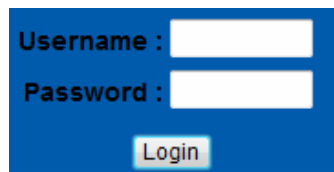
You can also browse web UI to configure the device. Firstly you need to launch the Setup Wizard browser first and then the Setup Wizard will guide you step-by-step to finish the basic setup process.

Browse to Activate the Setup Wizard

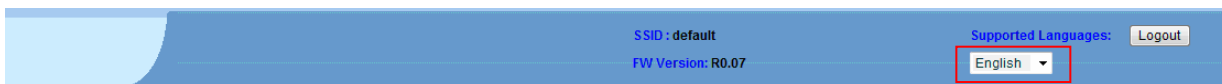
Type in the IP Address (<http://192.168.123.254>)



Type the default Username and password '**admin**' in the System Password and then click '**login**' button.



Select your **language**.

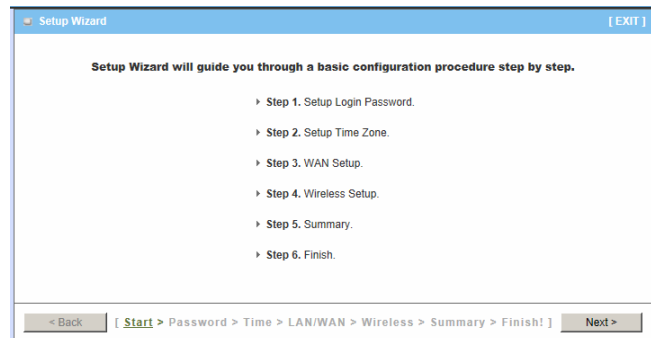


Select “**Wizard**” for basic settings in a simple way.

Or, you can go to **Basic Network / Advanced Network / Applications / System** to setup the configuration by your own selection.



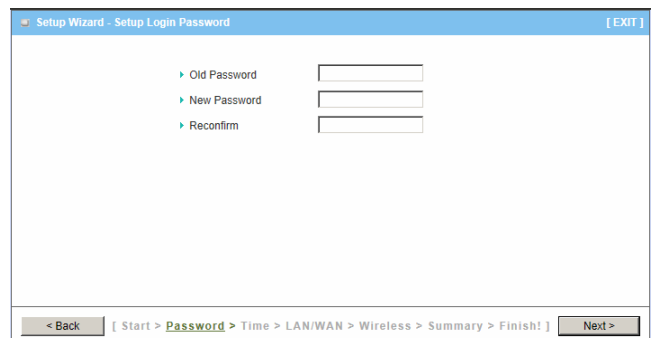
Press “**Next**” to start the Setup Wizard.



Configure with the Setup Wizard

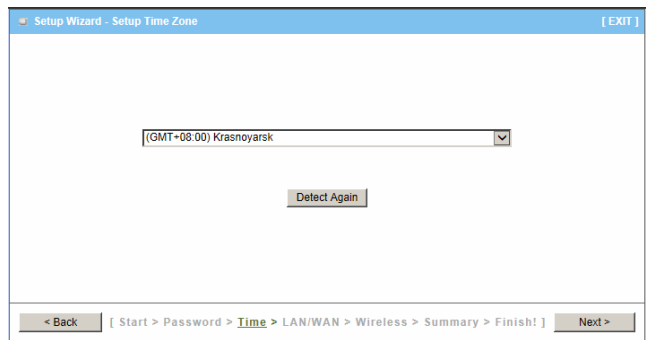
Step 1

You can change the password of administrator here.



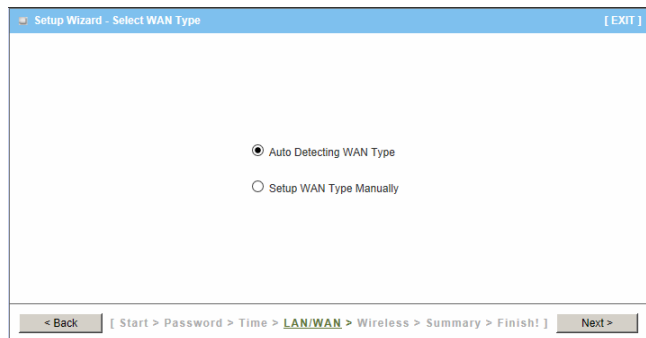
Step 2

Select Time Zone.



Step 3

You can select Auto detecting WAN type or setup WAN type manually.



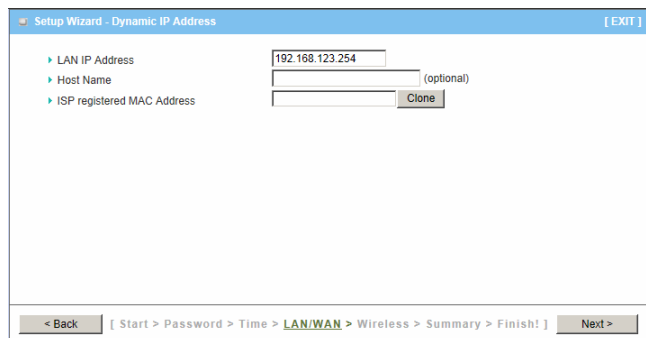
Step 4

The system will detect the WAN type if you choose to let the system detect automatically.



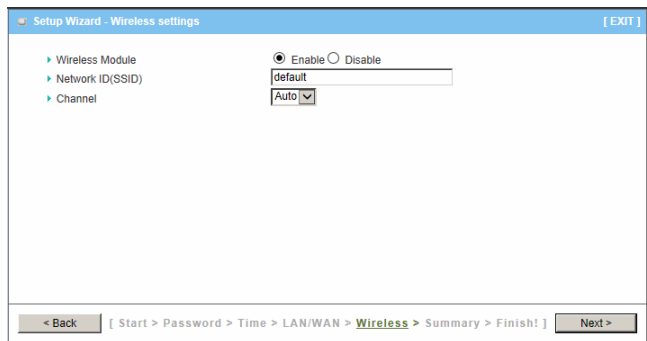
Step 5

Type in Host name and ISP registered MAC address. (if no such information, you can go next)



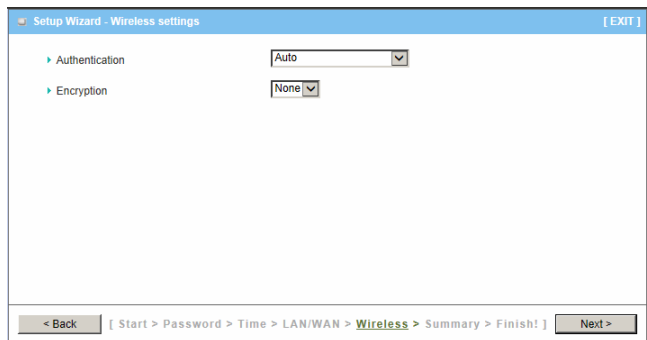
Step 5-1

Wireless setting.



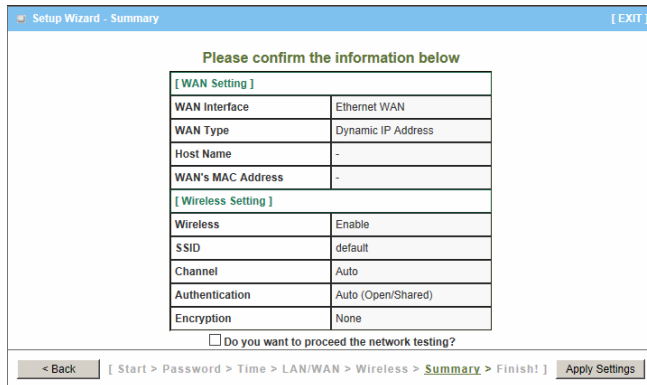
Step 5-2

Wireless authentication and encryption.



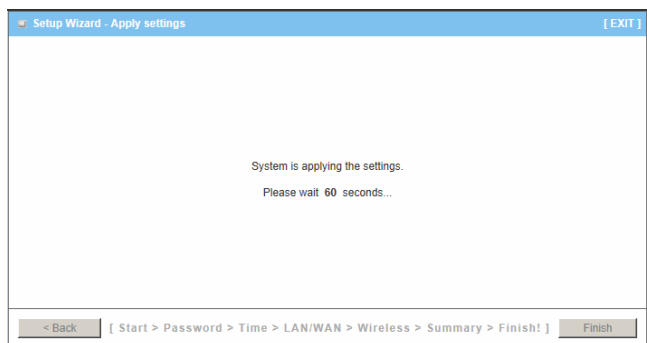
Step 6

Check the information again.



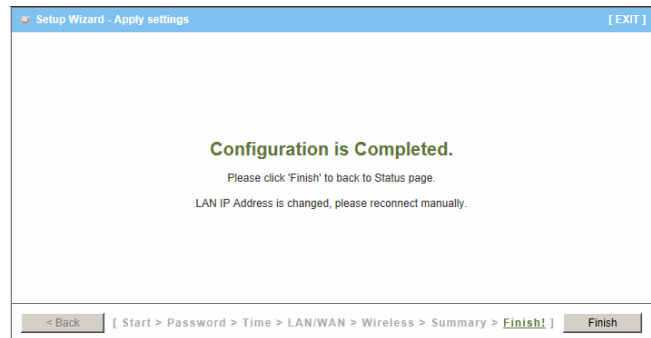
Step 7

System is applying the setting.



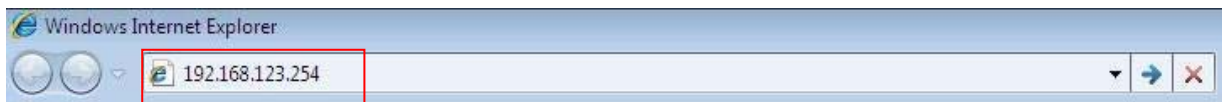
Step 8

Click finish to complete it.



Chapter 3 Making Configurations

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the device. The default IP Address is: **192.168.123.254**. In the configuration section you may want to check the connection status of the router, to do Basic or Advanced Network setup or to check the system status. These task buttons can be easily found in the cover page of the UI (User Interface).



Enter the default username and password “**admin**” in the System Password and then click ‘**login**’ button.

A screenshot of the router's web interface. On the left, there is a login section with a "Password:" label, an input field, a "Login" button, and the text "(default: admin)". This section is highlighted with a red box. The main area shows a central router icon with various connection status icons: 3G/4G (with a red 'X'), xDSL/Cable (with a red 'X'), WiFi (Client:0), and Ethernet (Client:1). Below this is a table titled "IPv4 System Status" with a "[HELP]" link.

Item	WAN Status	Sidenote
Remaining Lease Time	-	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

Afterwards, you can go **Wizard**, **Basic Network**, **Advanced Network**, **Application** or **System** respectively on left hand side of web page.



Note: You can see the Connection Status screen below after you logged in.

Item	WAN Status	Sidenote
Remaining Lease Time	-	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0 , 0.0.0.0	Edit

Item	Status	Sidenote
Card Info	N/A	
Link Status	Disconnected.	
Signal Strength	N/A	
Network Name	N/A	

	Receive	Transmit
WAN	0 Packets	6 Packets
LAN	39628 Packets	34789 Packets
WLAN	470 Packets	0 Packets

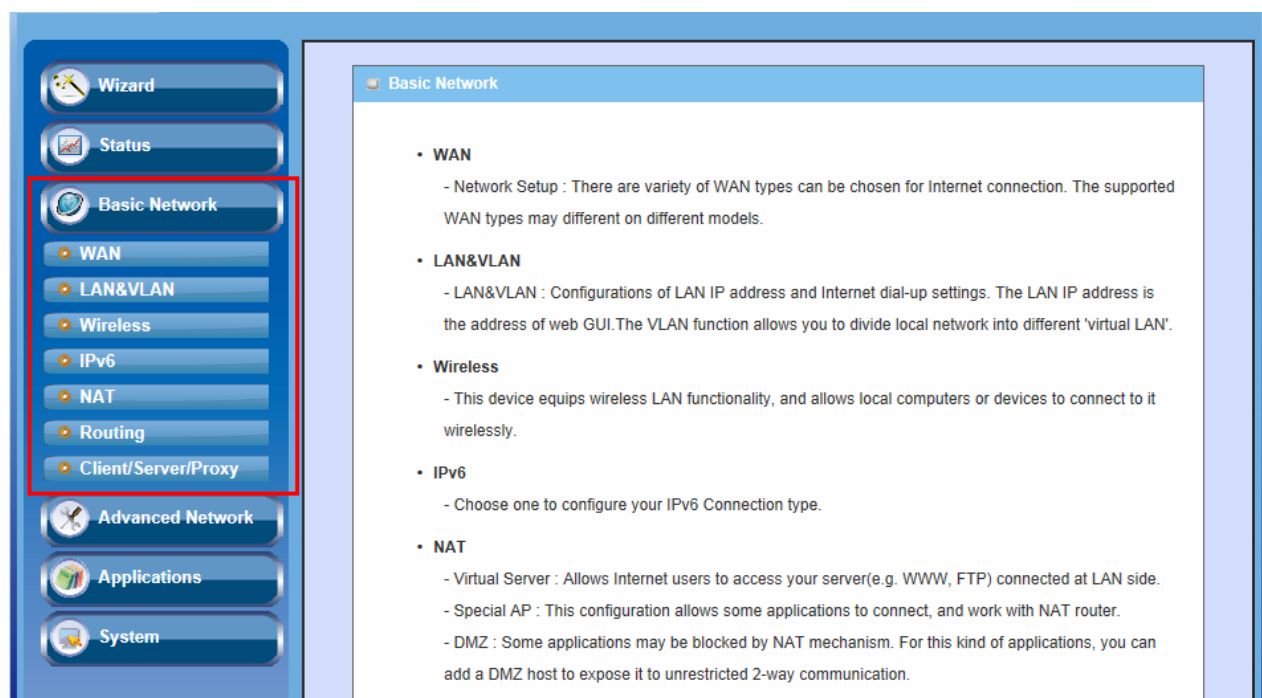
Wireless Status AP 1		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	default	<input type="button" value="Edit"/>
Channel	Auto	
Security	Auto	(None)
MAC address	00:50:18:00:07:F0	

Wireless Status AP 2		
Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	default	<input type="button" value="Edit"/>
Channel	Auto	
Security	Open	(None)
MAC address	00:50:18:00:06:F0	

Note : You can see all the status of this device in the 'Status' main menu section.

3.1 Basic Network

You can enter Basic Network for **WAN, LAN&VLAN, Wireless, IPv6, NAT, Routing, and Client/Server/Proxy** settings as the icon here shown

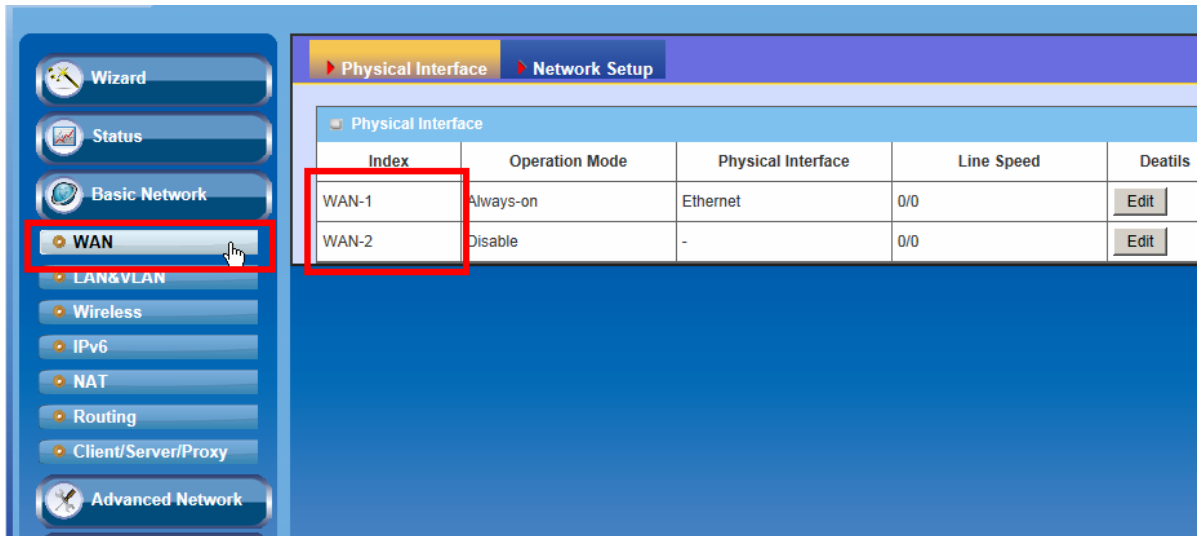


3.1.1 WAN Setup

This device is equipped with two WAN Interfaces to support different WAN types of connection. You can configure one by one to get proper internet connection setup.

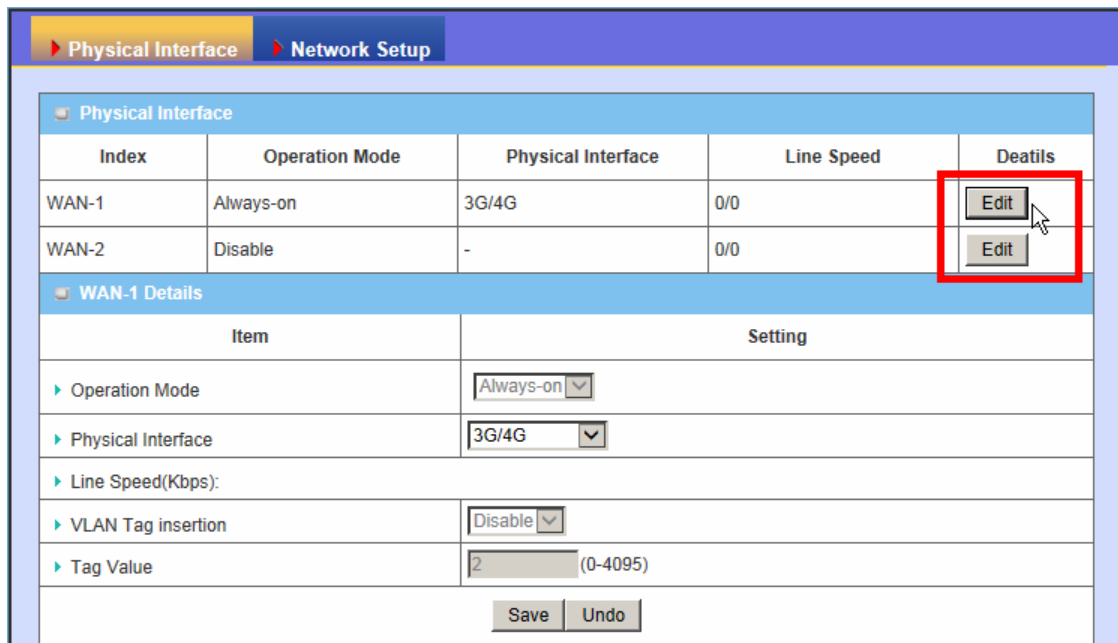
3G/4G WAN: The router has one USB Port and support 3G/4G USB Dongle follow UI setting to setup.

Ethernet WAN: The router has one RJ45 WAN port can be configured to WAN connection. Please plug in RJ45 cable from your external DSL modem and follow UI setting to setup.



3.1.1.1 Physical Interface

Click on the “**Edit**” button for each WAN interface and you can get the detail physical interface settings and then configure the settings as well.



1. **WAN-1:** The operation mode of this interface is forced to “**Always-on**” mode, and operates as the primary internet connection. You can click on the respective “**Edit**” button and configure the rest items for this interface.
2. **WAN-2:** The operation mode of this interface is disabled by default, you can click on the respective “**Edit**” button and configure the second WAN interface to operate as “**fail over**” mode, so that when the WAN-1 connection broken, the device will try to failover the internet connection to WAN-2.
3. **Physical Interface:** Select the WAN interface from the available list. For this

device, there are “Ethernet” and “3G/4G” items. If you would like the RJ45 WAN port to operate as the primary internet connection, Please choose “Ethernet”; Otherwise, choose “3G/4G” for configuring the embedded 3G/4G modem as primary WAN connection.

4. **Line Speed (Kbps):** You can specify the downstream / upstream speed for the corresponding WAN connection. Such information will be referred in QoS and load balance function to manage the traffic load for each WAN connection.
5. **VLAN Tag Insertion, Tag Value:** If your ISP required a VLAN tag been inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.1.2 Network Setup

There are two physical WAN interfaces that you can configure one by one to get proper internet connection setup. They include the Wireless WAN - the remote wireless ISP such as 3G (WCDMA, HSxPA, HSPA+, CDMA2000, EV-DO, TD-SCDMA), and the Ethernet WAN - the DSL ISP such as Dynamic IP, Static IP, PPPoE, PPTP and L2TP

3.1.1.2.1 Wireless WAN – 3G/4G

Click on the “**Edit**” button for the 3G/4G WAN interface and you can get the detail WAN settings and then configure the settings as well.

The screenshot shows the 'Network Setup' page with the following configuration details:

Index	Operation Mode	Physical Interface	WAN Type	Details
WAN-1	Always-on	3G/4G	3G	<input type="button" value="Edit"/>
WAN-2	Disable	-	-	<input type="button" value="Edit"/>

WAN-1 Details

- WAN Type:** 3G
- Dial-Up Profile:** Auto-Detection Manual
- PIN Code:** (optional)
- Connection Control:** Auto Reconnect (always-on)
- Allowed Connection Time:** Always By Schedule
- MTU:** 0 (0 is auto)
- Keep Alive:**
 - Disable
 - LCP Echo Request
 - Interval: 10 seconds
 - Max. Failure Time: 3 times
 - Ping Remote Host
 - Host IP: []
 - Interval: 60 seconds
- Multicast:** Disable
- IGMP Snooping:** Enable
- Disable PPTP Passthrough:** Enable
- Disable L2TP Passthrough:** Enable
- Disable IPSec Passthrough:** Enable

Buttons: Save, Undo

1. **WAN Type:** Choose “3G” from the drop list
2. **Dial-up Profile:** Choose “Auto-Detection” or “Manual”. If you select “Auto-Detection”, then system will check the information automatically. If you select “Manual”, then you have to specify more ISP-related settings, such as Country, Service Provider, and APN, to get the 3G/4G service. The “Auto-Detection” option is suggested.

WAN-1 Details	
▶ WAN Type	3G
▶ Dial-Up Profile	<input type="radio"/> Auto-Detection <input checked="" type="radio"/> Manual
▶ Country	Albania
▶ Service Provider	Vodafone
▶ APN	(optional)
▶ PIN Code	(optional)
▶ Dialed Number	
▶ Account	(optional)
▶ Password	(optional)
▶ Authentication	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP
▶ Primary DNS	(optional)
▶ Secondary DNS	(optional)
▶ Connection Control	Auto Reconnect (always-on)
▶ Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule
▶ MTU	0 (0 is auto)
▶ Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> LCP Echo Request ▶ Interval 10 seconds ▶ Max. Failure Time 3 times <input type="radio"/> Ping Remote Host ▶ Host IP ▶ Interval 60 seconds

3. **PIN Code:** Enter the PIN Code for your SIM card(Optional)
4. **Dialed Number:** Enter the dialed number that is provided by your ISP.
5. **Account, Password:** Enter the account / Password that is provided by your ISP(Optional).
6. **Authentication:** Choose “auto”, “PAP”, or “CHAP” according your ISP’s authentication approach.
7. **Primary / Secondary DNS:** Enter the Domain Name Server settings (Optional)
8. **Connection Control:** Select your connection control scheme from the drop list; “auto-reconnect (always-on)” option is recommended.
9. **Allowed Connection Time:** You can select “Always” or “By Schedule” for connection method. If you choose “By Schedule” rule, you have to add a new schedule for this connection.
10. **MTU:** Most ISP offers MTU value to users. The default value is 0 (auto).
11. **Keep Alive:** You can do preferred settings by using this feature to prevent the built-in 3G modem from some sort of auto-timeout and disconnects from

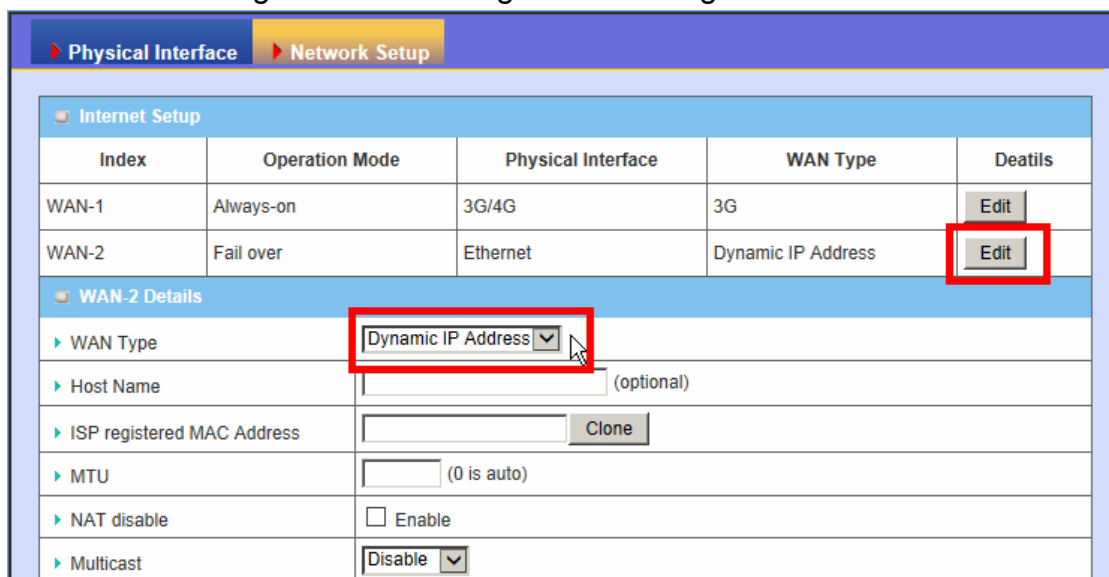
the internet after a period of inactivity.

12. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
13. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
14. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.1.2.2 Ethernet WAN

Click on the “Edit” button for the Ethernet WAN interface and you can get the detail WAN settings and then configure the settings as well.



The screenshot displays the WAN configuration interface. At the top, there are tabs for 'Physical Interface' and 'Network Setup'. Below this is the 'Internet Setup' section, which contains a table with the following data:

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	3G/4G	3G	Edit
WAN-2	Fail over	Ethernet	Dynamic IP Address	Edit

Below the table is the 'WAN-2 Details' section, which includes the following settings:

- WAN Type: Dynamic IP Address (highlighted with a red box)
- Host Name: [] (optional)
- ISP registered MAC Address: [] Clone
- MTU: [] (0 is auto)
- NAT disable: Enable
- Multicast: Disable (highlighted with a red box)

3.1.1.2.2.1 Dynamic IP Address

The screenshot shows the 'Network Setup' page with the 'Internet Setup' section expanded. A table lists WAN configurations:

Index	Operation Mode	Physical Interface	WAN Type	Details
WAN-1	Always-on	3G/4G	3G	<input type="button" value="Edit"/>
WAN-2	Fail over	Ethernet	Dynamic IP Address	<input type="button" value="Edit"/>

Below the table, the 'WAN-2 Details' section is expanded. The 'WAN Type' dropdown menu is set to 'Dynamic IP Address'. Other fields include 'Host Name' (optional), 'ISP registered MAC Address' (with a 'Clone' button), 'MTU' (0 is auto), 'NAT disable' (checkbox), 'Multicast' (dropdown set to 'Disable'), 'IGMP Snooping' (checkbox), 'Disable PPTP Passthrough' (checkbox), 'Disable L2TP Passthrough' (checkbox), 'Disable IPSec Passthrough' (checkbox), and 'WAN IP Alias' (10.0.0.1, checkbox). 'Save' and 'Undo' buttons are at the bottom.

1. **WAN Type:** choose “Dynamic IP Address” from the drop list
2. **Host Name:** Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address:** Enter the WAN MAC address of this device. (Optional)
4. **MTU:** Most ISP offers MTU value to users. The default value is 0 (auto)
5. **NAT disable:** If you enable this option, it will act with a non-NAT function.
6. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
7. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
8. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.1.2.2.2 Static IP Address

Select this option to give your static IP information. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

The screenshot shows the 'Network Setup' page with 'Internet Setup' expanded. A table lists WAN configurations:

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	3G/4G	3G	Edit
WAN-2	Fail over	Ethernet	Dynamic IP Address	Edit

Below the table, the 'WAN-2 Details' section is expanded. The 'WAN Type' dropdown menu is highlighted with a red box and shows 'Static IP Address' selected. Other fields include:

- WAN IP Address:
- WAN Subnet Mask:
- WAN Gateway:
- Primary DNS:
- Secondary DNS:
- MTU: (0 is auto)
- NAT disable: Enable
- Multicast: (dropdown)
- IGMP Snooping: Enable
- Disable PPTP Passthrough: Enable
- Disable L2TP Passthrough: Enable
- Disable IPSec Passthrough: Enable
- WAN IP Alias: Enable

At the bottom of the form are 'Save' and 'Undo' buttons.

1. **WAN Type:** Choose “Static IP Address” from the drop list
2. **WAN IP address/ Subnet Mask/ Gateway:** Enter the IP address, subnet mask, and gateway address, provided to you by your ISP.
3. **Primary DNS/ Secondary DNS:** input the Primary/Secondary DNS if necessary.
4. **MTU:** Most ISP offers MTU value to users. The default value is o (auto)
5. **NAT disable:** If you enable this option, it will act with a non-NAT function.
6. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
7. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable

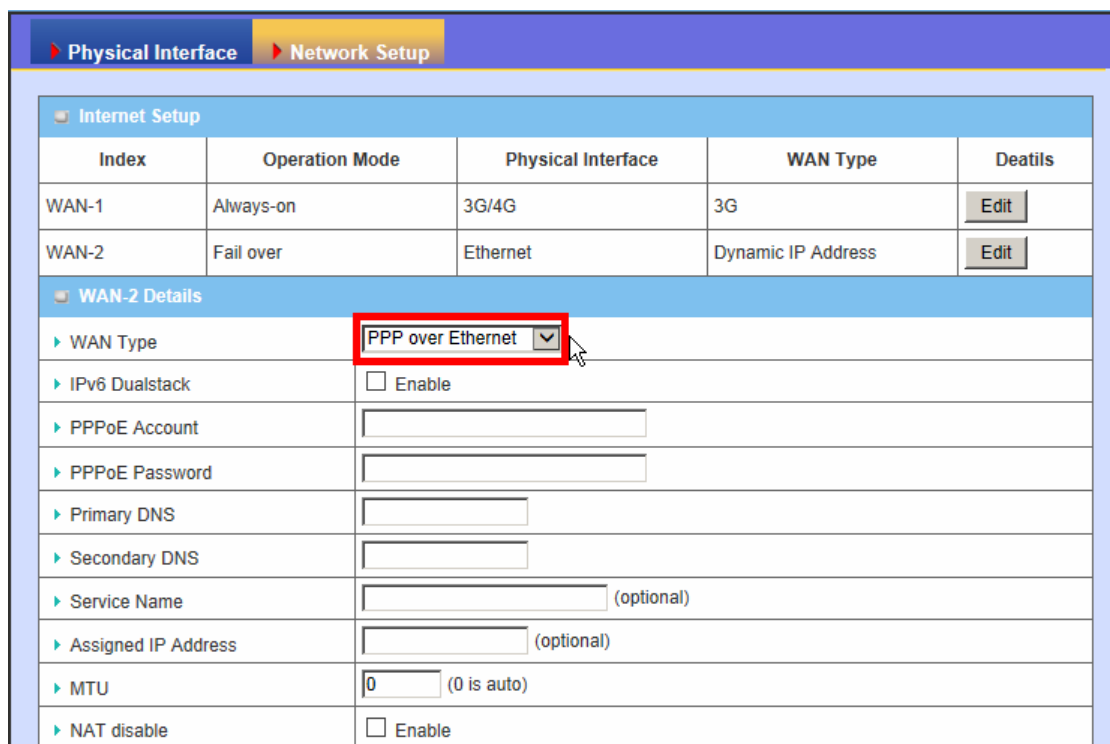
the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.

8. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
9. **WAN IP alias:** The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.1.2.2.3 PPP over Ethernet

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services.



The screenshot shows the 'Network Setup' configuration page. Under 'Internet Setup', there is a table with columns: Index, Operation Mode, Physical Interface, WAN Type, and Details. Two WAN entries are listed: WAN-1 (Always-on, 3G/4G, 3G) and WAN-2 (Fail over, Ethernet, Dynamic IP Address). Below the table, the 'WAN-2 Details' section is expanded. The 'WAN Type' dropdown menu is highlighted with a red box and shows 'PPP over Ethernet' selected. Other fields include IPv6 Dualstack (checkbox), PPPoE Account and Password (text boxes), Primary and Secondary DNS (text boxes), Service Name (text box, optional), Assigned IP Address (text box, optional), MTU (text box, 0 is auto), and NAT disable (checkbox).

Index	Operation Mode	Physical Interface	WAN Type	Details
WAN-1	Always-on	3G/4G	3G	Edit
WAN-2	Fail over	Ethernet	Dynamic IP Address	Edit

WAN-2 Details

- WAN Type: **PPP over Ethernet** (selected)
- IPv6 Dualstack: Enable
- PPPoE Account:
- PPPoE Password:
- Primary DNS:
- Secondary DNS:
- Service Name: (optional)
- Assigned IP Address: (optional)
- MTU: (0 is auto)
- NAT disable: Enable

▶ Multicast	<input type="text" value="Disable"/> ▾
▶ IGMP Snooping	<input type="checkbox"/> Enable
▶ Disable PPTP Passthrough	<input type="checkbox"/> Enable
▶ Disable L2TP Passthrough	<input type="checkbox"/> Enable
▶ Disable IPSec Passthrough	<input type="checkbox"/> Enable
▶ WAN IP Alias	<input type="text" value="10.0.0.1"/> <input type="checkbox"/> Enable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

1. **WAN Type:** Choose “PPP Over Ethernet” from the drop list
 2. **IPv6 Dualstack:** You can enable / disable the function of IPv4/IPv6 dual stack.
 3. **PPPoE Account and Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
 4. **Primary DNS / Secondary DNS:** Input the Primary/Secondary DNS if necessary.
 5. **Service Name / Assigned IP Address:** Input the Service Name and Assigned IP address if necessary.
 6. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
 7. **NAT disable :** If you enable this option, it will act with a non-NAT function.
 8. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
 9. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
 10. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
 11. **WAN IP alias:** The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.
- Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.1.2.2.4 PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP used a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

The screenshot shows a network configuration page with tabs for 'Physical Interface' and 'Network Setup'. Under 'Network Setup', there is an 'Internet Setup' section with a table of WAN configurations. Below this is the 'WAN-2 Details' section, which is expanded to show various settings. Two dropdown menus are highlighted with a red box: 'WAN Type' is set to 'PPTP' and 'IP Mode' is set to 'Dynamic IP Address'. Other settings include fields for Server IP Address/Name, PPTP Account, PPTP Password, Connection ID, MTU, and checkboxes for MPPE, IGMP Snooping, and various Passthrough options. A 'WAN IP Alias' field is also present with the value '10.0.0.1' and an 'Enable' checkbox. 'Save' and 'Undo' buttons are at the bottom.

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	3G/4G	3G	Edit
WAN-2	Fail over	Ethernet	Dynamic IP Address	Edit

WAN-2 Details

- WAN Type: PPTP
- IP Mode: Dynamic IP Address
- Server IP Address/Name:
- PPTP Account:
- PPTP Password:
- Connection ID: (optional)
- MTU: (0 is auto)
- MPPE:
- Multicast: Disable
- IGMP Snooping: Enable
- Disable PPTP Passthrough: Enable
- Disable L2TP Passthrough: Enable
- Disable IPSec Passthrough: Enable
- WAN IP Alias: 10.0.0.1 Enable

[Save](#) [Undo](#)

- WAN Type:** Choose “PPTP” from the drop list
- IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “My IP Address”, “My Subnet Mask”, and “Gateway IP” settings provided by your ISP.

WAN 2 Details	
▶ WAN Type	PPTP
▶ IP Mode	Static IP Address
▶ My IP Address	<input type="text"/>
▶ My Subnet Mask	<input type="text"/>
▶ Gateway IP	<input type="text"/>
▶ Server IP Address/Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ MTU	0 (0 is auto)
▶ MPPE	<input type="checkbox"/>

3. **Server IP Address / Name:** The IP address of the PPTP server and designated Gateway provided by your ISP.
4. **PPTP Account and Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
5. **Connection ID:** Optional, input the connection ID if your ISP requires it.
6. **MTU :** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
7. **MPPE (Microsoft Point-to-Point Encryption):** Enable or disable this function.
8. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
9. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
10. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
11. **WAN IP alias:** The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the

changes.

3.1.1.2.2.5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP used a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

The screenshot shows the 'Network Setup' tab in a configuration utility. Under 'Internet Setup', there is a table with columns: Index, Operation Mode, Physical Interface, WAN Type, and Details. The table lists two WAN connections: WAN-1 (Always-on, 3G/4G, 3G) and WAN-2 (Fail over, Ethernet, Dynamic IP Address). Below the table, the 'WAN-2 Details' section is expanded. The 'WAN Type' dropdown is set to 'L2TP' and the 'IP Mode' dropdown is set to 'Dynamic IP Address'. Both dropdowns are highlighted with a red box. Other fields include 'Server IP Address/Name', 'L2TP Account', 'L2TP Password', 'MTU' (set to 0), 'MPPE' (unchecked), 'Multicast' (set to Disable), and several 'Disable Passthrough' options (IGMP Snooping, PPTP, L2TP, IPsec) which are all unchecked. The 'WAN IP Alias' is set to 10.0.0.1 and is also unchecked. 'Save' and 'Undo' buttons are at the bottom.

Index	Operation Mode	Physical Interface	WAN Type	Details
WAN-1	Always-on	3G/4G	3G	Edit
WAN-2	Fail over	Ethernet	Dynamic IP Address	Edit

WAN-2 Details

- WAN Type: L2TP
- IP Mode: Dynamic IP Address
- Server IP Address/Name:
- L2TP Account:
- L2TP Password:
- MTU: (0 is auto)
- MPPE:
- Multicast: Disable
- IGMP Snooping: Enable
- Disable PPTP Passthrough: Enable
- Disable L2TP Passthrough: Enable
- Disable IPsec Passthrough: Enable
- WAN IP Alias: Enable

[Save](#) [Undo](#)

1. **WAN Type:** Choose “L2TP” from the drop list
2. **IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “IP Address”, “Subnet Mask”, and “WAN Gateway IP” settings provided by your ISP.

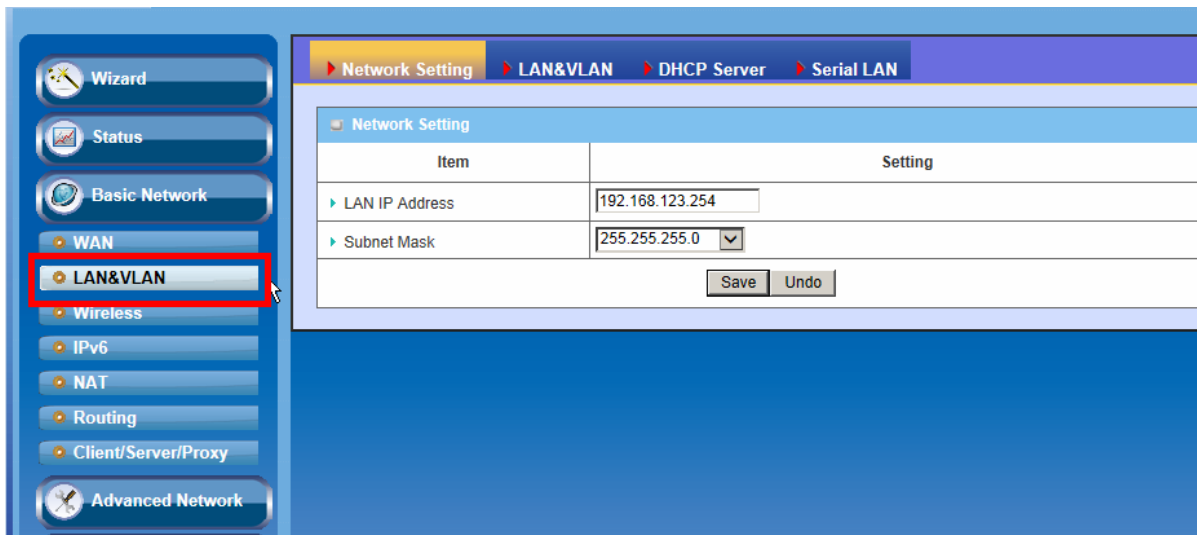
WAN-2 Details	
▶ WAN Type	L2TP
▶ IP Mode	Static IP Address
▶ IP Address	
▶ Subnet Mask	
▶ WAN Gateway IP	
▶ Server IP Address/Name	
▶ L2TP Account	
▶ L2TP Password	
▶ MTU	0 (0 is auto)
▶ MPPE	<input type="checkbox"/>

3. **Server IP Address / Name:** The IP address of the PPTP server and designated Gateway provided by your ISP.
4. **L2TP Account and Password:** The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
5. **MTU :** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
6. **MPPE (Microsoft Point-to-Point Encryption):** Enable or disable this function.
7. **Multicast:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
8. **IGMP Snooping:** Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
9. **Disable PPTP / L2TP / IPSec Passthrough:** By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
10. **WAN IP alias:** The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

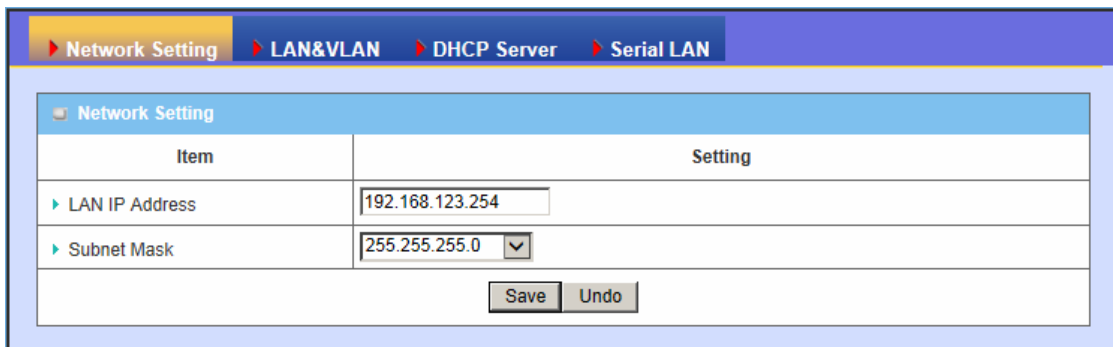
3.1.2 LAN & VLAN Setup

This device is equipped with four fast Ethernet LAN ports as to connect your local devices via Ethernet cables. Besides, VLAN function is provided to organize your local networks.



3.1.2.1 Network Setting

Please follow the following instructions to do IPv4 Network Setup.



- LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.
- Subnet Mask:** Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.2.2 LAN & VLAN

This section provides a brief description of VLANs and explains how to create, and modify virtual LANs which are more commonly known as VLANs. A VLAN is a group of ports that form a logical network under a certain switch or router device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN.

The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly.

This Device supports port-based VLAN and tag-based VLAN. You can select either one operation mode and then configure according to your network configuration.

3.1.2.2.1 Port-Based VLAN

A port-based VLAN is a group of ports on a Ethernet switch or router that form a logical Ethernet segment. There are four LAN ports and up to eight virtual APs in this device, so you can have various VLAN configurations to organization the available LAN ports and virtual APs if required.

Please Select the Operations: Port-Based VLAN

LAN VLAN Settings [HELP]						
Ethernet	Type	LAN VID	Tx TAG	DHCP Server	WAN maps VID	Edit
Port1	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
Port3	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
Port4	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
Virtual AP	Type	VID	Tx TAG	DHCP Server	WAN maps VID	Edit
VAP1	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP2	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP3	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP4	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP5	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP6	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP7	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit
VAP8	NAT	1	X	DHCP1/Enable 192.168.123.0/24	0	Edit

By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN is a NAT type network, all the local device IP addresses are allocated by DHCP

server 1. If you want to divide them into different VLANs, click on the “Edit” button related to each port.

1. **Type:** Select “NAT” or “Bridge” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
2. **LAN VID:** Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN.
3. **Tx TAG:** If ISP requests a “**VLAN Tag**” with your outgoing data, please check the checkbox of “Tx TAG”.
4. **DHCP Server:** Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
5. **WAN Maps VID:** The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed, and the value is forced to “0”; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.

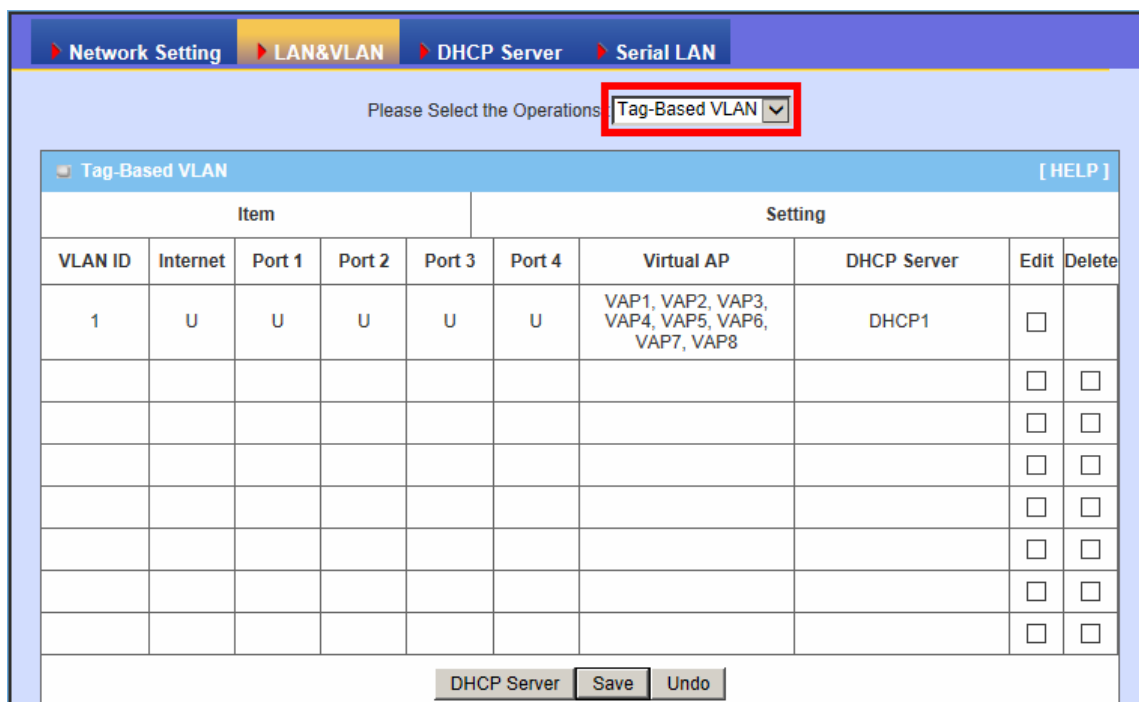
Summary				
VLAN ID on LAN	Membership	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port0, Port1, Port2, Port3, Port4, VAP-1, VAP-2, VAP-3, VAP-4, VAP-5, VAP-6, VAP-7, VAP-8	No	NAT	0

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.2.2.2 Tag-Based VLAN

The second type of VLAN is the tag-based VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the port VIDs assigned to the ports determine VLAN membership

When the device receives a frame with a VLAN tag, referred to as a tagged frame, the device forwards the frame only to those ports that share the same VID.



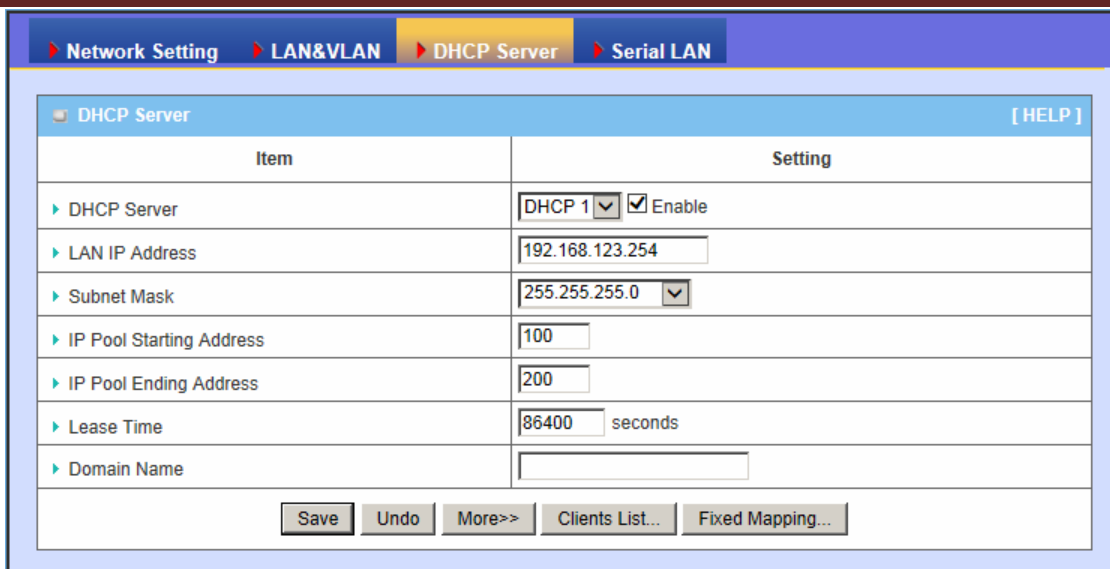
By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN ID is forced to “1”. It is a special tag based VLAN for device to operated, there is no tag required for this default VLAN ID.

If you want to configure your own tag-based VLANs, click on the “Edit” checkbox on a new VLAN ID row.

1. **VLAN ID:** Specify a VLAN tag for this VLAN group. The ports with the same VID are in the same VLAN.
2. **Internet:** Specify whether this VLAN can access Internet or not. If it is checked, all the packet will be un-tagged before it is forward to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forward to the destination belongs to this configuring VLAN group.
3. **Port 1 ~ Port 4, VAP1 ~ VAP8:** Specify whether it is belong to the VLAN group or not. You just have to check the checkbox of the selected ports.
4. **DHCP Server:** Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.2.3 DHCP Server



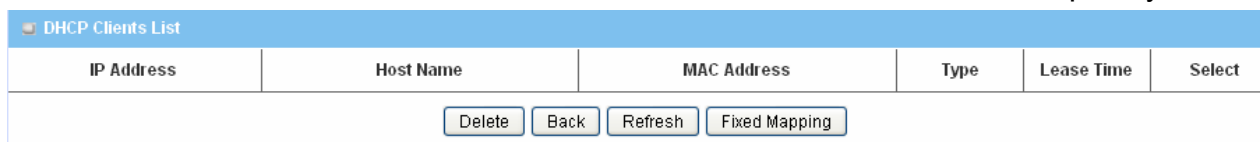
Item	Setting
DHCP Server	DHCP 1 <input checked="" type="checkbox"/> Enable
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 seconds
Domain Name	

1. **DHCP Server:** Choose DHCP Server to **Enable**. If you enable the DHCP Server function, the following settings will be effective. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
2. **IP Pool Starting/Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
3. **Lease Time:** DHCP lease time to the DHCP client.
4. **Domain Name:** Optional, this information will be passed to the clients.

Press “**More>>**” and you can find more settings.

5. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign a DNS Servers
6. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign a WINS Servers
7. **Gateway:** Optional. Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

Press “**Clients List**” and the list of DHCP clients will be shown consequently.



IP Address	Host Name	MAC Address	Type	Lease Time	Select
<input type="button" value="Delete"/> <input type="button" value="Back"/> <input type="button" value="Refresh"/> <input type="button" value="Fixed Mapping"/>					

Press “**Fixed Mapping**” and you can specify a certain IP address for designated local device (MAC address), so that the DHCP Server will reserve the special IP for designated devices.

Fixed Mapping [HELP]

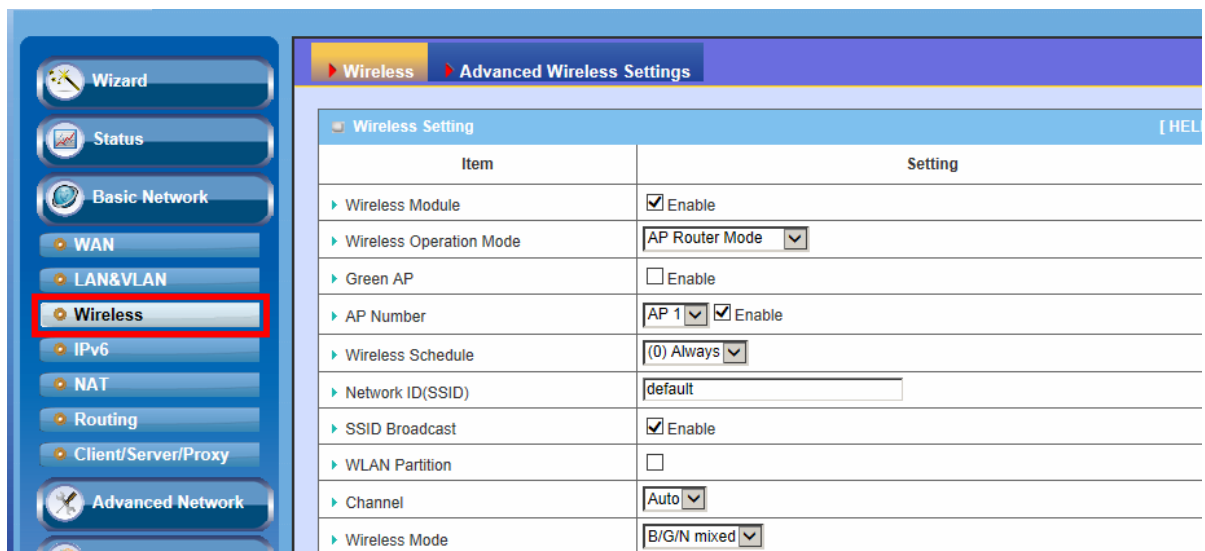
DHCP clients: Copy to ID:

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

<<Previous Next>> Save Undo Back

3.1.3 Wireless Setup

Wireless settings allow you to set the WLAN (WiFi) configuration items. When the wireless configuration is done your WiFi LAN is ready to support your local WiFi devices such as your laptop PC, wireless printer and some portable wireless devices.

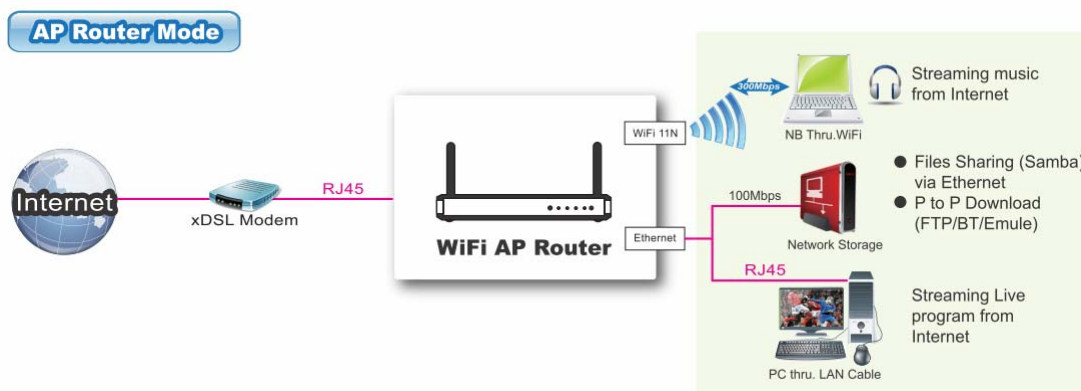


3.1.3.1 Wireless Setup

There are several wireless operation modes provided by this device. They are: “**AP Router Mode**”, “**WDS Hybrid Mode**” and “**WDS Only Mode**”. You can choose the expected mode from the list.

3.1.3.1.1 AP Router Mode

This mode allows you to get your wired and wireless devices connected with NAT.



The screenshot shows the 'Advanced Wireless Settings' page with the following configuration:

Item	Setting
Wireless Module	<input checked="" type="checkbox"/> Enable
Wireless Operation Mode	AP Router Mode
Green AP	<input type="checkbox"/> Enable
AP Number	AP 1 <input checked="" type="checkbox"/> Enable
Wireless Schedule	(0) Always
Network ID(SSID)	default
SSID Broadcast	<input checked="" type="checkbox"/> Enable
WLAN Partition	<input type="checkbox"/>
Channel	Auto
Wireless Mode	B/G/N mixed
Authentication	Auto
Encryption	None

Buttons at the bottom: Save, Undo, WPS Setup..., Wireless Client List...

1. **Wireless Module:** Enable the wireless function.
2. **Wireless Operation Mode:** Choose “**AP Router Mode**” from the list.
3. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
4. **AP Number:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.
5. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
6. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
7. **SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
8. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
9. **Channel:** The radio channel number. The permissible channels depend on the

Regulatory Domain. The factory default setting is auto channel selection.

10. **Wireless Mode:** Choose “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open (include 802.1x), Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA/WPA2.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The AP will Select the Open or Shared by the client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

- **WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA2**

Select Encryption mode and enter RADIUS Server related information. You

have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

- **WPA-PSK/WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key.

- **WPA/WPA2**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

- **802.1x**

When you select “Open” Authentication, GUI will display 802.1x. Please RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then select wep64 or wep128.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Press “**WPS Setup**”, you can configure and enable the easy setup feature WPS (Wi-Fi Protected Setup) for your wireless network.

Wi-Fi Protected Setup [HELP]	
Item	Setting
▶ WPS	<input checked="" type="checkbox"/> Enable
▶ AP PIN	00020329 <input type="button" value="Generate New PIN"/>
▶ Config Mode	<input type="text" value="Registrar"/> ▼
▶ Config Status	CONFIGURED <input type="button" value="Release"/>
▶ Disable WPS-PIN Method	<input type="checkbox"/>
▶ Config Method	<input type="text" value="Push Button"/> ▼
▶ WPS status	IDLE
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Undo"/>	

1. **WPS:** You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.

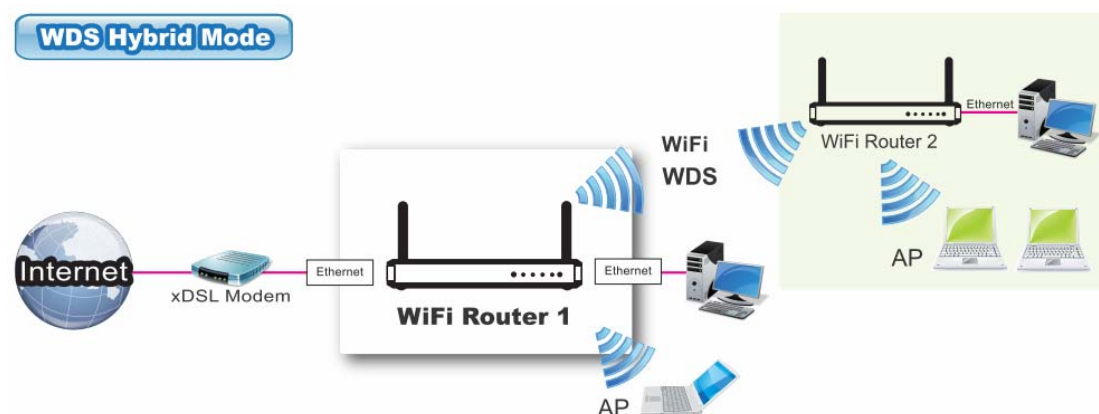
2. **AP PIN:** You can press Generate New Pin to get an AP PIN.
3. **Config Mode:** Select your configuration Mode from “Registrar” or “Enrollee”. For a AP router or AP, it should be in “Registrar” mode, so that other wireless clients in “Enrollee” mode can connect to the discovered “Registrar”.
4. **Config Status:** It shows the status of your configuration.
5. **Config Method:** You can select the Configuration Method here from “Pin Code” or “Push Button”.
6. **WPS status:** According to your setting, the status will show “Start Process” or “No used”.

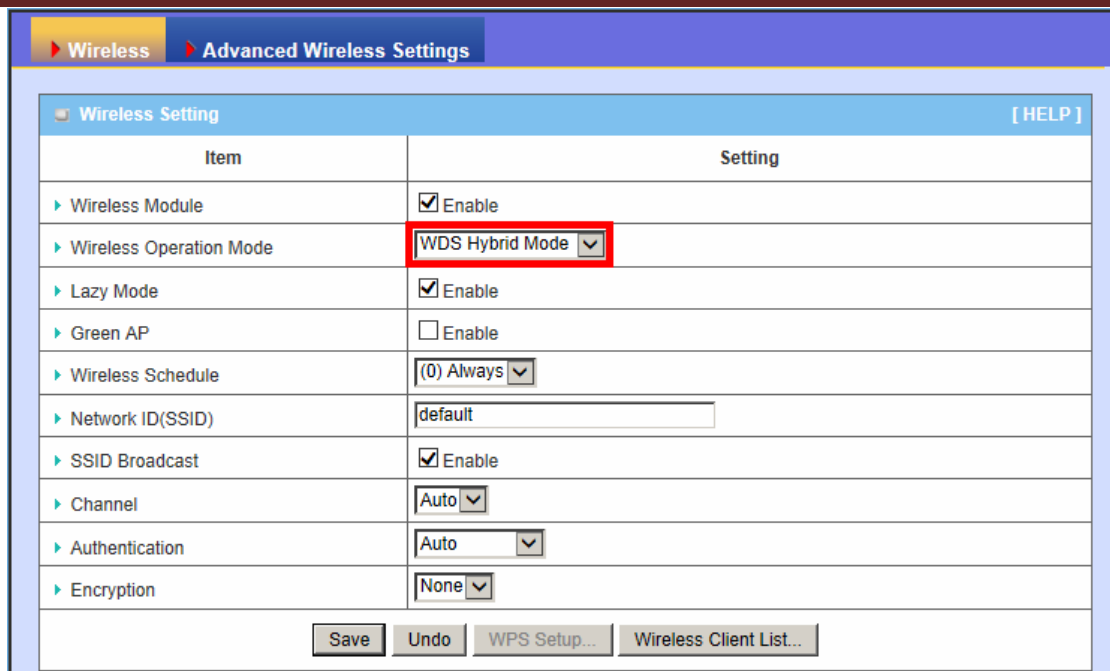
Press “**Wireless Clients List**”, and the list of connected wireless clients will be shown consequently.

2.4G Wireless Clients List [HELP]						
Please Choose One: ALL						
IP Address	Host Name	MAC Address	Mode	Rate	Signal	Interface
Back Refresh						

3.1.3.1.2 WDS Hybrid Mode

While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection



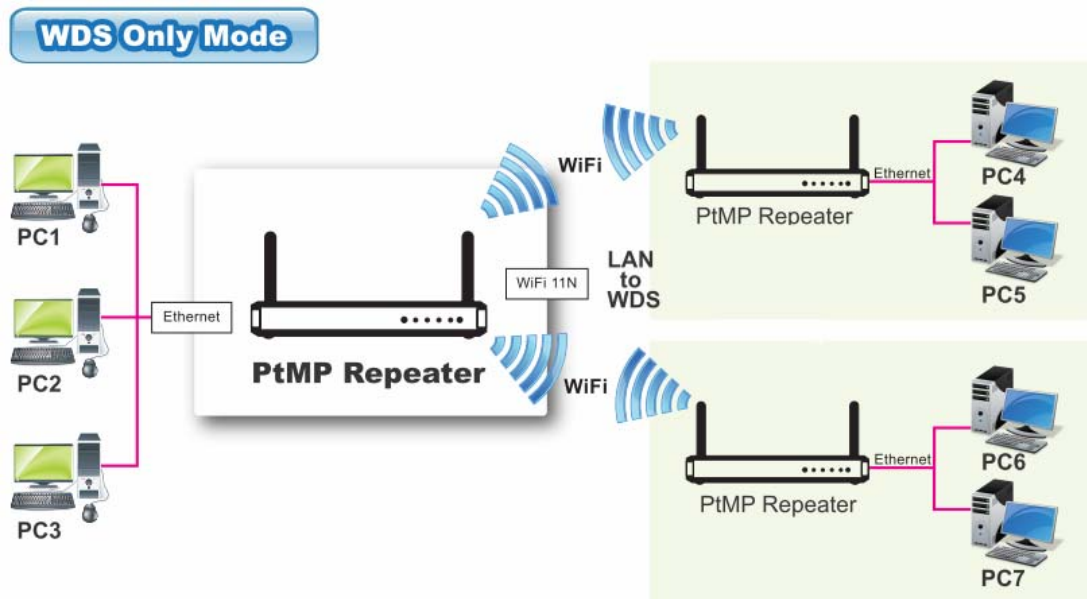


1. **Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.
2. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
3. **Wireless Schedule:** The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
4. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is "default")
5. **SSID Broadcast:** The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", the wireless clients can not find the device from beacons.
6. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
7. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
8. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

9. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one. Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.3 WDS Only Mode

WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools ...etc.



Wireless > Advanced Wireless Settings

Wireless Setting [HELP]

Item	Setting
Wireless Module	<input checked="" type="checkbox"/> Enable
Wireless Operation Mode	WDS Only Mode
Lazy Mode	<input checked="" type="checkbox"/> Enable
Green AP	<input type="checkbox"/> Enable
Channel	Auto
Authentication	Auto
Encryption	None

Save Undo

1. **Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.

2. **Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
 3. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
 4. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.
 5. **Remote AP MAC 1 ~ Remote AP MAC 4:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.
- Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.2 Advanced Wireless Setup

This device provides advanced wireless setup for professional user to optimize the wireless performance under the specific installation environment.

Item	Setting
Regulatory Domain	US (1-11)
Beacon Interval	100 (msec, range:1~1000)
Transmit Power	100%
RTS Threshold	2347 (1~2347)
Fragmentation	2346 (256~2346)
DTIM Interval	1 (range: 1~255)
WMM Capable	<input checked="" type="checkbox"/> Enable
TX Rates	Best

1. **Beacon interval:** Beacons are packets sent by a wireless router to synchronize wireless devices.
2. **Transmit Power:** Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.
3. **RTS Threshold:** If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the

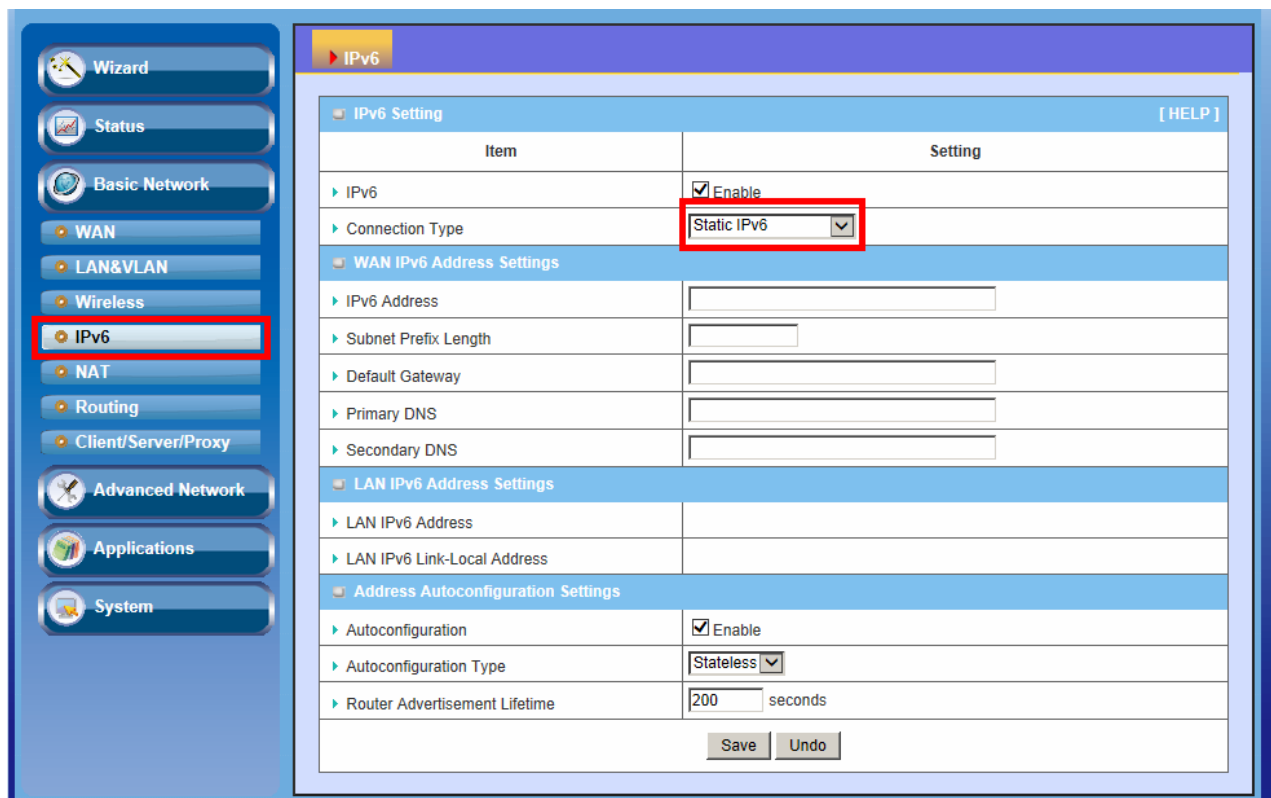
RTS/CTS (Request to Send/Clear to Send) threshold value.

4. **Fragmentation:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.
5. **DTIM interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.
6. **WMM Capable:** WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
7. **TX Rate:** Can Fix TX Rate to transmit date.

3.1.4 IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6 (Internet Protocol version 6)** is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This router supports various types of IPv6 connection (Static IPv6 / DHCPv6 / PPPoE / 6 to 4 / IPv6 in IPv4 tunnel). **Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.**

3.1.4.1 Static IPv6



When “Static IPv6” is selected you need to do the following settings:

1. WAN IPv6 address settings:

- A. **IPv6 address:** Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is

“2001:0db8:85a3:0000:0000:8a2e:0370:7334”

- B. **Subnet Prefix Length:** Enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.
 - C. **Default Gateway:** Enter the Default Gateway address here; A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table.
 - D. **Primary / Secondary DNS:** You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
3. **Address auto configuration settings:**
- A. **Auto-configuration:** Disable or enable this auto configuration setting.
 - B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
 - C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.2 DHCP v6

The screenshot shows the IPv6 configuration interface. The 'Connection Type' dropdown menu is highlighted with a red box and set to 'DHCPv6'. Other settings include 'IPv6' (checked), 'IPv6 DNS Settings' (radio buttons for automatic or manual), 'LAN IPv6 Address Settings' (empty fields), and 'Address Autoconfiguration Settings' (checked, Stateless, 200 seconds).

Item	Setting
IPv6	<input checked="" type="checkbox"/> Enable
Connection Type	DHCPv6
IPv6 DNS Settings	
DNS Setting	<input checked="" type="radio"/> Obtain DNS Server address Automatically <input type="radio"/> Use the following DNS address
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
LAN IPv6 Address Settings	
LAN IPv6 Address	<input type="text"/>
LAN IPv6 Link-Local Address	<input type="text"/>
Address Autoconfiguration Settings	
Autoconfiguration	<input checked="" type="checkbox"/> Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 seconds

When “DHCP v6” is selected you need to do the following settings:

1. **IPv6 DNS (WAN IPv6 address) settings:** You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
3. **Address auto configuration settings:**
 - A. **Auto-configuration:** Disable or enable this auto configuration setting.
 - B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
 - C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then

must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.3 PPPoE

The screenshot shows a web-based configuration interface for IPv6 settings. The main heading is "IPv6 Setting" with a "[HELP]" link. The interface is organized into several sections:

- IPv6 Setting:** A table with two columns: "Item" and "Setting".
 - Item: IPv6, Setting: Enable
 - Item: Connection Type, Setting: PPPoE (highlighted with a red box)
- PPPoE Settings:** A section with several input fields:
 - Account: []
 - Password: []
 - Service Name: []
 - Reconnect Mode: Auto Reconnect (always-on)
 - MTU: []
- LAN IPv6 Address Settings:** A section with two input fields:
 - LAN IPv6 Address: []
 - LAN IPv6 Link-Local Address: []
- Address Autoconfiguration Settings:** A section with three settings:
 - Autoconfiguration: Enable
 - Autoconfiguration Type: Stateless (dropdown)
 - Router Advertisement Lifetime: 200 seconds

At the bottom of the form, there are "Save" and "Undo" buttons.

When “PPPoE” is selected you need to do the following settings:

- WAN IPv6 address settings:**
 - Username:** enter the Username that you got from your ISP
 - Password:** enter the Password that you got from your ISP
 - Service Name:** enter the Service Name that you got from your ISP
 - Reconnection Mode:** leave the setting as “AutoReconnect (always-on)”
 - Max. Idle Time:** give max. idle time that you want here
 - MTU (Maximum Transmission Unit):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
- LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.
- Address auto configuration settings:**

- A. **Auto-configuration:** Disable or enable this auto configuration setting.
- B. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
- C. **Router advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.4 6 to 4

The screenshot shows the IPv6 configuration interface. The 'Connection Type' dropdown menu is highlighted with a red box and set to '6 to 4'. Below it, the '6 to 4 Settings' section is visible, including fields for '6 to 4 Address', 'Primary DNS', and 'Secondary DNS'. The 'LAN IPv6 Address Settings' section includes fields for 'LAN IPv6 Address' and 'LAN IPv6 Link-Local Address'. The 'Address Autoconfiguration Settings' section includes checkboxes for 'Autoconfiguration' (checked), a dropdown for 'Autoconfiguration Type' (set to 'Stateless'), and a text input for 'Router Advertisement Lifetime' (set to '200 seconds'). 'Save' and 'Undo' buttons are at the bottom.

Item	Setting
IPv6	<input checked="" type="checkbox"/> Enable
Connection Type	6 to 4
6 to 4 Settings	
6 to 4 Address	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
LAN IPv6 Address Settings	
LAN IPv6 Address	
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	<input checked="" type="checkbox"/> Enable
Autoconfiguration Type	Stateless
Router Advertisement Lifetime	200 seconds

When “6 to 4 IPv6” is selected you need to do the following settings:

1. **6 to 4 Settings:** You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address settings:** Enter “LAN IPv6 address” and “LAN IPv6

Link-Local address”.

3. **Address auto configuration settings:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

3.1.4.5 IPv6 in IPv4 Tunnel

The screenshot shows a configuration window for IPv6. At the top, there is a blue header with 'IPv6' and a [HELP] link. Below this is a table with two columns: 'Item' and 'Setting'. The table is organized into several sections:

- IPv6 Setting:** Contains 'IPv6' (checked 'Enable') and 'Connection Type' (set to 'IPv6 in IPv4 Tunnel', which is highlighted with a red box).
- IPv6 in IPv4 Tunnel Settings:** Contains 'Remote IPv4 Address', 'Local IPv4 Address', 'Local IPv6 Address' (with a '/64' suffix), 'Primary DNS', and 'Secondary DNS', each with an input field.
- LAN IPv6 Address Settings:** Contains 'LAN IPv6 Address' and 'LAN IPv6 Link-Local Address', each with an input field.
- Address Autoconfiguration Settings:** Contains 'Autoconfiguration' (checked 'Enable'), 'Autoconfiguration Type' (set to 'Stateless'), and 'Router Advertisement Lifetime' (set to '200 seconds').

At the bottom of the table, there are 'Save' and 'Undo' buttons.

When “IPv6 in IPv4 Tunnel” is selected you need to do the following settings:

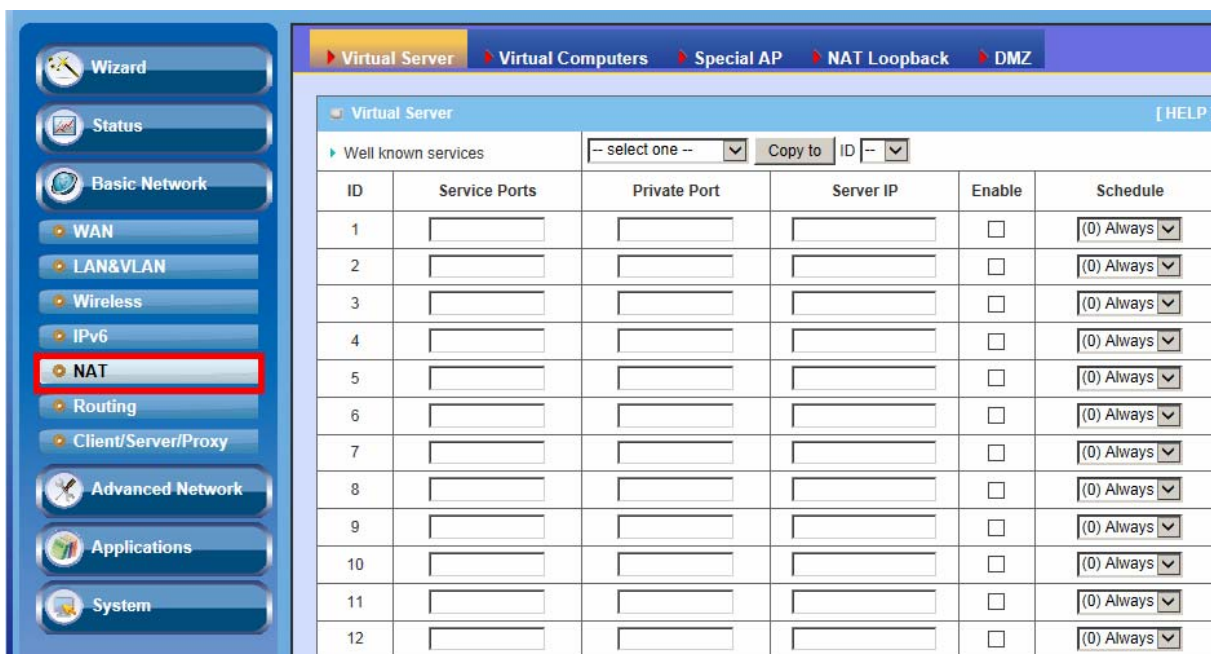
1. **IPv6 in IPv4 Tunnel Settings:** you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address.
3. **Address auto configuration setting:** Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

3.1.5 NAT Setup

3.1.5.1 Virtual Server

This device's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **Scheduling Rule**.



For example, if you have an **FTP server (Service port 21)** at **192.168.123.1**, a **Web server1 (Service port 80)** at **192.168.123.2**, a **Web server2 (Service Port 8080 and Private port 80)** at **192.168.123.3**, and a **VPN server** at **192.168.123.6**, then you need to specify the following virtual server mapping table

Service Port	Private Port	Server IP	Enable
21		192.168.123.1	V
80		192.168.123.2	V
8080	80	192.168.123.3	v
1723		192.168.123.6	V

Afterwards, click on **“Save”** to store your settings or click **“Undo”** to give up the changes.

3.1.5.2 Virtual Computers

Virtual Computers [HELP]			
ID	Global IP	Local IP	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

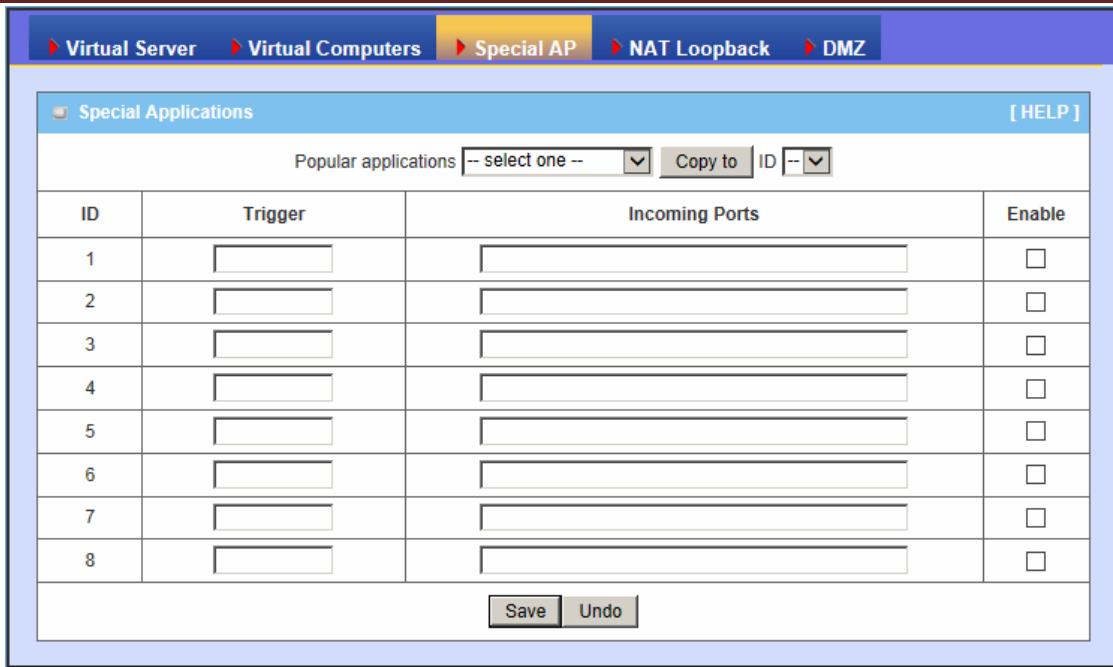
Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

1. **Global IP:** Enter the global IP address assigned by your ISP.
2. **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
3. **Enable:** Check this item to enable the Virtual Computer feature.

Virtual Computers [HELP]			
ID	Global IP	Local IP	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

3.1.5.3 Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

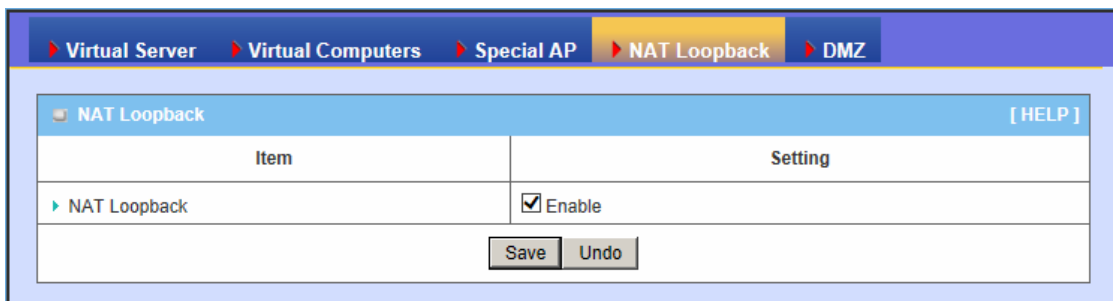


This device provides some predefined settings. Select your application and click “Copy to” to add the predefined setting to your list.

1. **Trigger:** The outbound port number issued by the application.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Enable:** Check this item to enable the Special AP feature.

Afterwards, Click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.5.4 NAT Loopback



Allow you to access the external IP address from inside your home or office network. This is useful when you run a server inside your network.

3.1.5.5 DMZ

DMZ Settings [HELP]		
Item	Setting	Enable
▶ IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>

Save Undo

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

3.1.6 Routing Setup

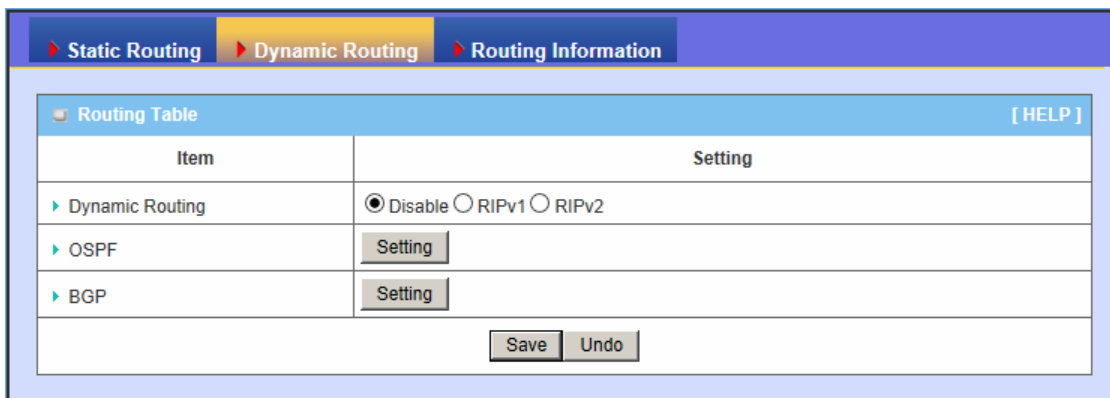
If you have more than one routers and subnets, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other.

3.1.6.1 Static Routing

Item		Setting			
▶ Static Routing		<input type="checkbox"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

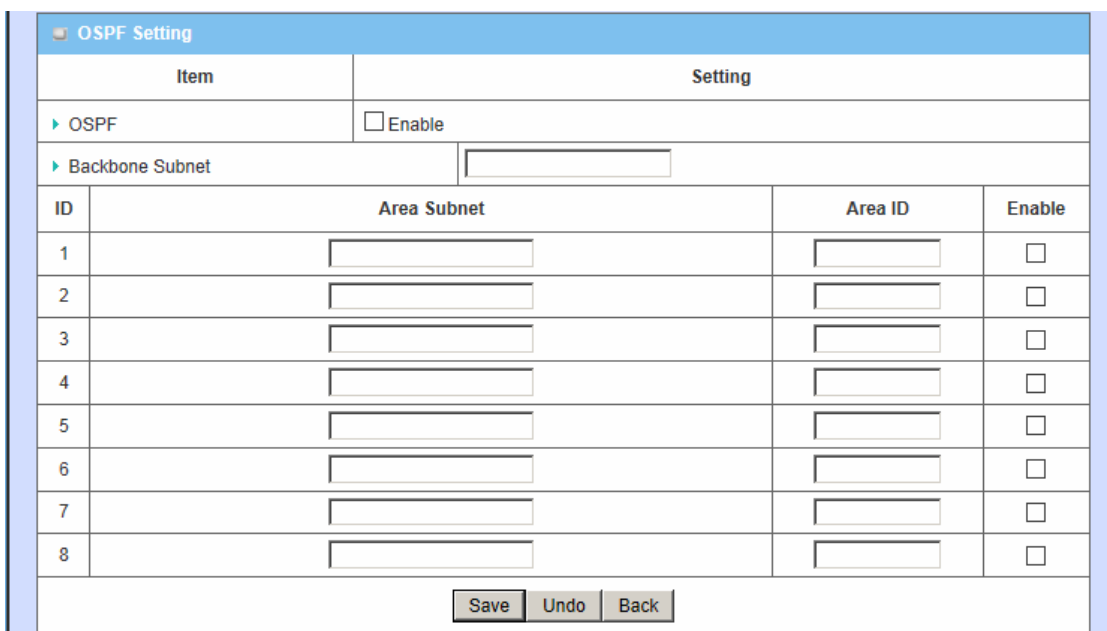
3.1.6.2 Dynamic Routing



1. **Dynamic Routing:** Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

When you finished setting, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

2. **OSPF:** OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.



You can enable the OSPF routing function by click on the “Setting” button and fill in the corresponding setting for your OSPF routing configuration. When you finished setting, click on “**Save**” to store your settings or click “**Undo**” to give up

the changes.

3. **BGP:** Border Gateway Protocol (BGP) is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule-sets. For this reason, it is more appropriately termed a reach-ability protocol rather than routing protocol.

Item		Setting	
▶ BGP		<input type="checkbox"/> Enable	
▶ Self ID		<input type="text"/>	
ID	Neighbor IP	Neighbor ID	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

You can enable the BGP routing function by click on the “Setting” button and fill in the corresponding setting for your BGP routing configuration. When you finished setting, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.1.6.3 Routing Information

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.123.0	0.0.0.0	255.255.255.0	0	LAN
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN
127.0.0.0	0.0.0.0	255.0.0.0	0	lo

A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table

contains information about the topology of the network immediately around it.

This page displays the routing table maintained by this device. It is generated according to your network configuration.

3.1.7 Client/Server/Proxy

3.1.7.1 Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

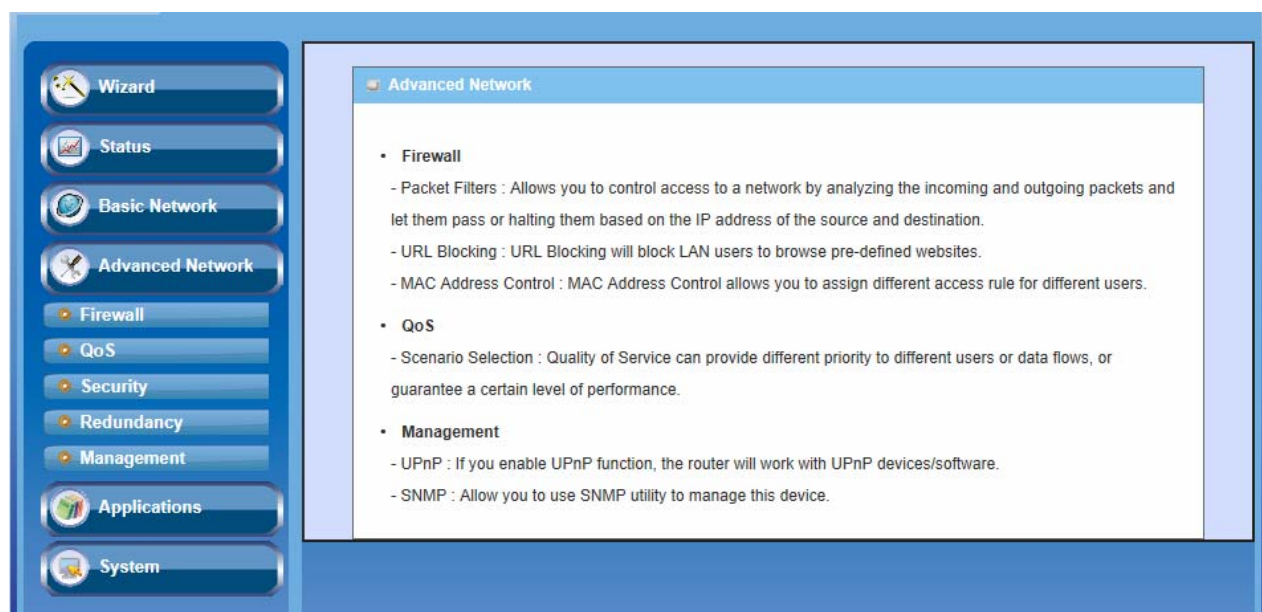
Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.

Item	Setting
▶ DDNS	<input type="checkbox"/> Enable
▶ Provider	DynDNS.org(Dynamic)
▶ Host Name	
▶ Username / E-mail	
▶ Password / Key	

1. **DDNS:** Select enable if you would like to trigger this function.
 2. **Provider:** The DDNS provider supports service for you to bind your IP(even private IP) with a certain Domain name. You could choose your favorite provider.
 3. **Host Name:** Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname(you specify) and a suffix(DDNS provider specifies).
 4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you select.
 5. **Password/Key:** Input password or key based on the DDNS provider you select.
- Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2 Advanced Network

This router also supports many advanced network features, such as Firewall, QoS, Security, Redundancy, and Management. You can finish those configurations in this section.



3.2.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filter, L7 Application Filter, IPS, MAC Address Control and Others.

3.2.1.1 Packet Filters

Packet Filters include both outbound filter and inbound filter. And they have the same way to setting. It enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to virtual servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules.
2. Deny all to pass except those match the specified rules.

[Packet Filters](#) > [URL Blocking](#) > [Web Content Filter](#) > [L7 Application Filter](#) > [IPS](#) > [MAC Address Control](#) > [Others](#)

Packet Filters [HELP]

Item	Setting				
▶ Packet filter	<input type="checkbox"/> Enable				
▶ Well known services	-- select one -- <input type="button" value="Copy to"/> ID --				
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.					
ID	Source IP	Destination IP : Ports	Protocol	Enable	Schedule
1	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
2	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
3	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
4	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
5	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
6	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
7	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
8	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
9	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
10	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
11	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always
12	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/> : <input type="text"/> - <input type="text"/>	TCP	<input type="checkbox"/>	(0) Always

You can specify rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address or range
- Destination IP address or range
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule Schedule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). An empty implies all IP addresses.

For destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules**, and give user more flexibility on Access control. For more details, please refer to the **Scheduling Rule** section.

Each rule can be enabled or disabled individually.

Afterwards, click on **“Save”** to store your settings or click **“Undo”** to give up the changes.

3.2.1.2 URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can both filter domain input suffix (like .com or .org, etc) and a keyword “bct” or “mpe”.

URL Blocking [HELP]			
Item	Setting		
▶ URL Blocking	<input checked="" type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.			
ID	URL	Enable	Schedule
1	sex, boy	<input checked="" type="checkbox"/>	(0) Always ▼
2	www.ccc.com, abc	<input checked="" type="checkbox"/>	(0) Always ▼
3		<input type="checkbox"/>	(0) Always ▼
4		<input type="checkbox"/>	(0) Always ▼
5		<input type="checkbox"/>	(0) Always ▼
6		<input type="checkbox"/>	(0) Always ▼
7		<input type="checkbox"/>	(0) Always ▼
8		<input type="checkbox"/>	(0) Always ▼
9		<input type="checkbox"/>	(0) Always ▼
10		<input type="checkbox"/>	(0) Always ▼

1. **URL Blocking:** Check if you want to enable URL Blocking.
2. **URL:** If any part of the Website's URL matches the pre-defined word, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by ",", e.g., “abc, bt, org”; In addition to URL keywords, it can also block the designated domain name, like “www.xxx.com”, “www.123aaa.org, mma.com”.
3. **Enable:** Check to enable each rule.
4. **Schedule:** The rule can be turn off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.3 Web Content Filter

Web Content filter can block files with the specific extension, like ".exe", ".bat" (applications), "mpeg" (video), and Scripts Type, like Java Applet, Java Scripts, cookies, Active X.

[Packet Filters](#) > [URL Blocking](#) > [Web Content Filter](#) > [L7 Application Filter](#) > [IPS](#) > [MAC Address Control](#) > [Others](#)

Web Content Filter [HELP]

Item	Setting
▶ Web Content	<input checked="" type="checkbox"/> Enable
▶ Popular web content	<input checked="" type="checkbox"/> Cookie <input checked="" type="checkbox"/> Java <input checked="" type="checkbox"/> ActiveX

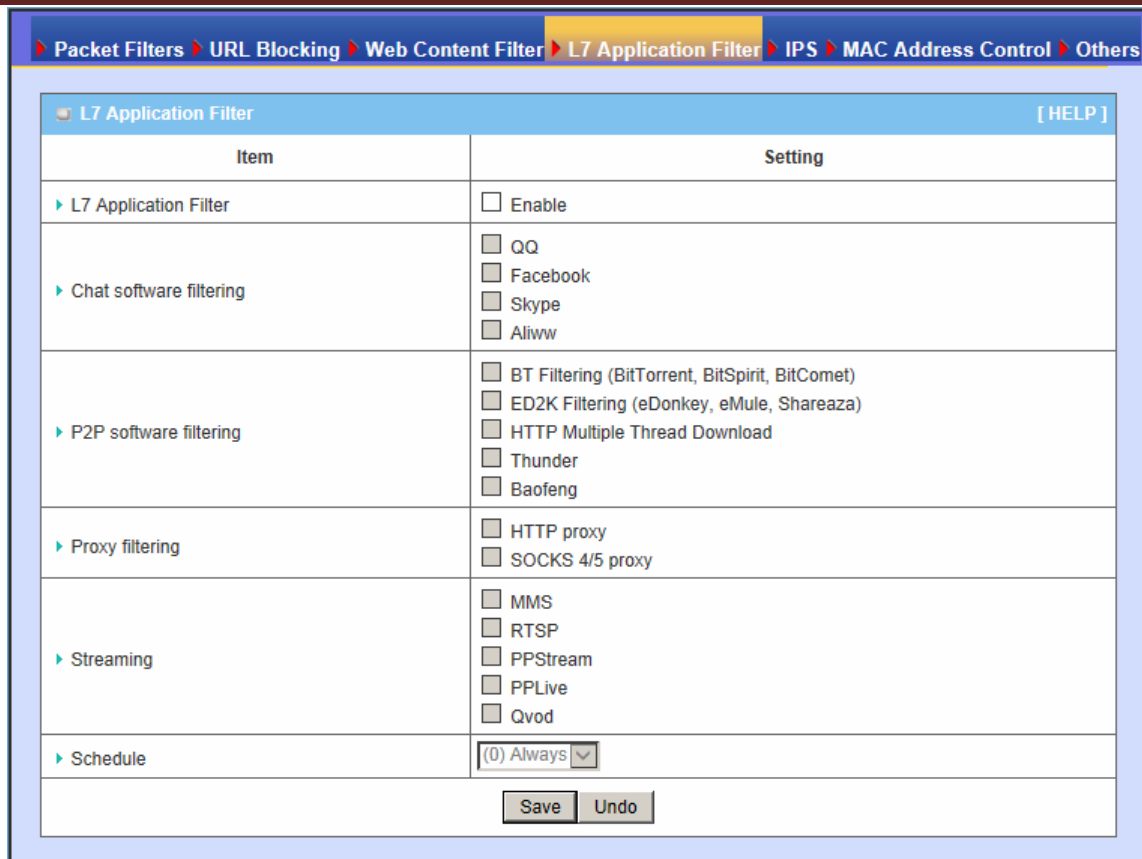
ID	File Extension List	Enable	Schedule
1	<input type="text" value="exe, bat, com"/>	<input checked="" type="checkbox"/>	(0) Always ▼
2	<input type="text" value="avi, asf, wmv, flv"/>	<input checked="" type="checkbox"/>	(0) Always ▼
3	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
4	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
5	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
6	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
7	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
8	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
9	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼
10	<input type="text"/>	<input type="checkbox"/>	(0) Always ▼

1. **File Extension List:** You can enter up to 10 file extensions in a rule to be blocked.
2. **Enable:** Check to enable each rule.
3. **Schedule:** The rule can be turn off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.4 L7 Application Filter

L7 Application Filter can categorize Internet Protocol packets based on their application layer data.



This device supports the L7 application filter for various Internet Chat, P2P download, Proxy, and streaming Video. You can select the applications to be blocked after the function is enabled, and specify the schedule rule for such application filter.

3.2.1.5 IPS

IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

[Packet Filters](#) > [URL Blocking](#) > [Web Content Filter](#) > [L7 Application Filter](#) > **IPS** > [MAC Address Control](#) > [Others](#)

☐ Dos Defense [HELP]

Item	Setting
▶ Dos Defense	<input type="checkbox"/> Enable
▶ SYN Flooding	<input type="checkbox"/> Enable <input type="text" value="300"/> Packet/Sec
▶ UDP Flooding	<input type="checkbox"/> Enable <input type="text" value="300"/> Packet/Sec
▶ ICMP Flooding	<input type="checkbox"/> Enable <input type="text" value="300"/> Packet/Sec
▶ Port Scan	<input type="checkbox"/> Enable <input type="text" value="300"/> Packet/Sec
▶ Block IP spoof	<input type="checkbox"/> Enable
▶ Block TCP Flag scan	<input type="checkbox"/> Enable
▶ Land Attack	<input type="checkbox"/> Enable
▶ Block Tear Drop	<input type="checkbox"/> Enable
▶ Block Smurf	<input type="checkbox"/> Enable
▶ Block Ping of Death	<input type="checkbox"/> Enable
▶ Block trace route	<input type="checkbox"/> Enable
▶ Block ICMP fragment	<input type="checkbox"/> Enable
▶ Block SYN fragment	<input type="checkbox"/> Enable
▶ Block Fraggle Attack	<input type="checkbox"/> Enable

You can enable the DoS Defense function and check the listed intrusion activities if necessary.

3.2.1.6 MAC Address Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

[Packet Filters](#)
[URL Blocking](#)
[Web Content Filter](#)
[L7 Application Filter](#)
[IPS](#)
[MAC Address Control](#)
[Others](#)

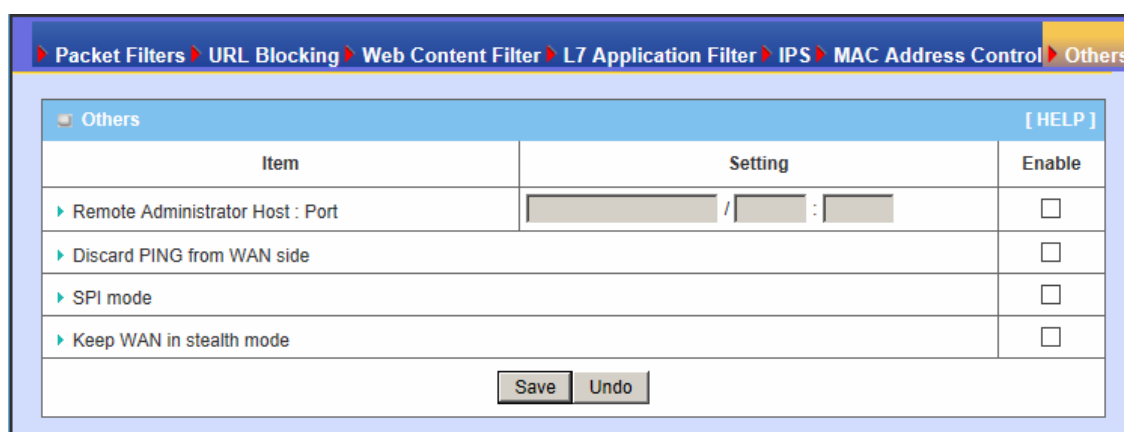
MAC Address Control [HELP]

Item	Setting		
MAC Address Control	<input type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with C checked can connect to this device; and <input type="text" value="allow"/> unspecified MAC addresses to connect.		
DHCP clients <input type="text" value="-- select one --"/> <input type="button" value="Copy to"/> ID <input type="text" value="--"/>			
ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

1. **MAC Address Control:** Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.
2. **Connection control:** Check "Connection control" to enable the control of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet consequently. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to connect to this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.7 Others



1. **Remote Administrator Host/Port:** In general, only local clients (LAN users) can browse the device's built-in web pages for device administration setting. This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

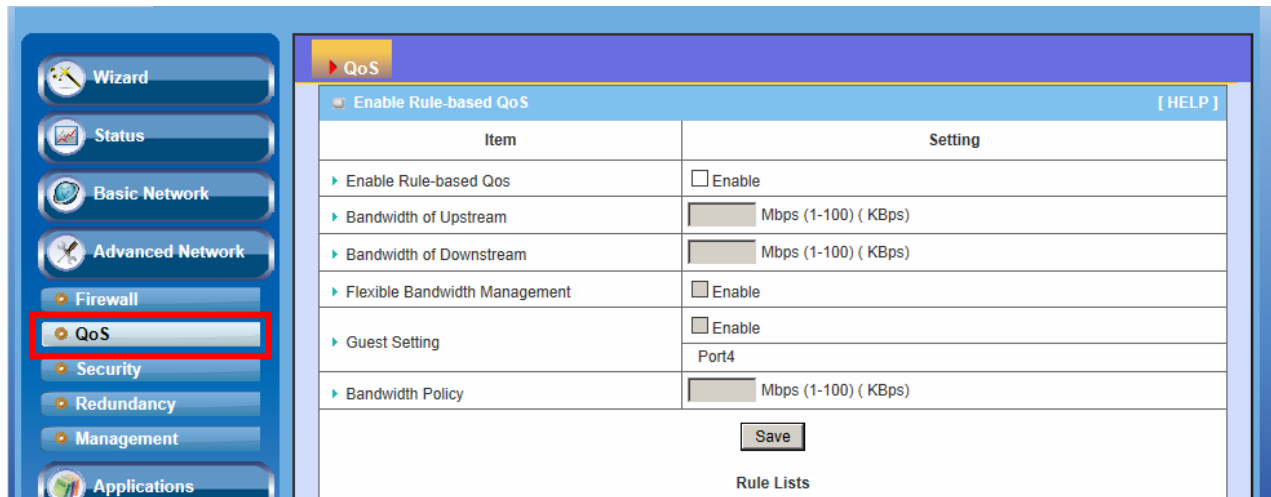
2. **Discard PING from WAN side:** When this feature is enabled, any host on the WAN side cannot ping this product.
3. **SPI Mode:** SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol
4. **Keep WAN in stealth mode:** If enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

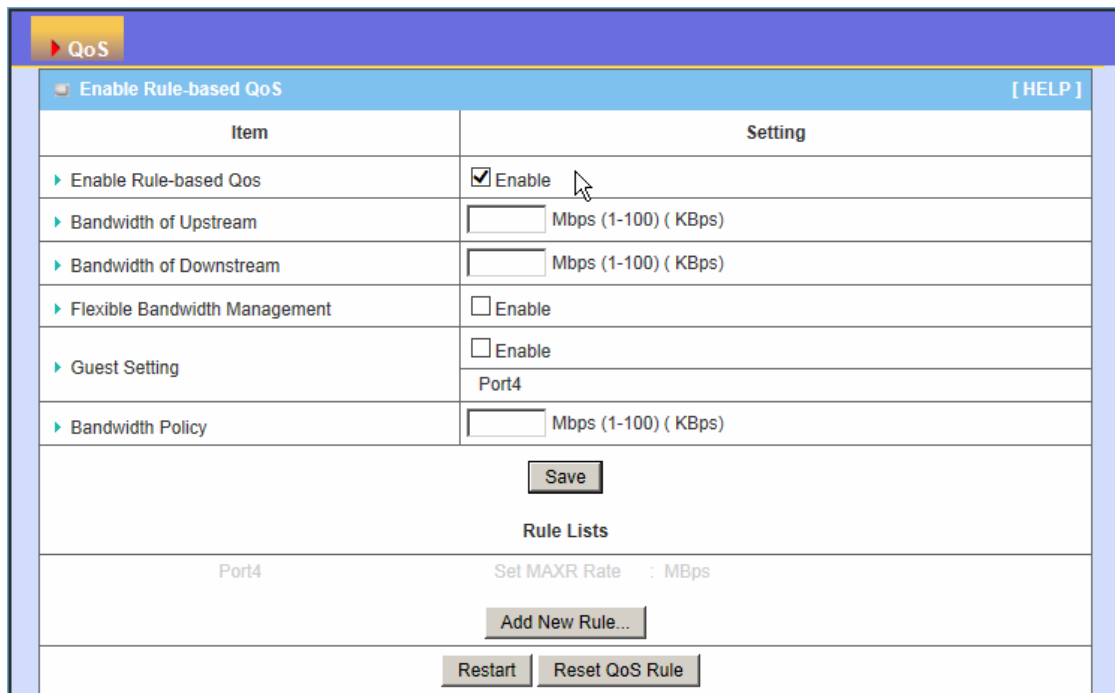
3.2.2 QoS (Quality of Service)

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.



3.2.2.1 Rule-based QoS



1. **QoS:** You can enable/disable this QoS function.
2. **Bandwidth of Upstream / Bandwidth of Downstream:** You can input the value of maximum upstream and downstream bandwidth from your ISP
3. **Flexible Bandwidth Management (FBM):** When this management is enabled, system will share the bandwidth to normal applications
4. **Guest Setting / Bandwidth Policy:** This device can allocate a designated

internet bandwidth for the forth LAN port (Port4). If you want to enable this function, check the “Enable” checkbox and enter the allowed bandwidth.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Create a QoS Rule:

You can click on the button “Add New Rule” shown in the icon above to create a new QoS rule.

Item	Setting
▶ Rule	<input type="checkbox"/> Enable
▶ Grouping	IP [] - []
▶ Service	DSCP [] ▶ DiffServ CodePoint [Default]
▶ Control	PRI [] []
▶ Direction	In []
▶ Schedule	(0) Always []

[Save] [Undo]

1. **Rule:** Enable the rule setting first.
2. **Grouping:** Select the QoS grouping class from the drop list, and specify the grouping information accordingly.

Grouping	Description
IP	IP address based
MAC	MAC based

3. **Service:** Set your own “Service” type to enable the QoS rule as below.

Service	Description
DSCP	DiffServ Code Point
Service Port	Mean TCP or UDP Port
Pre-defined Application profiles	Normal service Application
Connection Sessions	NAT Session

4. **Control:** Set the corresponding control type for the selected service type.

Control	Description	Data
DSCP Marking	Priority as you select DiffServ CodePoint	CS1 ~ AF
PRI	Priority	1~6(1 is highest Priority)

MAXR	Maximum bandwidth Rate	KBps/MBps
MINR	Minimum bandwidth Rate	KBps/MBps
SESSION	Connection session	Number (1~20000)

5. **Direction:** Select the traffic direction to be applied for this QoS rule.

Direction	
IN	In-bond
OUT	Out-bond
BOTH	In-bond & Out-bond

6. **Schedule:** The QoS rule can be turn off according to the schedule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Example for adding a “DSCP” type QoS rule:

Item	Setting
▶ Rule	<input checked="" type="checkbox"/> Enable
▶ Grouping	IP 192.168.12.10 -- 40
▶ Service	DSCP ▶ DiffServ CodePoint IP Precedence 4(CS4)
▶ Control	DSCP MARKING AF Class2(High Drop)
▶ Direction	In
▶ Schedule	(0) Always

Save Undo

Grouping: Select “IP” and entry IP Range.

Service: Select “DSCP” and “Source Network Packets” which DiffServ are set as CS4.

Control: Select “DSCP Marking” and mark these Packets as “AF Class 2”.

Direction: Select “IN” for In-bound traffic only.

Schedule: Leave the default value of “(0)Always” as it is.

This Rule means IP Packets from WAN or other interfaces with DiffServ value of CS4 will be modified with DSCP Marking of “AF Class 2”, then forward corresponding packets to the Clients whose IP address is in the range of 192.168.12.10~40.

Example for adding a “Connection Sessions” type QoS rule:

QoS Rule Setting - Rule ID11	
Item	Setting
▶ Rule	<input checked="" type="checkbox"/> Enable
▶ Grouping	IP 192.168.123.100 - 120
▶ Service	Connection Sessions
▶ Control	SESSION 200 (Session 1~20000)
▶ Direction	Out
▶ Sharing Method	Single
▶ Schedule	(0) Always

Save Undo

Control: Set NAT session number as 200.

Direction: Select “Out” for Out-bound traffic only. It is for the client devices under the Gateway to establish session with servers on the Internet.

Sharing Method: Select “Single” or “Grouping” from the drop list. In this case, “Single” is selected.

Schedule: leave the default value of “(0)Always” as it is.

This Rule defines that each single user, whose IP address is in the range of 192.168.123.100~120, can access to a remote server on the Internet, and keep a maximum 200 sessions at the same time.

Finishing QoS settings:

Once you saved the QoS rule, it will be displayed in the Rule List area as below.

Advanced Setting								
QoS Rules Table								
<input checked="" type="checkbox"/>	1.	↓	<input checked="" type="checkbox"/> UDP	5060	Set MARKING none	CS2	(Both)	(Always)
<input checked="" type="checkbox"/>	2.	↑	<input checked="" type="checkbox"/> UDP	1701	Set MARKING none	AF31	(In)	(Always)

Add New Rule...

Besides, you can move up or down the priority of all rules by clicking on the ‘↑’ or ‘↓’ icon if you want to change the priority of rules. You can also unmark any rule in the list if you don’t want to enable it.

Advanced Setting								
QoS Rules Table								
<input checked="" type="checkbox"/>	1.	↓	<input checked="" type="checkbox"/> UDP	1701	Set MARKING none	AF31	(In)	(Always)
<input checked="" type="checkbox"/>	2.	↑	<input checked="" type="checkbox"/> UDP	5060	Set MARKING none	CS2	(Both)	(Always)

Add New Rule...

Restart Reset

Move down Rule 1 OK!

3.2.3 VPN Setup

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

3.2.3.1 VPN-IPSec

Item		Setting	
▶ VPN-IPSEC		<input type="checkbox"/> Enable	
▶ Netbios over IPSEC		<input type="checkbox"/> Enable	
▶ NAT Traversal		<input type="checkbox"/> Enable	
▶ Max. number of tunnels		<input type="text" value="5"/>	

Item	Status	Action	Enable
Dynamic IP VPN		<input type="button" value="Edit"/>	<input type="checkbox"/>

ID	Tunnel Name	Remote Addr.	Gateway	Status	Action	Enable
1					<input type="button" value="Edit"/>	<input type="checkbox"/>
2					<input type="button" value="Edit"/>	<input type="checkbox"/>
3					<input type="button" value="Edit"/>	<input type="checkbox"/>
4					<input type="button" value="Edit"/>	<input type="checkbox"/>
5					<input type="button" value="Edit"/>	<input type="checkbox"/>

1. **VPN-IPSEC:** You could trigger the function of VPN-IPSEC if you click “**enable**”.
2. **Netbios over IPSEC:** If you would like two LAN to receive the Netbios from Network Neighborhood, you have to click “**enable**”.
3. **NAT Traversal:** Some NAT router will block IPSec packets if it doesn't support IPSec pass-through. If you connect to another NAT router which doesn't support IPSec pass-through at WAN side, you need to activate this option.
4. **Max. number of tunnels:** The device supports up to 32 IPSec tunnels. You can

define the required IPsec tunnel settings by clicking on the corresponding “Edit” button and then check the “Enable” checkbox to enable it.

5. **Dynamic IP VPN:** Enable it when you need remote mobile hosts build security tunnel with the Gateway. It is disabled by default. Click “Edit” button to finish configuration.

3.2.3.1.1 Dynamic IP VPN

VPN gateway can ignore IP information of client when using Dynamic VPN, so it is suitable for users to build VPN tunnel with VPN gateway from a remote mobile host.

VPN Dynamic IP Setting [HELP]	
Item	Setting
▶ Tunnel Name	<input type="text"/>
▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>
▶ Phase1 Key Life Time	<input type="text"/> seconds
▶ Phase2 Key Life Time	<input type="text"/> seconds
▶ Encapsulation Protocol	ESP ▾
▶ PFS Group	Disable ▾
▶ Preshare Key	<input type="text"/>
▶ Remote ID	Type: Username ▾ ID: <input type="text"/>
▶ Local ID	Type: Username ▾ ID: <input type="text"/>
▶ Dead Peer Detection (DPD)	<input type="checkbox"/> Enable ▶ Timeout: <input type="text"/> seconds ▶ Delay: <input type="text"/> seconds
▶ XAUTH	<input checked="" type="radio"/> None <input type="radio"/> Server

Set IKE Proposal				
ID	Encryption	Authentication	DH Group	Enable
1	DES ▾	SHA1 ▾	Group 1 ▾	<input type="checkbox"/>
2	DES ▾	SHA1 ▾	Group 1 ▾	<input type="checkbox"/>

Set IPSEC Proposal			
ID	Encryption	Authentication	Enable
1	DES ▾	None ▾	<input type="checkbox"/>
2	DES ▾	None ▾	<input type="checkbox"/>

1. **Tunnel name:** Assign a name of this tunnel.
2. **Local subnet:** The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
3. **Local Netmask:** The local netmask and associated local subnet can define a

subnet domain for the devices connected via the VPN tunnel.

4. **Phase 1 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.
5. **Phase 2 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 2 between both end gateways.
6. **Encapsulation Protocol:** There are three protocols can be selected: ESP, AH, or ESP+AH.
7. **PFS Group:** Configures Perfect Forward Secrecy for connections created with this IPsec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.
 - Disable:** No PFS group
 - Group 1:** 768-bit Diffie-Hellman prime modulus group
 - Group 2:** 1024-bit Diffie-Hellman prime modulus group
 - Group 5:** 1536-bit Diffie-Hellman prime modulus group
8. **Preshare key:** The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be the same one for both VPN gateways and clients.
9. **Remote ID:** The Type and the Value of the local VPN gateway must be the same as that of the local ID of the remote VPN gateway.
10. **Local ID:** The Type and the Value of the local VPN gateway must be the same as that of the Remote ID of the remote VPN gateway.
11. **Dead Peer Detection:** This feature will detect if remote VPN gateway still exists. Indicate time of interval between every detection, and assigns value of timeout.
12. **XAUTH:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or VPN gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server.
 - XAUTH - None:** Without Extended Authentication (xAuth).
 - XAUTH - Server:** Check this checkbox if the device behaves as a VPN server, and will validate the user information of VPN clients. You can click on "XAUTH Account" button at IPsec Setting main page to edit the permitted user account / password.
13. **Set IKE Proposal:** Check this checkbox to enable IKE proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.

Authentication: There are two algorithms can be selected: SHA1 and MD5.

DH Group: There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).

Enable: Check this checkbox to enable the IKE Proposal with this rule.

14. **Set IPSec Proposal:** Check this checkbox to enable IPSec proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.

Authentication: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPSec proposal.

Enable: Check this checkbox to enable IPSec Proposal with this rule.

Click on “Save” to store what you just select or” Undo” to give up

3.2.3.1.2 IPSec-IKE Setting

VPN Settings - Tunnel 1 [HELP]																
Item	Setting															
▶ Tunnel Name	<input type="text"/>															
▶ Method	IKE <input type="button" value="v"/>															
▶ Local Subnet	<input type="text"/>															
▶ Local Netmask	<input type="text"/>															
▶ Remote Subnet	<input type="text"/>															
▶ Remote Netmask	<input type="text"/>															
▶ Remote Gateway	<input type="text"/>															
▶ Phase1 Key Life Time	<input type="text"/> seconds															
▶ Phase2 Key Life Time	<input type="text"/> seconds															
▶ Encapsulation Protocol	ESP <input type="button" value="v"/>															
▶ PFS Group	Disable <input type="button" value="v"/>															
▶ Aggressive Mode	<input type="checkbox"/> Enable															
▶ Preshare Key	<input type="text"/>															
▶ Connection Type	Connect-on-Demand <input type="button" value="v"/>															
▶ Remote ID	Type: Username <input type="button" value="v"/> ID: <input type="text"/>															
▶ Local ID	Type: Username <input type="button" value="v"/> ID: <input type="text"/>															
▶ Dead Peer Detection (DPD)	<input type="checkbox"/> Enable ▶ Timeout : <input type="text"/> 180 seconds ▶ Delay : <input type="text"/> 30 seconds															
▶ XAUTH	<input checked="" type="radio"/> None <input type="radio"/> Server <input type="radio"/> Client ▶ Username : <input type="text"/> ▶ Password : <input type="text"/>															
▶ Set IKE Proposal	<input type="checkbox"/> Enable															
	<table border="1"> <thead> <tr> <th>ID</th> <th>Encryption</th> <th>Authentication</th> <th>DH Group</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DES <input type="button" value="v"/></td> <td>SHA1 <input type="button" value="v"/></td> <td>None <input type="button" value="v"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>2</td> <td>DES <input type="button" value="v"/></td> <td>SHA1 <input type="button" value="v"/></td> <td>None <input type="button" value="v"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	ID	Encryption	Authentication	DH Group	Enable	1	DES <input type="button" value="v"/>	SHA1 <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>	2	DES <input type="button" value="v"/>	SHA1 <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>
ID	Encryption	Authentication	DH Group	Enable												
1	DES <input type="button" value="v"/>	SHA1 <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>												
2	DES <input type="button" value="v"/>	SHA1 <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>												
▶ Set IPSEC Proposal	<input type="checkbox"/> Enable															
	<table border="1"> <thead> <tr> <th>ID</th> <th>Encryption</th> <th>Authentication</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>DES <input type="button" value="v"/></td> <td>None <input type="button" value="v"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>2</td> <td>DES <input type="button" value="v"/></td> <td>None <input type="button" value="v"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	ID	Encryption	Authentication	Enable	1	DES <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>	2	DES <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>			
ID	Encryption	Authentication	Enable													
1	DES <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>													
2	DES <input type="button" value="v"/>	None <input type="button" value="v"/>	<input type="checkbox"/>													
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>																

1. **Tunnel name:** Assign a name of this tunnel.
2. **Method:** There are IKE and Manual options. Please choose IKE here.
3. **Local subnet:** The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
4. **Local Netmask:** The local netmask and associated local subnet can define a

- subnet domain for the devices connected via the VPN tunnel.
5. **Remote subnet:** The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.
 6. **Remote Netmask:** The remote netmask and associated remote subnet can define a subnet domain for the devices connected via the VPN tunnel.
 7. **Remote Gateway:** Enter the IP address of remote VPN gateway.
 8. **Phase 1 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.
 9. **Phase 2 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 2 between both end gateways.
 10. **Encapsulation Protocol:** There are three protocols can be selected: ESP, AH, or ESP+AH.
 11. **PFS Group:** Configures Perfect Forward Secrecy for connections created with this IPsec transport profile by assigning a Diffie-Hellman prime modulus group. There are three groups can be selected: Group 1, Group 2, Group 5.
 - Disable:** No PFS group
 - Group 1:** 768-bit Diffie-Hellman prime modulus group
 - Group 2:** 1024-bit Diffie-Hellman prime modulus group
 - Group 5:** 1536-bit Diffie-Hellman prime modulus group
 12. **Aggressive Mode:** Enabling this mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.
 13. **Preshare key:** The first key that supports IKE mechanism of both VPN gateway and VPN client host for negotiating further security keys. The pre-shared key must be the same one for both VPN gateways and clients.
 14. **Connection Type:** There are three options for you to choose when the VPN tunnel will be established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”.
 15. **Remote ID:** The Type and the Value of the local VPN gateway must be the same as that of the local ID of the remote VPN gateway.
 16. **Local ID:** The Type and the Value of the local VPN gateway must be the same as that of the Remote ID of the remote VPN gateway.
 17. **Dead Peer Detection:** This feature will detect if remote VPN gateway still exists. Indicate time of interval between every detection, and assigns value of timeout.
 18. **XAUTH:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or VPN gateway). The VPN server would reject the connect request from VPN

clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server.

XAUTH - None: Without Extended Authentication (xAuth).

XAUTH - Server: Check this checkbox if the device behaves as a VPN server, and will validate the user information of VPN clients. You can click on "XAUTH Account" button at IPsec Setting main page to edit the permitted user account / password.

XAUTH - Client: Check this checkbox if the device behaves as a VPN client, and will send user information to remote VPN server for extended authentication. You need to fill in correct user name and password to pass the extended authentication.

19. **Set IKE Proposal:** Check this checkbox to enable IKE proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256.

Authentication: There are two algorithms can be selected: SHA1 and MD5.

DH Group: There are three groups can be selected: Group 1 (MODP768), Group 2 (MODP1024), and Group 5 (MODP1536).

Enable: Check this checkbox to enable the IKE Proposal with this rule.

20. **Set IPsec Proposal:** Check this checkbox to enable IPsec proposals.

Encryption: There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. But when the encapsulation protocol is set to AH, you can choose Null without encryption.

Authentication: There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for IPsec proposal.

Enable: Check this checkbox to enable IPsec Proposal with this rule.

Click on "Save" to store what you just select or "Undo" to give up

3.2.3.1.3 IPSec-Manual Setting

VPN Settings - Tunnel 1 [HELP]	
Item	Setting
▶ Tunnel Name	<input type="text"/>
▶ Method	Manually ▼
▶ Local Subnet	<input type="text"/>
▶ Local Netmask	<input type="text"/>
▶ Remote Subnet	<input type="text"/>
▶ Remote Netmask	<input type="text"/>
▶ Remote Gateway	<input type="text"/>
▶ Encapsulation Protocol	ESP ▼
▶ Outbound SPI	0x <input type="text"/>
▶ Inbound SPI	0x <input type="text"/>
▶ Encryption Algorithm	3DES ▼
▶ Encryption Key	<input type="text"/> <input type="text"/>
▶ Authentication Algorithm	None ▼
▶ Authentication Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

1. **Tunnel name:** Assign a name of this tunnel.
2. **Method:** There are IKE and Manual options. Please choose “Manual” here.
3. **Local subnet:** The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.
4. **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the devices connected via the VPN tunnel.
5. **Remote subnet:** The subnet of LAN site of remote VPN gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.
6. **Remote Netmask:** The remote netmask and associated remote subnet can define a subnet domain for the devices connected via the VPN tunnel.
7. **Remote Gateway:** Enter the IP address of remote VPN gateway.
8. **Encapsulation Protocol:** There are two protocols can be selected: ESP or AH.
9. **Outbound SPI:** SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.
10. **Inbound SPI:** Inbound SPI will be included in the inbound packet transmitted from WAN site of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of outbound SPI should be set in hex formatted.

- 11. **Encryption Algorithm:** There are two algorithms can be selected: DES, or 3DES.
- 12. **Encryption Key:** Encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex formatted.
- 13. **Authentication Algorithm:** There are two algorithms can be selected: SHA1 or MD5.
- 14. **Authentication Key:** Authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex formatted.

Click on “Save” to store what you just select or” Undo” to give up

3.2.3.1.4 XAUTH Account

IPsec XAUTH Server side setting

ID	Account	Password
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

You can edit user information with this configuration page. This user information is only valid for VPN Server with XAuth Server mode selected.

3.2.3.2 VPN-PPTP Server

The VPN gateway can behave as a PPTP server, and allows remote hosts to access LAN servers behind the PPTP server. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

The screenshot shows the configuration page for the PPTP Server. The navigation bar at the top includes IPsec, PPTP Server (selected), PPTP Client, L2TP Server, and L2TP Client. The main content area is titled 'PPTP Server' and contains the following sections:

- PPTP Server:** A table with 'Item' and 'Setting' columns. The 'VPN-PPTP Server' item has an 'Enable' checkbox.
- PPTP Server Configuration:** A table with 'Item' and 'Setting' columns.
 - 'Server virtual IP': 192.168.0.1
 - 'IP Pool Starting Address': 10
 - 'IP Pool Ending Address': 100
 - 'Authentication Protocol': Radio buttons for PAP, CHAP, MS_CHAP, and MS_CHAPv2.
 - 'MPPE Encryption Mode': An 'Enable' checkbox.
 - 'Encryption Length': Radio buttons for 40 bits, 56 bits, and 128 bits.
- User Account:** A table with columns for ID, Username, and Password. It contains 5 rows, each with a numeric ID and empty input fields for Username and Password.
- Connection Status:** A table with columns for Username, Peer IP, Virtual IP, Peer Call ID, and Operation. The current status is 'No connection from remote'. Below the table are 'Save', 'Undo', and 'Refresh' buttons.

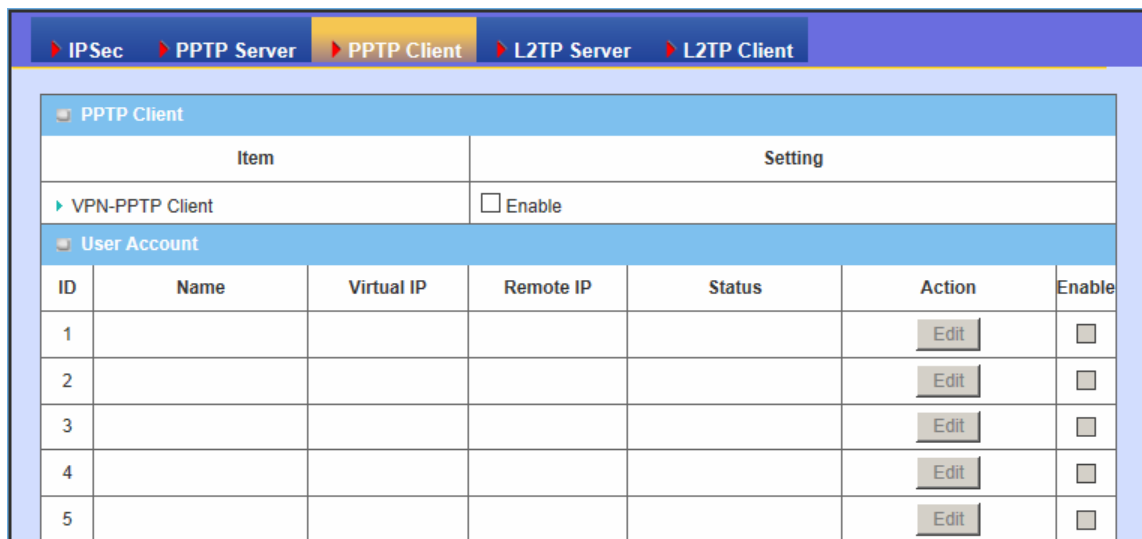
1. **VPN-PPTP Server:** Enable or Disable PPTP server function.
2. **Server Virtual IP:** The IP address of PPTP server. This IP address should be different from IP address of L2TP server and LAN subnet of VPN gateway.
3. **IP Pool Start Address:** This device will assign an IP address to remote PPTP client. This value indicates the beginning of IP pool.
4. **IP Pool End Address:** This device will assign an IP address to remote PPTP client. This value indicates the end of IP pool.
5. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2).
6. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption.

Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method.

7. **Encryption Length:** You can choose encryption length of MPPE encryption.
8. **User Account:** You can input up to 10 different user accounts for PPTP server.
9. **Connection Status:** The connected PPTP user & connection information will be shown in this table.

Click on “Save” to store what you just select or” Undo” to give up

3.2.3.3 VPN-PPTP Client



PPTP Client						
Item	Setting					
▶ VPN-PPTP Client	<input type="checkbox"/> Enable					
User Account						
ID	Name	Virtual IP	Remote IP	Status	Action	Enable
1					Edit	<input type="checkbox"/>
2					Edit	<input type="checkbox"/>
3					Edit	<input type="checkbox"/>
4					Edit	<input type="checkbox"/>
5					Edit	<input type="checkbox"/>

1. **VPN-PPTP Client:** Enable or Disable PPTP client function.
2. **User Account:** You can input up to 10 different user accounts for PPTP client, define each user account settings by clicking on the corresponding “Edit” button and then check the “Enable” checkbox to enable it.

User Account - 1 [HELP]	
Item	Setting
▶ Name	<input type="text"/>
▶ Peer IP/Domain	<input type="text"/>
▶ Username	<input type="text"/>
▶ Password	<input type="text"/>
▶ Default Gateway	<input type="checkbox"/> Enable
▶ Peer Subnet	<input type="text"/>
▶ Connection Control	Connect-on-Demand ▼
▶ Option	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT
▶ Authentication	<input type="checkbox"/> Enable
▶ Authentication Protocol	▶ PAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ CHAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ MSCHAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ MSCHAPV2 <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject
▶ LCP Echo Type	<input checked="" type="radio"/> Auto <input type="radio"/> Manually <input type="radio"/> Disable ▶ Interval <input type="text" value="30"/> seconds ▶ Max. Failure Time <input type="text" value="6"/> times
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

3. **Name:** The name of this rule.
4. **Peer IP/Domain:** The IP address or Domain name of remote PPTP server.
5. **User Name:** The user name which is provided by remote PPTP server.
6. **Password:** The password which is provided by remote PPTP server.
7. **Default Gateway:** You can check the “Enable” checkbox to set this tunnel as the default gateway for WAN connection.
8. **Peer Subnet:** The LAN subnet of remote PPTP server.
9. **Connection Control:** There are three options for users to choose when the PPTP tunnel is established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”.
10. **Option:** Enable or disable the MPPE and NAT function. If you enable MPPE, then this PPTP tunnel will be encrypted.
11. **Authentication:** You need to enable this option if remote PPTP server requests it.
12. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2). The protocol you choose must be supported by remote PPTP server.
13. **LCP Echo Type:** Choose the way to do connection keep alive.

3.2.3.4 VPN-L2TP Server

The VPN gateway can behave as a L2TP server, and allows remote hosts to access LAN servers behind the L2TP server. The device can support three authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

L2TP Server [HELP]

Item	Setting
▶ VPN-L2TP Server	<input type="checkbox"/> Enable
▶ L2TP Over IPsec	<input type="checkbox"/> Enable

L2TP Server Configuration

Item	Setting
▶ Server virtual IP	192.168.10.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	100
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS_CHAP <input type="checkbox"/> MS_CHAPv2
▶ MPPE Encryption Mode	<input type="checkbox"/> Enable
▶ Encryption Length	<input type="checkbox"/> 40 bits <input type="checkbox"/> 56 bits <input type="checkbox"/> 128 bits

User Account

ID	Username	Password
1		
2		
3		
4		
5		

Connection Status

Username	Peer IP	Virtual IP	Peer Call ID	Operation
No connection from remote				

Save Undo Refresh

1. **VPN-L2TP Server:** Enable or Disable L2TP server function.
2. **L2TP Over IPsec:** L2TP over IPsec VPNs allow you to transport data over the Internet, while still maintaining a high level of security to protect data. Enter a Pre-sharekey when you use some devices, like Apple related mobile devices to establish L2TP tunnels

▶ L2TP Over IPsec Enable
▶ Preshare Key

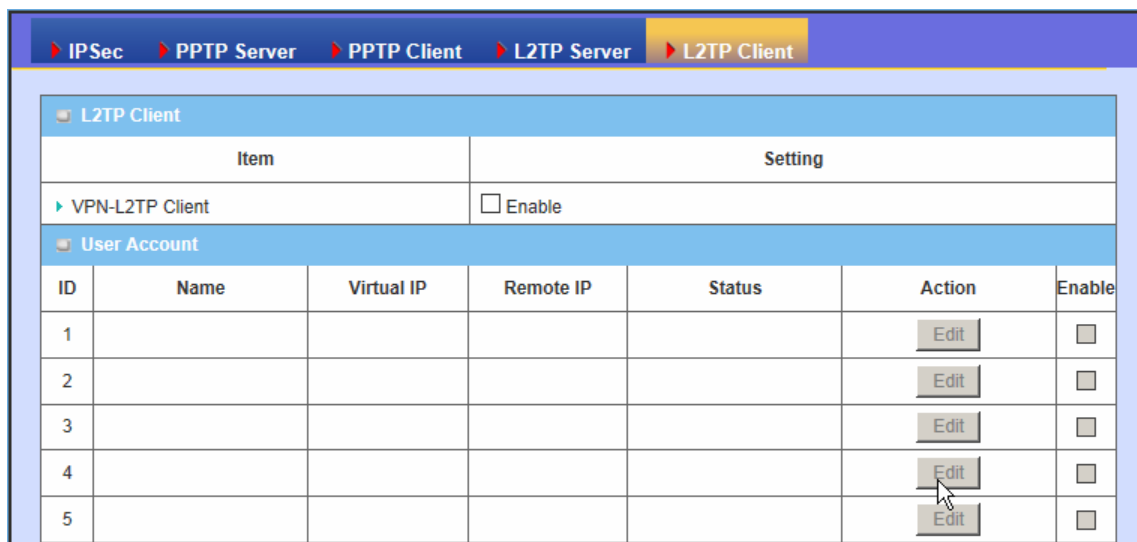
3. **Server Virtual IP:** The IP address of L2TP server. This IP address should be

different from IP address of PPTP server and LAN subnet of VPN gateway.

4. **IP Pool Starting Address:** This device will assign an IP address to remote L2TP client. This value indicates the beginning of IP pool.
5. **IP Pool Ending Address:** This device will assign an IP address to remote L2TP client. This value indicates the end of IP pool.
6. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2).
7. **MPPE Encryption Mode:** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method.
8. **Encryption Length:** You can choose encryption length of MPPE encryption.
9. **User Account:** You can input up to 10 different user accounts for L2TP server.
10. **Connection Status:** The connected L2TP user & connection information will be shown in this table.

Click on “Save” to store what you just select or” Undo” to give up

3.2.3.5 VPN-L2TP Client



1. **VPN-L2TP Client:** Enable or Disable L2TP client function.
2. **User Account:** You can input up to 10 different user accounts for L2TP client, define each user account settings by clicking on the corresponding “Edit” button and then check the “Enable” checkbox to enable it.

User Account - 1 [HELP]	
Item	Setting
▶ Name	<input type="text"/>
▶ Peer IP/Domain	<input type="text"/>
▶ Username	<input type="text"/>
▶ Password	<input type="text"/>
▶ Default Gateway	<input type="checkbox"/> Enable
▶ Peer Subnet	<input type="text"/>
▶ Connection Control	Connect-on-Demand ▼
▶ Option	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT <input type="checkbox"/> CCP
▶ Authentication	<input type="checkbox"/> Enable
▶ Authentication Protocol	▶ PAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ CHAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ MSCHAP <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject ▶ MSCHAPV2 <input checked="" type="radio"/> Default <input type="radio"/> Accept <input type="radio"/> Reject
▶ LCP Echo Type	<input checked="" type="radio"/> Auto <input type="radio"/> Manually <input type="radio"/> Disable ▶ Interval <input type="text" value="30"/> seconds ▶ Max. Failure Time <input type="text" value="6"/> times
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

3. **Name:** The name of this rule.
4. **Peer IP/Domain:** The IP address or Domain name of remote L2TP server.
5. **User Name:** The user name which is provided by remote L2TP server.
6. **Password:** The password which is provided by remote L2TP server.
7. **Default Gateway:** You can check the “Enable” checkbox to set this tunnel as the default gateway for WAN connection.
8. **Peer Subnet:** The LAN subnet of remote L2TP server.
9. **Connect:** There are three options for users to choose when the L2TP tunnel will be established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”.
10. **Option:** Enable or disable MPPE, NAT, and CCP function. If you enable MPPE, then this L2TP tunnel will be encrypted.
11. **Authentication:** You need to enable this option if remote PPTP server requests it.
12. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MSCHAP(v1), or MSCHAP(v2). The protocol you choose must be supported by remote L2TP server.
13. **LCP Echo Type:** Choose the way to do connection keep alive.

Click on “Save” to store what you just select or “Undo” to give up

3.2.3.6 GRE Tunnel

Item		Setting					
▶ Default Gateway		None ▼					
ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

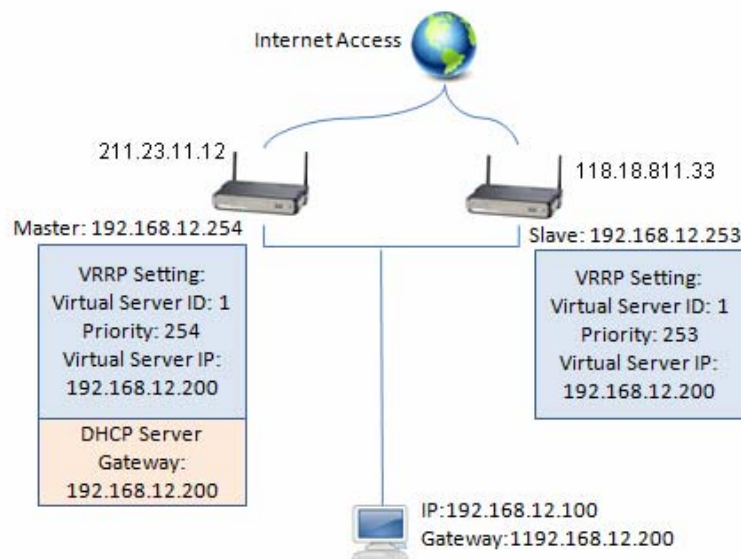
1. **Default Gateway:** You can choose a tunnel as the default gateway for WAN connection.
2. **Names:** The name of this GRE tunnel.
3. **Tunnel IP:** Assign a virtual IP address of this tunnel.
4. **Peer IP:** Enter the IP address of remote host that you want to connect.
5. **Key:** Enter the password to establish GRE tunnel with remote host.
6. **TTL:** Time-To-Live for packets. The value is within 1 to 255. If a packet passes number of TTL routers and still can't reach the destination, then this packet will be dropped.
7. **Subnet:** Enter the local subnet of remote host. If a packet wants to go to this subnet, the GRE tunnel will be established automatically
8. **Enable:** Enable or Disable this GRE tunnel.

Click on “Save” to store what you just select or” Undo” to give up

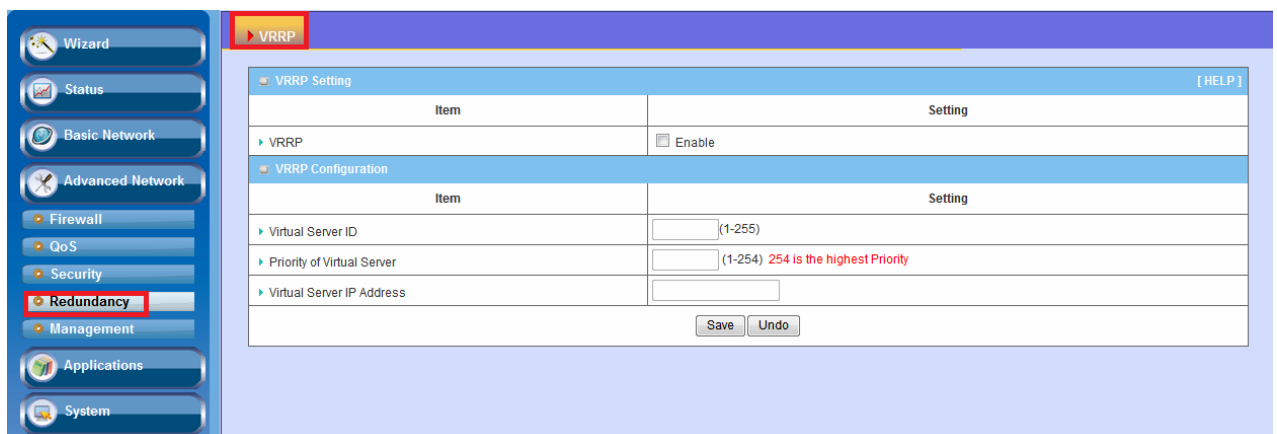
3.2.4 Redundancy

3.2.4.1 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol providing device redundancy. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.



The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.



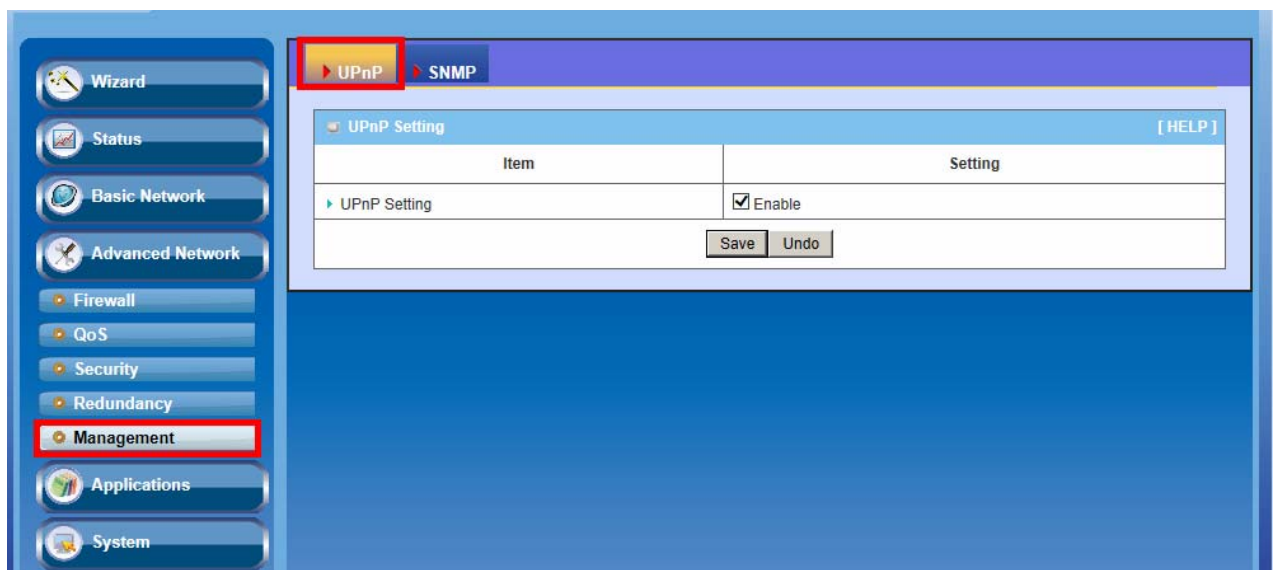
1. **Enable:** Enable or Disable the VRRP function.
2. **Virtual Server ID:** Means Group ID. Specify the ID number of the virtual server.
3. **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are 1-254, and a larger value has higher priority.
4. **Virtual Server IP Address:** Specify the IP address of the virtual server.

Click on “Save” to store what you just select or” Undo” to give up

3.2.5 Management

3.2.5.1 UPnP

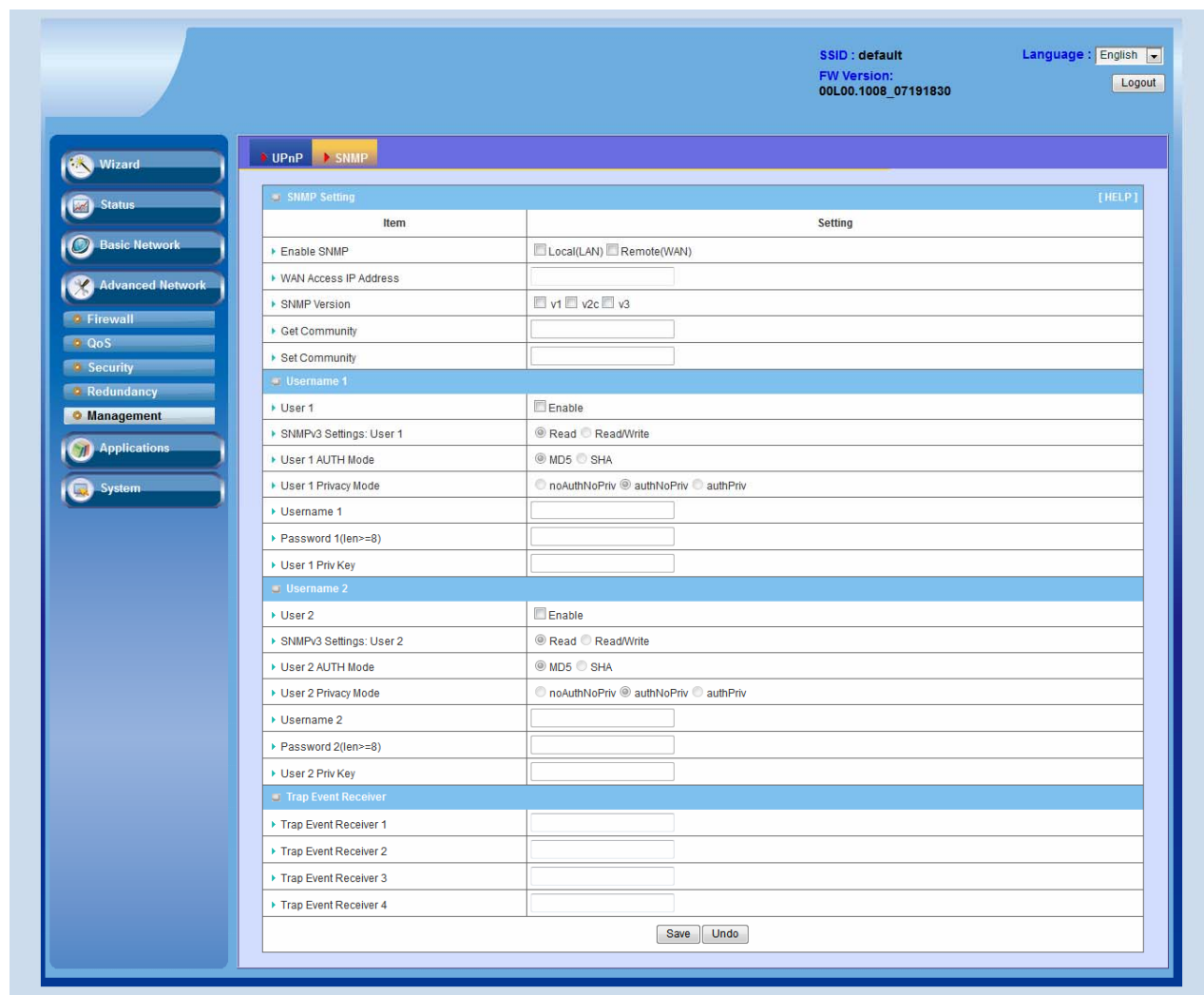
UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming



This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

3.2.5.2 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.



1. **Enable SNMP:** You can check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond to the request from LAN. If “Remote” is checked, this device will respond to be request from WAN.
2. **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.
3. **SNMP Version:** Supports SNMP V1, V2c, and V3.
4. **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to

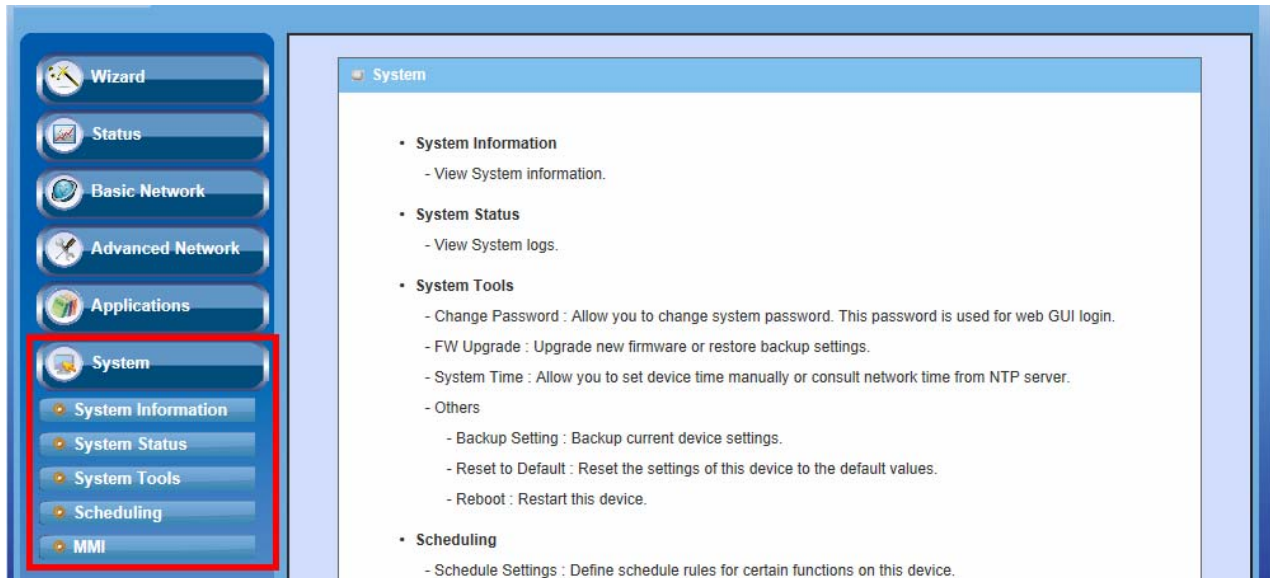
agents of managed network devices.

5. **Set Community:** The community of SetRequest that this device will accept.
6. **SNMPv3 Settings: User 1/2:** This device supports up to two SNMP management accounts. You can specify the account permission as “Read” or “Read/Write” respectively.
7. **User 1/2 AUTH Mode:** Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
8. **User 1/2 Privacy Mode:** You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
9. **Username 1/2:** Use this field to identify the user name for the specified level of access.
10. **Password 1/2:** Use this field to set the password for the specified level of access.
11. **User 1/2 Priv Key:** Use this field to define the encryption key for the specified level of access.
12. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

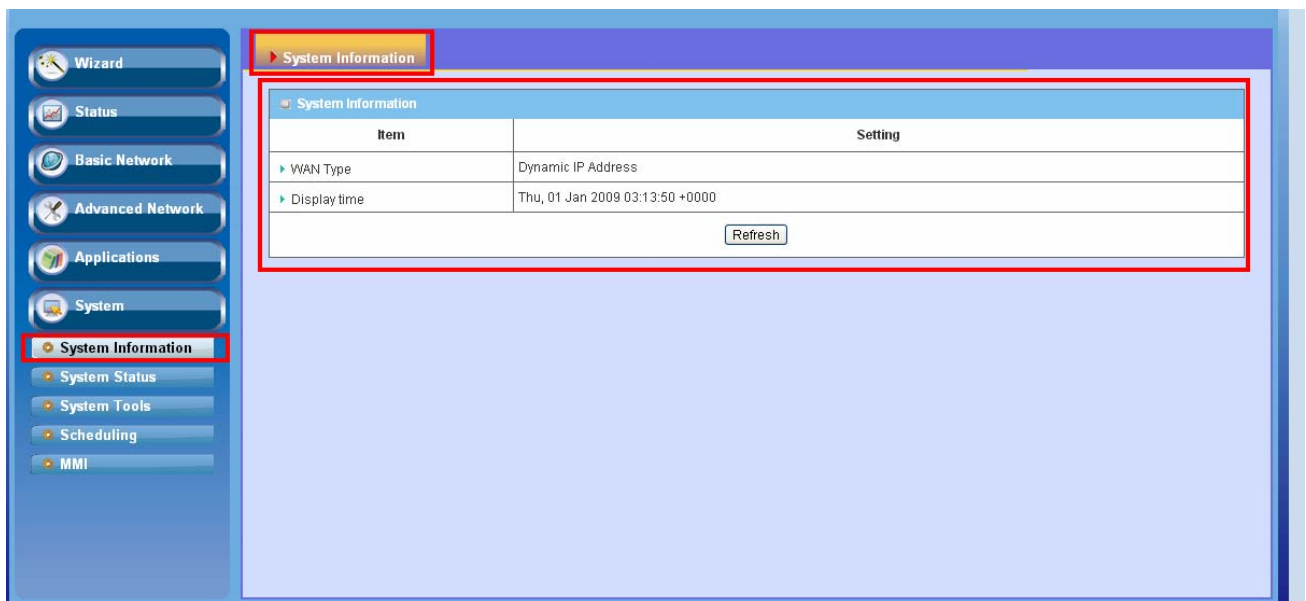
3.3 System

In this section you can see system information, system logs, use system tools for system update and do service scheduling and system administration setting.



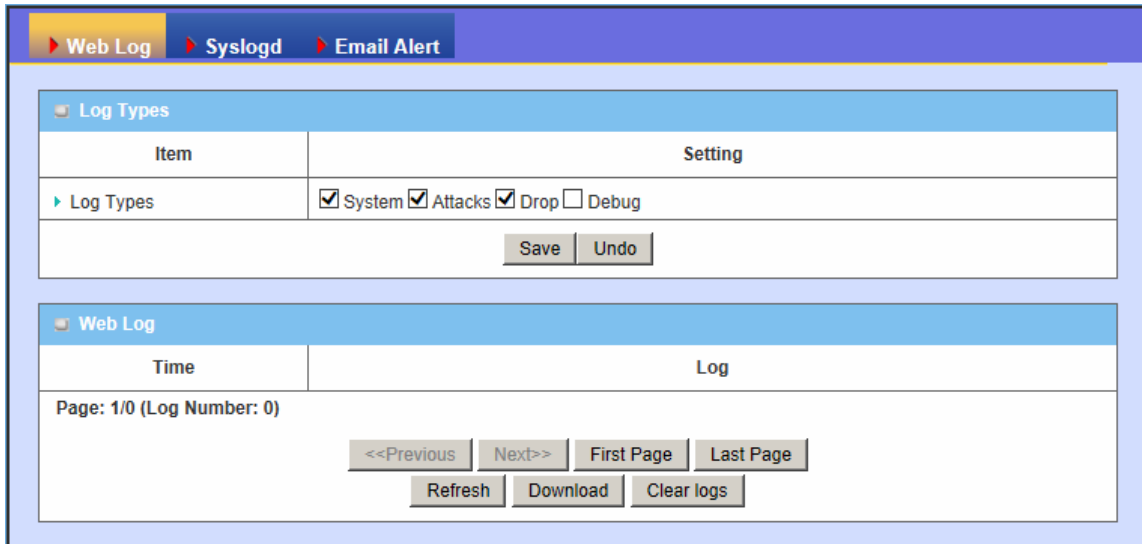
3.3.1 System Information

You can view the System Information in this page.



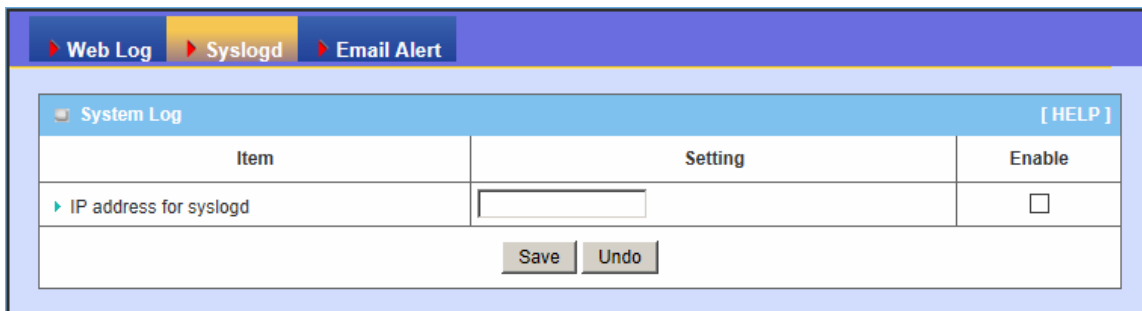
3.3.2 System Status

3.3.2.1 Web Log



1. **Log Types:** You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.
2. **Web Log:** You can browse, refresh, download, and clear the log messages.

3.3.2.2 Syslog



This device can also export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslogs

The items you have to setup include:

1. **IP Address for syslogd:** Host IP of destination where syslog will be sent to. Check **Enable** to enable this function.

3.3.2.3 Email Alert

Item	Setting	Enable
▶ Setting of Email alert		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

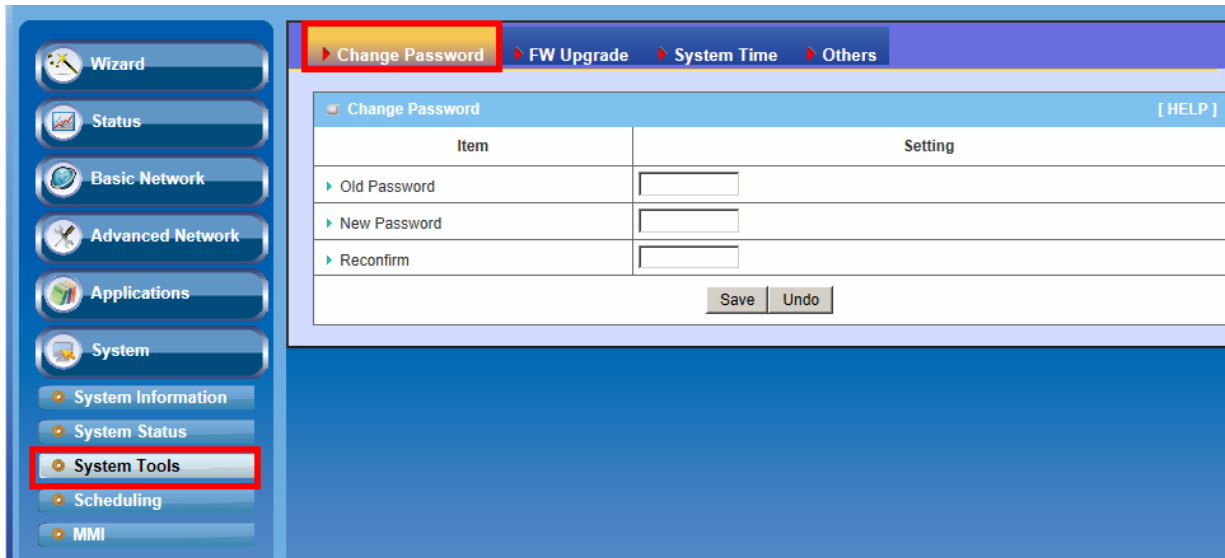
1. **Setting of Email alert:** Check if you want to enable Email alert (send syslog via email).
2. **SMTP Server: Port:** Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25. For example, "mail.your_url.com" or "192.168.1.100:26".
3. **SMTP Username:** Enter the Username offered by your ISP.
4. **SMTP Password:** Enter the password offered by your ISP.
5. **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
6. **E-mail Subject:** The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.3 System Tools

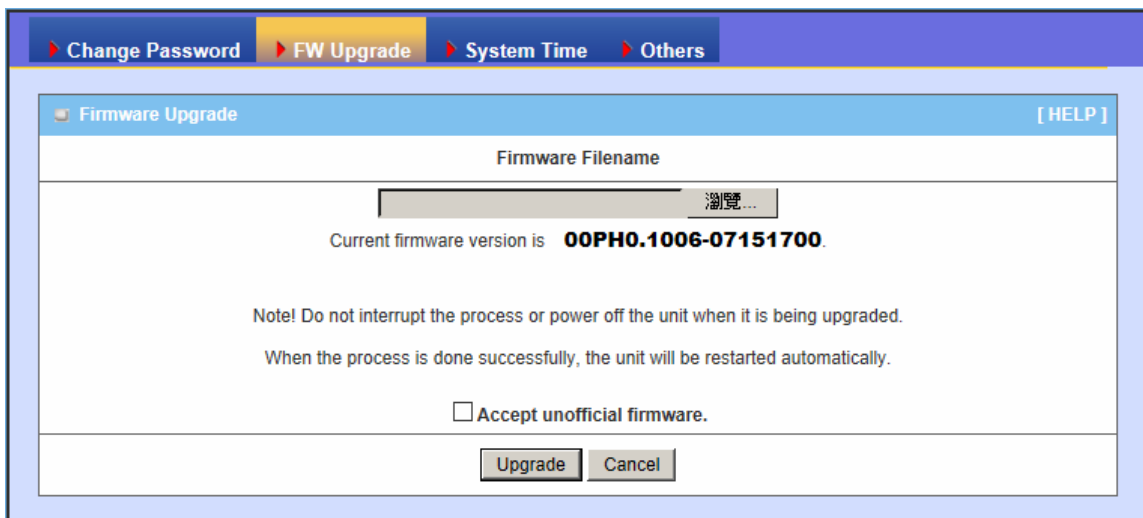
3.3.3.1 Change Password

You can change the System Password here. We **strongly** recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



3.3.3.2 FW Upgrade

If new firmware is available, you can upgrade router firmware through the WEB GUI here.



Press “browse” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

3.3.3.3 System Time

If new firmware is available, you can upgrade router firmware through the WEB GUI here.

Item	Setting
▶ Time Zone	* Not yet configured! The default is GMT+00:00
▶ Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): Auto
▶ Daylight saving time	<input type="checkbox"/>
▶ Date And Time Manually	2010 / July / 24 (Year/Month/Day) 12 : 01 : 25 (Hour:Minute:Second)

1. **Time Zone:** Select a time zone where this device locates.
2. **Auto-Synchronization:** Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
3. **Sync with Time Server:** Click on the button if you want to set Date and Time by NTP Protocol.
4. **Sync with my PC:** Click on the button if you want to set Date and Time using the PC’s Date and Time.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.3.3.4 Others

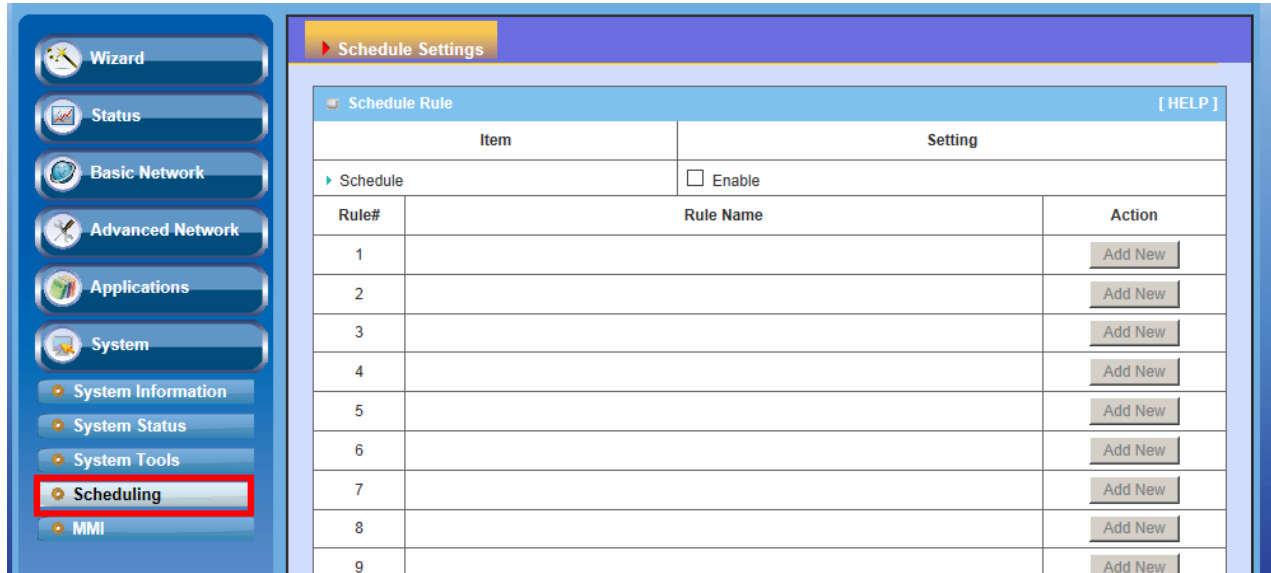
In this section you can do system backup, reset to default, system reboot settings and ping test.

Item	Setting
▶ Backup Setting	Backup
▶ Reset to Default	Reset
▶ Reboot	Reboot
▶ MAC Address for Wake-on-LAN	<input type="text"/> Wake up
▶ Domain Name or IP address for Ping Test	<input type="text"/> Ping
▶ Domain Name or IP address for Traceroute	<input type="text"/> Traceroute

1. **Backup Setting:** You can backup your settings by clicking the “**Backup**” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.
2. **Reset to Default:** You can also reset this device to factory default settings by clicking the “**Reset**” button.
3. **Reboot:** You can also reboot this device by clicking the “**Reboot**” button.
4. **MAC Address for Wake-on-LAN:** Wake-on-LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can enter the MAC address of the computer, in your LAN network, to be remotely turned on.
5. **Domain Name or IP address for Ping Test:** This allows you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.
6. **Domain Name or IP address for Traceroute:** Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point

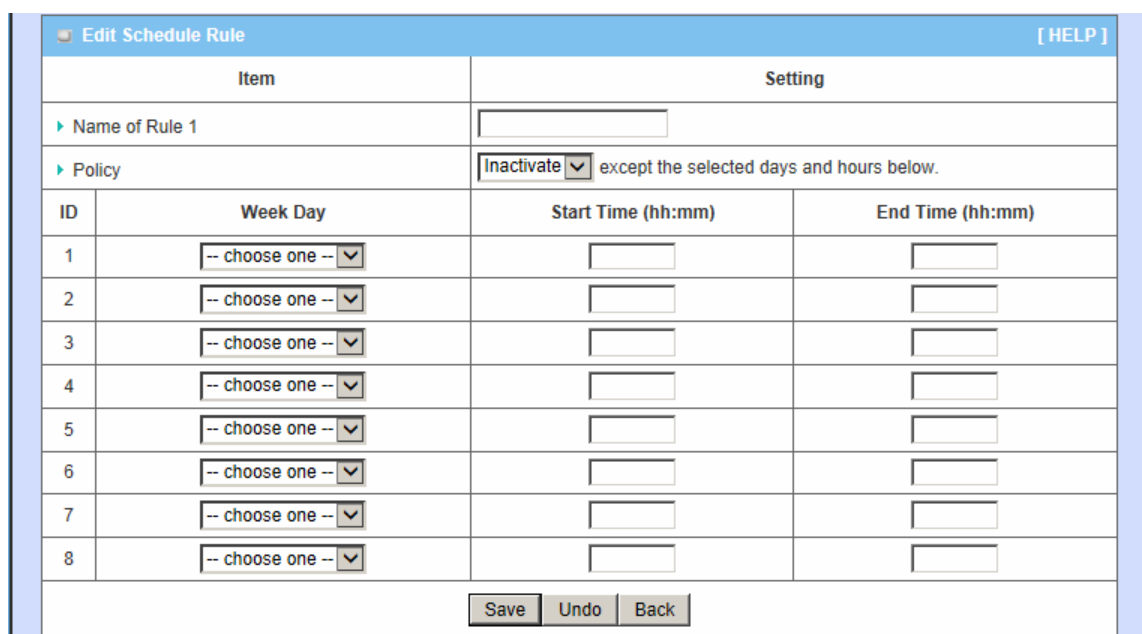
3.3.4 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed.



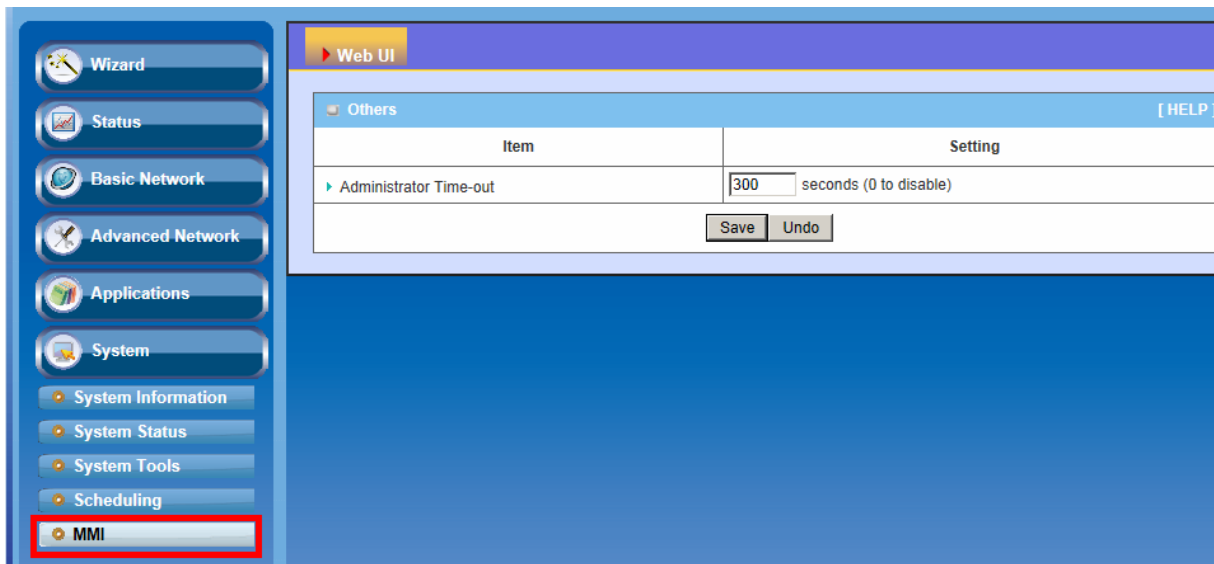
Add New Rule: To create a schedule rule, click the “Add New” button or the “Add New Rule...” button at the bottom. When the next dialog popped out you can edit the **Name of Rule**, **Policy**, and set the schedule time (**Week day**, **Start Time**, and **End Time**).

Afterwards, click “**save**” to store your settings or click “**Undo**” to give up the changes.



3.3.5 MMI

3.3.5.1 Web UI



You can set UI administration time-out duration give remote administration host port in this page. When the host port is given please remember to check the enable box and save your settings.

CHAPTER 4 Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the WiFi Broadband Router. You can refer to the following if you are having problems.

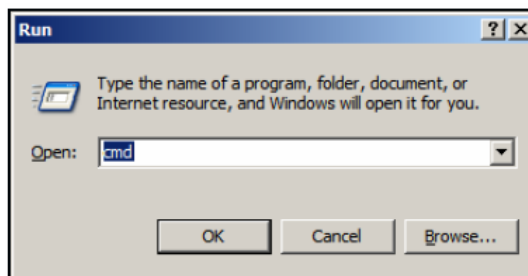
1 Why can't I configure the router even the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the WiFi Broadband Router is responding.

Note: It is recommended that you

Go to **Start > Run**.

1. Type **cmd**.



2. Press **OK**.
3. Type **ipconfig** to get the IP of default gateway.
4. Type "**ping 192.168.123.254**". Assure that you ping the correct IP Address assigned to the WiFi Broadband Router. It will show four replies if you ping correctly.

```
Pinging 192.168.123.254 with 32 bytes of data:  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64  
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed

properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on “My Computer” > Properties**.
2. **Select the Hardware Tab**.
3. Click **Device Manager**.
4. Double-click on **“Network Adapters”**.
5. Right-click on **Wireless Card bus Adapter** or **your specific network adapter**.
6. Select **Properties** to ensure that all drivers are installed properly.
7. Look under **Device Status** to see if the device is working properly.
8. Click **“OK”**.

2 What can I do if my Ethernet connection does not work properly?

- A. Make sure the RJ45 cable connects with the router.
- B. Ensure that the setting on your Network Interface Card adapter is “Enabled”.
- C. If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.
- D. If the connection still doesn’t work properly, then you can reset it to default.

3 Something wrong with the wireless connection?

- A. **Can’t setup a wireless connection?**
 - I. Ensure that the SSID and the encryption settings are exactly the same to the Clients.
 - II. Move the WiFi Broadband Router and the wireless client into the same room,

and then test the wireless connection.

- III. Disable all security settings such as **WEP**, and **MAC Address Control**.
- IV. Turn off the WiFi Broadband Router and the client, then restart it and then turn on the client again.
- V. Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.
- VI. Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- VII. If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors...

B. What can I do if my wireless client can not access the Internet?

- I. Out of range: Put the router closer to your client.
- II. Wrong SSID or Encryption Key: Check the SSID or Encryption setting.
- III. Connect with wrong AP: Ensure that the client is connected with the correct Access Point.
 - i. **Right-click** on the **Local Area Connection icon** in the taskbar.
 - ii. Select **View Available Wireless Networks in Wireless Configure**.
Ensure you have selected the correct available network.
 - iii. Reset the WiFi Broadband Router to default setting

C. Why does my wireless connection keep dropping?

- I. Antenna Orientation.
 - i. Try different antenna orientations for the WiFi Broadband Router.
 - ii. Try to keep the antenna at least 6 inches away from the wall or other objects.

- II. Try changing the channel on the WiFi Broadband Router, and your Access Point and Wireless adapter to a different channel to avoid interference.
- III. Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4 What to do if I forgot my encryption key?

1. Go back to advanced setting to set up your Encryption key again.
2. Reset the WiFi Broadband Router to default setting

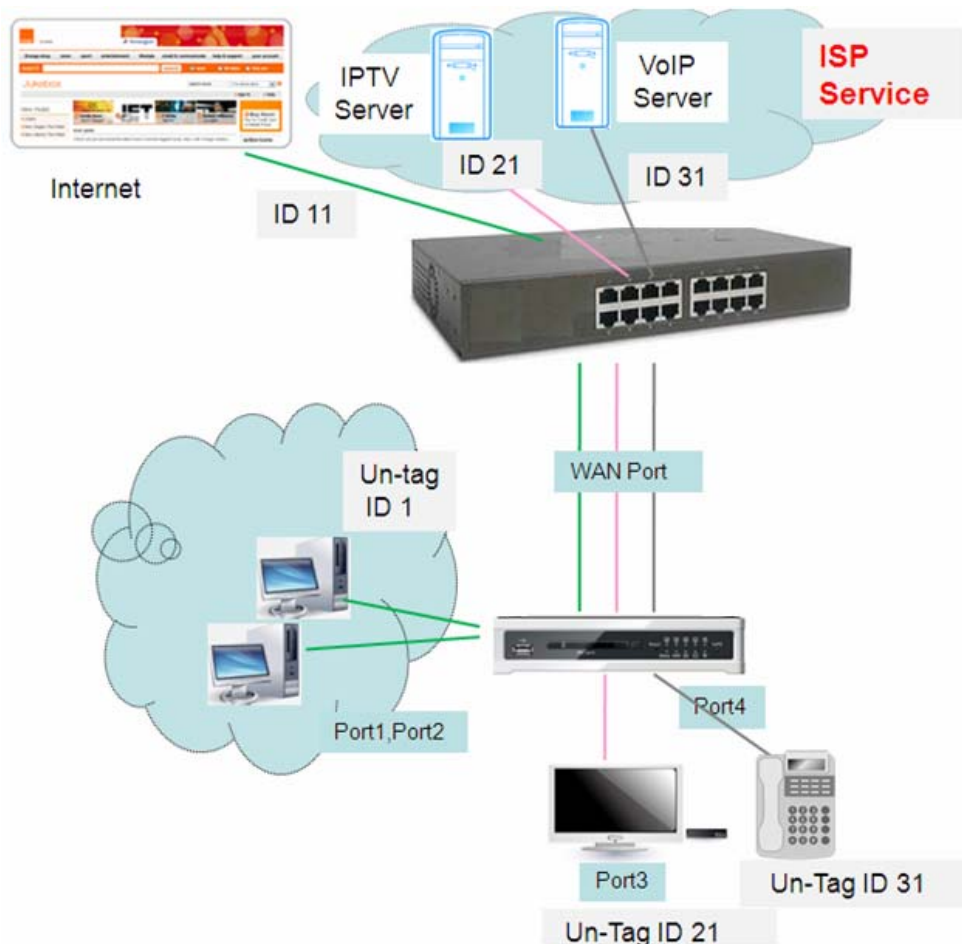
5 How to reset to default?

1. Ensure the WiFi Broadband Router is powered on
2. Find the **Reset** button on the right side
3. Press the **Reset** button for 8 seconds and then release.
4. After the WiFi Broadband Router reboots, it has back to the factory **default** settings.

CHAPTER 5 Application Description

5.1 VLAN Application

Application 1: Bundled ISP Service by Port-based VLAN Feature.



If you want to map WAN ID, you can setup WAN VLAN setting, and change router type to Bridge and add WAN Map VLAN ID to your value.

For example: The Setting as follows:

LAN VLAN Settings [HELP]						
Ethernet	Type	LAN VID	Tx TAG	DHCP Server	WAN maps VID	Edit
Port1	NAT	1	X	DHCP1/Disable 192.168.12.0/24	11	Edit
Port2	NAT	1	X	DHCP1/Disable 192.168.12.0/24	11	Edit
Port3	Bridge	X	X		21	Edit
Port4	Bridge	X	X		31	Edit

Application 2: Port-Based VLAN Feature for User Group and Guest Group

Description: User VLAN to segment 2 Groups. One is User Group, the other is Guest Group

Step1:Setup Port1~Port3 is User Group which DHCP1 and Port4 is Guest Group which DHCP2

Please Select the Operations : Port-Based VLAN

Ethernet	Type	LAN VID	Tx TAG	DHCP Server	WAN maps VID	Edit
Port1	NAT	1	X	DHCP1/Enable 192.168.12.0/24	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.12.0/24	0	Edit
Port3	NAT	1	X	DHCP1/Enable 192.168.12.0/24	0	Edit
Port4	NAT	3	X	DHCP2/Enable 192.168.2.0/24	0	Edit

VLAN ID on LAN	Membership	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port3	No	NAT	0
3	Port4	No	NAT	0

Save VLAN Routing Group

Step2: Configure and Enable DHCP2 Server

DHCP1 assigns IP Address to User Group Clients IP (192.168.12.x) and DHCP2 assigns IP Address to Guest Group Clients(192.168.2.x)

Item	Setting
DHCP Server	DHCP 2 <input checked="" type="checkbox"/> Enable
LAN IP Address	<input type="text" value="192.168.2.254"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="200"/>
Lease Time	<input type="text" value="86400"/> Seconds
Domain Name	<input type="text"/>

Save Undo More... Clients List... Fixed Mapping...

Step3: Administrator can bases on different IP subnet to setup different Access Policies with Rule-based QoS.

For example, Admin can limit the Bandwidth of guest group to 500kbps.

Scenario Selection

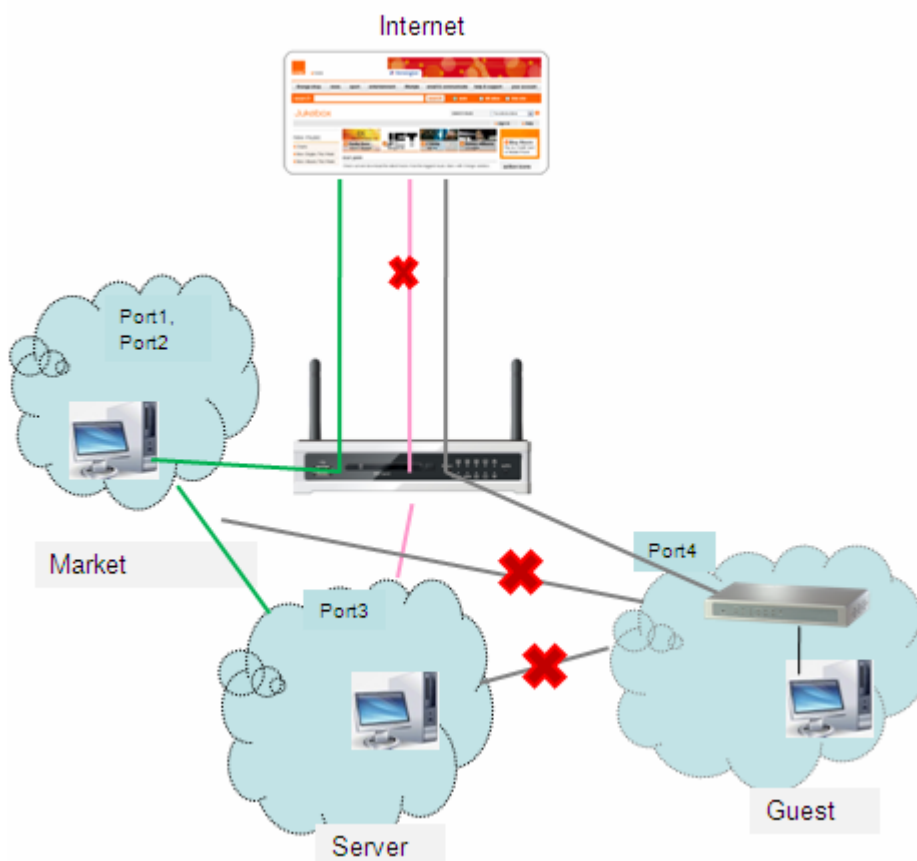
QoS Rule Setting - Rule ID11 [HELP]

Item	Setting
Rule	<input checked="" type="checkbox"/> Enable
Grouping	IP 192.168.2.2 -- 100
Service	Pre-defined Application profiles Service Type HTTP(TCP:80)
Control	MAXR 500 (KBps)
Direction	Both
Schedule	(0) Always

Save Undo

Application 3: Based on different VLAN ID to define different Access Policy.

Description: There are 3 Groups. First group is Guest and only can access Internet and can not access intranet. Second group is Market Group and can access Internet and Intranet. Third group is Server and only for Intranet.



Step1: Port-based VLAN Feature : Market is Prot1 and Port2.

Server is Port3.Guest is Port4

Please Select the Operations : Port-Based VLAN

LAN VLAN Settings [HELP]

Ethernet	Type	LAN VID	Tx TAG	DHCP Server	WAN maps VID	Edit
Port1	NAT	1	X	DHCP1/Enable 192.168.12.0/24	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.12.0/24	0	Edit
Port3	NAT	3	X	DHCP2/Disable 192.168.2.0/24	0	Edit
Port4	NAT	4	X	DHCP3/Disable 192.168.3.0/24	0	Edit

Summary

VLAN ID on LAN	Membership	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1 Port2	No	NAT	0
3	Port3	No	NAT	0
4	Port4	No	NAT	0

[Save](#) [VLAN Routing Group](#)

Step2: VLAN Routing Group : VLAN ID1(Port1 and Port2) and VLAN ID3(Port4) can access Internet.

VLAN ID1(Port1 and Port2) and VLAN ID3 (Port3) can access each other.

Summary

LAN VLAN Settings

Ethernet	Type	LAN VID	Tx TAG
Port1	NAT	1	<input type="checkbox"/>
Port2	NAT	1	<input type="checkbox"/>
Port3	NAT	3	<input type="checkbox"/>
Port4	NAT	4	<input type="checkbox"/>

VLAN Routing Group

VLAN ID on LAN	Membership	Internet Access(WAN)
1,4	PORT1, PORT2, PORT4	Allow Edit
3	PORT3	Deny
Group Access		
1,3	PORT1, PORT2, PORT3	Edit
		Edit
		Edit
		Edit

[Save](#) [Back](#)

5.2 VPN Setup

Application 1: Tablet PC or Smart Phone (Android or IOS System) establishes PPTP tunnel with Embedded PPTP Server

For example:



Select PPTP for VPN connection

Description: Give VPN a name for this connection

Server: Need the actual address or domain name. Here, please entry "118.171.154.174"(refer to the status page) or domain name.

IPv4 System Status [HELP]		
Item	WAN Status	Sidenote
IP Address	118.171.154.174	PPPoE
Subnet Mask	255.255.255.255	
Gateway	168.95.98.254	
Domain Name Server	168.95.192.1 , 168.95.1.1	
Connection Time	00:05:31	

Account and Password: Entry the specified account and password.

RSA SecureID: Skip the item for PPTP Connection.

Connect to your VPN



Application 2: Tablet PC or Smart Phone (Android System) establishes L2TP tunnel with Embedded L2TP Server

To configure L2TP on the Android device:

Go to device's 'Settings > Wireless & Networks > VPN Settings > Add VPN' and select "Add L2TP". The following window will appear:

In the opened window:

Give a VPN Name to your connection (i.e. MyVpn).

In "Set VPN server", provide your VPN-1 server FQDN (DNS name) or IP address.

IPv4 System Status [HELP]		
Item	WAN Status	Sidenote
IP Address	118.171.154.174	PPPoE
Subnet Mask	255.255.255.255	
Gateway	168.95.98.254	
Domain Name Server	168.95.192.1 , 168.95.1.1	
Connection Time	00:05:31	

Here, please entry "118.171.154.174" (refer to the status page) or domain name
 You will have to define a new password for it.

Tap on menu to save changes.

The VPN Connection will be added to your VPN Settings configuration.

Connecting to the VPN Security Gateway: Go to device's 'Settings > Wireless & Networks > VPN Settings' and select your VPN connection. The user name and Password screen appears. Enter your credentials for authentication.

Important: We don't recommend using the L2TP option in Android due to security vulnerability issues.

Application 3 : Tablet PC or Smart Phone (Android or IOS System) Establishes L2TP tunnel with Embedded L2TP/ IPsec PSK VPN Server

To configure L2TP/IPsec PSK on the Gateway:

Go to Gateway's 'Settings > Advanced Network > Security > L2TP Sever
Enable L2TP over IPsec and enter Preshare Key"1234567890"

L2TP Server	
Item	Setting
▶ VPN-L2TP Server	<input checked="" type="checkbox"/> Enable
▶ L2TP Over IPsec	<input checked="" type="checkbox"/> Enable ▶ Preshare Key <input type="text"/>

To configure L2TP/IPsec PSK on the Android device:

Select Wireless and Network or Wireless Controls, depending on your version of your device

Select VPN Settings

Select Add VPN

Select Add L2TP/IPsec PSK VPN

Select VPN Name and enter a descriptive name

Select Set VPN Server and enter a server hostname:

IPv4 System Status [HELP]		
Item	WAN Status	Sidenote
IP Address	118.171.154.174	PPPoE
Subnet Mask	255.255.255.255	
Gateway	168.95.98.254	
Domain Name Server	168.95.192.1 , 168.95.1.1	
Connection Time	00:05:31	

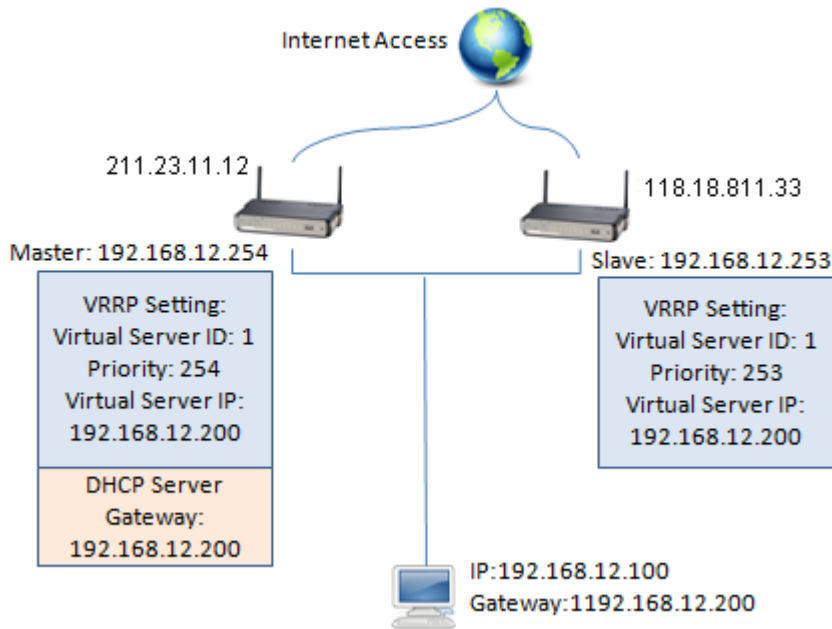
Here, please entry "118.171.154.174" (refer to the status page)

Select Set IPsec pre-shared key and enter "123456789"

Select Username and Password.

5.3 Redundancy

VRRP Setup



The Configuration of Master:

VRRP Configuration	
Item	
▶ Virtual Server ID	1 (1-255)
▶ Priority of Virtual Server	254 (1-254)
▶ Virtual Server IP Address	192.168.12.200

The Configuration of Slave:

VRRP Configuration	
Item	
▶ Virtual Server ID	1 (1-255)
▶ Priority of Virtual Server	253 (1-254)
▶ Virtual Server IP Address	192.168.12.200

※ 254 is the highest Priority

The clients under Gateway Master or Slave will get IP information from Gateway.

Appendix A. Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux Kernel	GPLv2	Linux-2.6.21
busybox	GPLv2	busybox_1.3.2
bridge-utils	GPLv2	bridge-utils 1.1
udhcp server	GPLv2	udhcp-0.9.9
udhcp client		
fdisk	GPLv2	util-linux 2.12q
mke2fs, e2fsck	GPLv2	e2fsprogs v1.40.2
samba	GNUv2	samba 3.0.20
wireless tools	GPLv2	wireless tools
vsftpd	GPLv2	vsftpd-2.0.3
Transmission	MIT	Transmission-1.74
mt-daapd	GNUv2	mt-daapd-0.2.4
dnrd	GNUv2	DNRD-2.17
libcurl		cURL-7.19.6
OpenSSL		BSD openssl-1.00b3
ntfs-3g	GNUv2	ntfs-3g-2009.4.4
Zebra	GNUv2	zebra-0.95a
snmpd		CMUsnmp-4.1.2
pptp	GNUv2	pptp-1.7.1
pppoe	GPLv2	pppoe-3.8
pppd		BSD ppp-2.4
l2tpd	GPLv2	l2tp-0.4
iptables	GNUv2	iptables-1.4.2
tc	GNUv2	iproute2-2.6.11
wget		GNU wget-1.7.1

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running

the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software

Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the Instructions , may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution:

1. This device complies with Part 15 of the FCC rules/Industry Canada RSS 210 standard . Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.
2. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.
3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE : (For Mobile Device Configuration)

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

END OF TERMS AND CONDITIONS