



DG-LB1054UV

LOAD BALANCING ROUTER WITH 2xFE WAN , 1x3G/4G

ENABLED USB, 3xFE LAN

User Manual

V1.0

2015-04-06

As our products undergo continuous development the specifications are subject to change without prior notice

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	6
1.1 PACKAGE CONTENTS	6
1.2 HARDWARE INSTALLATION.....	7
1.2.1 ATTENTION.....	7
1.2.2 SYSTEM REQUIREMENTS	7
1.2.3 Hardware Configuration.....	8
1.2.4 LED Indicators.....	9
CHAPTER 2 GETTING STARTED	10
2.1 CONNECT YOUR DEVICE.....	10
2.2 EASY SETUP BY CONFIGURING WEB UI	10
CHAPTER 3 MAKING CONFIGURATIONS.....	14
3.1 BASIC NETWORK.....	18
3.1.1 WAN Setup	18
3.1.1.1 Physical Interface.....	19
3.1.1.2 Internet Setup	20
3.1.1.3 Load Balance.....	33
3.1.2 LAN & VLAN Setup	36
3.1.2.1 Ethernet LAN.....	36
3.1.2.2 VLAN	37
3.1.2.2.1 Port-Based VLAN.....	38
3.1.2.2.2 Tag-Based VLAN.....	39
3.1.3 IPv6 Setup.....	40
3.1.3.1 Static IPv6	40
3.1.3.2 DHCP v6	42
3.1.3.3 PPPoEv6.....	43
3.1.3.4 6 to 4.....	45
3.1.3.5 IPv6 in IPv4 Tunnel.....	46
3.1.4 NAT/Bridging.....	47
3.1.4.1 NAT Loopback.....	47
3.1.4.2 Virtual Server.....	47
3.1.4.3 Virtual Computers	48
3.1.4.4 Special AP	49
3.1.4.5 DMZ	50

3.1.5	Routing Setup.....	51
3.1.5.1	Static Routing	51
3.1.5.2	Dynamic Routing.....	52
3.1.5.3	Routing Information.....	54
3.1.6	Client/Server/Proxy.....	54
3.1.6.1	Dynamic DNS	54
3.1.6.2	DHCP Server.....	55
3.2	ADVANCED NETWORK	58
3.2.1	Firewall.....	58
3.2.1.1	Packet Filters.....	59
3.2.1.2	URL Blocking.....	60
3.2.1.3	Web Content Filter	61
3.2.1.4	MAC Control.....	62
3.2.1.5	Application Filters	63
3.2.1.6	IPS.....	64
3.2.1.7	Options.....	64
3.2.2	QoS (Quality of Service).....	65
3.2.2.1	QoS Configuration.....	66
3.2.2.2	Rule-based QoS	66
3.2.2.2.1	Creating a QoS Rule based on IP Grouping	68
3.2.3	VPN Setup	71
3.2.3.1	IPSec	72
3.2.3.1.1	IPSec VPN Tunnel Scenarios.....	72
3.2.3.1.2	IPSec Configuration	74
3.2.3.1.3	Tunnel List & Status.....	74
3.2.3.1.4	Tunnel Configuration	75
3.2.3.1.5	IPSec Phase.....	75
3.2.3.1.6	IPSec Proposal Definition.....	76
3.2.3.2	PPTP.....	77
3.2.3.2.1	PPTP Server.....	77
3.2.3.2.2	PPTP Client	78
3.2.3.3	L2TP	80
3.2.3.3.1	L2TP Server.....	80
3.2.3.3.2	L2TP Client	81
3.2.3.4	GRE Tunnel.....	83
3.2.3.4.1	GRE Configuration	83
3.2.3.4.2	GRE Tunnel Definitions	83

3.2.3.4.3	GRE rule Configuration.....	84
3.2.4	<i>Redundancy</i>	85
3.2.4.1	VRRP.....	85
3.2.5	<i>System Management</i>	86
3.2.5.1	TR-069.....	86
3.2.5.2	SNMP.....	87
3.2.5.3	Telnet with CLI.....	88
3.2.5.4	UPnP.....	88
3.2.6	<i>Certificate</i>	89
3.2.6.1	My Certificates.....	89
3.2.6.2	Trusted Certificates.....	90
3.2.6.3	Issue Certificates.....	91
3.3	SYSTEM.....	91
3.3.1	<i>System Related</i>	92
3.3.2	<i>Scheduling</i>	94
3.3.3	<i>Grouping</i>	95
3.3.4	<i>External Servers</i>	96
3.3.5	<i>MMI</i>	98
3.3.5.1	Web UI.....	98
CHAPTER 4 TROUBLESHOOTING		99

Copyright

Copyright 2015 by Smartlink Network Systems Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company.

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

Trademarks

DIGISOL™ is a trademark of Smartlink Network Systems Ltd. All other trademarks are the property of the respective manufacturers.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

Chapter 1 Introduction

Congratulations on your purchase of this outstanding product DG-LB1054UV. This device is specifically designed for SMB & SOHO offices, small shops and chain stores. No matter offices are located at wire unreachable area, it can connect to Intranet of headquarter instantly via fixed line and/or cellular network. No need to apply for expensive leased line in advance. With multiple WAN load balance and fail-over, it guarantees non-interrupt operation.

By IPSec/PPTP/L2TP VPN tunneling and failover technology, it can establish a secure non-stop connection with headquarter even IP is changing all the time. Firewall protection is useful to avoid hackers attacking. With embedded robust security and firewall function, it's suitable for remote branch offices to access the corporate database & servers located in headquarter data center through internet. Besides, this device also provides VoIP feature to enable secure and cost effective Intranet voice communication through internet.

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 Package Contents

Before you start using this load balancing router, please check the following items in the package.

- DG-LB1054UV (1 No.)
- Power Adapter
- Patch Cord
- Quick installation guide
- Installation software CD (includes User Manual & QIG)

If any of the above items are missing, contact your supplier as soon as possible.

1.2 Hardware Installation

1.2.1 ATTENTION



Attention

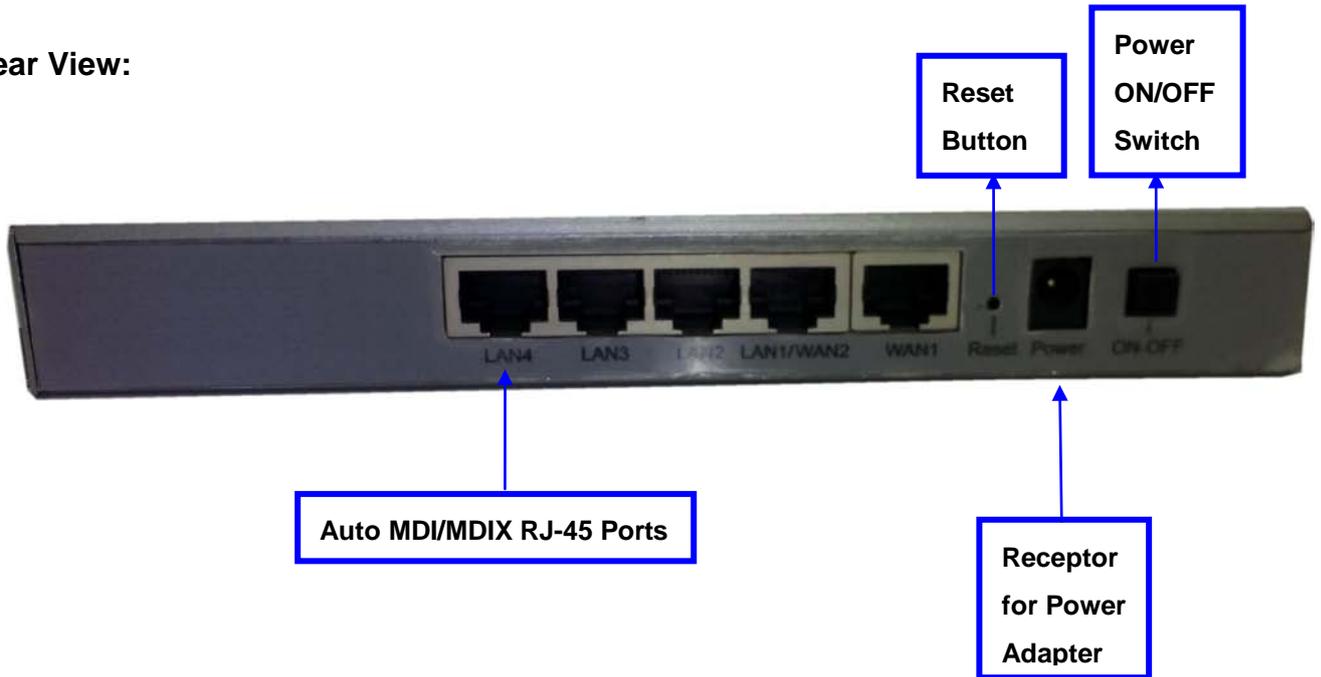
- Do not use the product in high humidity or high temperatures.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the product.
- Do not open or repair the case yourself. If the Product is too hot, turn off the power immediately and have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

1.2.2 SYSTEM REQUIREMENTS

Network Requirements	<ul style="list-style-type: none"> ● An Ethernet RJ-45 Cable or DSL modem ● 3G/4G cellular service subscription ● IEEE 802.11n or 802.11b/g wireless clients ● 10/100/1000 Ethernet adapter on PC / NB.
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.
CD Installation Wizard Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none"> ● Windows® 7 / 8, 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		OFF: Device is powered down.
		Orange: Device is booting up.
		Green(Steady): Device is powered on.
		Orange in flash: Device is in recovery mode or abnormal.
WAN		Green: Ethernet connection is established
		Green in flash: data packet transferred through WAN
		OFF: No Ethernet cable attached or Device not linked
LAN1 ~ LAN4		Green: Ethernet connection is established
		Green in flash: data packet transferred via Ethernet
		OFF: No Ethernet cable attached or Device not linked

Chapter 2 Getting Started

2.1 Connect Your Device

Before you can use this product, you need to connect your PC or NB to this gateway first. You can connect your PC to one of LAN1~LAN4 ports through an Ethernet cable. Your PC or device will get an IP address automatically after connecting to this gateway.

2.2 Easy Setup by Configuring Web UI

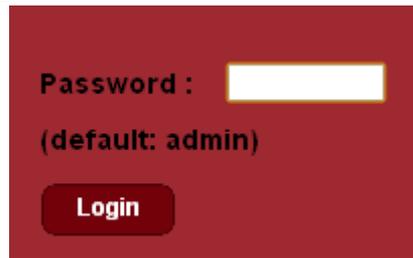
You can browse web UI to configure the device. Firstly you need to launch the Setup Wizard browser first and then the Setup Wizard will guide you step-by-step to finish the basic setup process.

Browse to Activate the Setup Wizard

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



Type the default Password ‘**admin**’ in the System Password and then click ‘**login**’ button.



Remark:

- * 1. The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to type the new IP address.
- *2. It's strongly recommending that you change this login password from default value.

Select your **language**.



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

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

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	Ethernet 1	Static IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:50:18:21:DC:C0	Disconnected	Edit
WAN-2		Disable							Edit
WAN-3	USB 3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				Edit

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
192.168.123.254	255.255.255.0		::64	Edit IPv4 Edit IPv6

3G/4G Modem Status					
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
USB 3G/4G	N/A	Disconnected	N/A	N/A	Detail

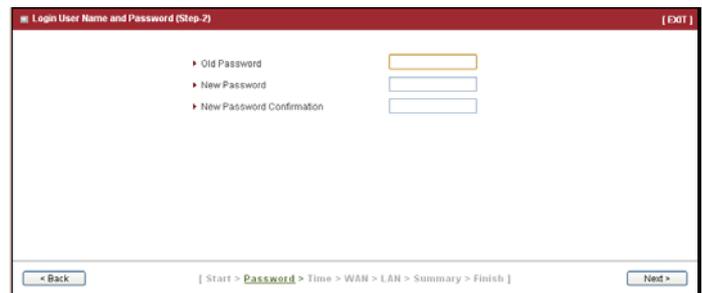
Press “Next” to start the Setup Wizard.



Configure with the Setup Wizard

Step 1

You can change the password of administrator here.



Step 2

Select Time Zone.



Step 3

Select the interface and the WAN type.



Step 4

Enter the WAN IP address, subnet mask, Gateway and the primary DNS.

Step 5

Enter the LAN IP address and Subnet Mask.

Step 6

Confirm the information as shown.

[WAN Settings]	
WAN Interface	Ethernet
WAN Type	Static IP Address
WAN IP Address	121.242.57.56
WAN Subnet Mask	255.255.255.0
WAN Gateway	121.242.57.33
Primary DNS	4.2.2.3
Secondary DNS	4.2.2.2

[Ethernet LAN Settings]	
IP Address	192.168.123.254
Subnet Mask	255.255.255.0

Step 7

Click on “Apply”. The unit will reboot. Then click on “Finish”

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 device, 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 password “admin” in the System Password and then click ‘login’ button.

DIGISOL™
Firmware Version: 00KE0.6001_03161430

Password:
(default: admin)
Login

Network Diagram: 802.11n, 802.11g, 802.11b, Client:0

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	Ethernet 1	Static IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:50:18:21:DC:C0	Disconnected	
WAN-2		Disable							
WAN-3		Disable							

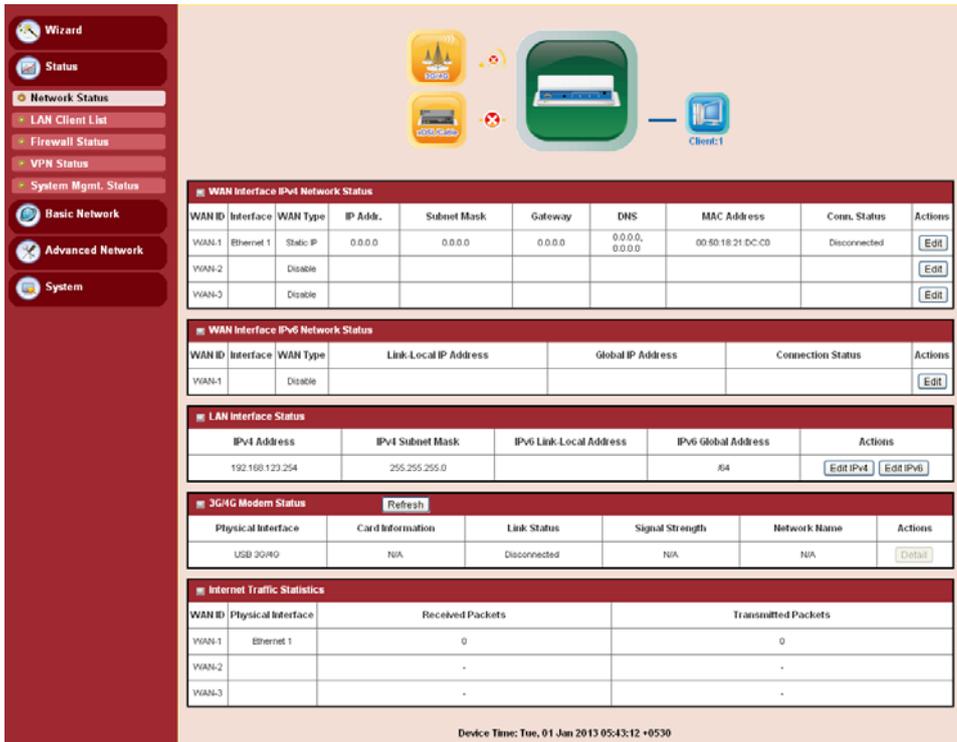
WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
192.168.123.254	255.255.255.0		/64	

3G/4G Modem Status					
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
USB 3G/4G	N/A	Disconnected	N/A	N/A	

Internet Traffic Statistics		
WAN ID	Physical Interface	Transmitted Packets
		Received Packets

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



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

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	Ethernet 1	Static IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:50:18:21:DC:C0	Disconnected	Edit
WAN-2		Disable							Edit
WAN-3		Disable							Edit

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				Edit

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
192.168.123.254	255.255.255.0		/64	Edit IPv4 Edit IPv6

3G/4G Modem Status					
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
USB 3G/4G	N/A	Disconnected	N/A	N/A	Detail

Internet Traffic Statistics			
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	Ethernet 1	0	0
WAN-2		-	-
WAN-3		-	-

You can also check status of wired clients at **LAN Client List** page, other advanced function status at **Firewall Status** page, **VPN Status** page or **System Management Status** page as shown below.

LAN Client Status List

LAN Interface	IP Address Configuration	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.123.100	savina	D0-27-88-5E-BC-F2	23:57:25

Firewall Status

Activated Filter Rule	Detected Contents	IP	Time

Activated Blocking Rule	Blocked URL	IP	Time

Activated Filter Rule	Detected Contents	IP	Time

Activated Control Rule	Blocked MAC Addresses	IP	Time

Filtered Application Category	Filtered Application Name	IP	Time

	Detected Intrusion	IP	Time

Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

VPN Status

Wizard

Status

- Network Status
- LAN Client List
- Firewall Status
- VPN Status**
- System Mgmt. Status

Basic Network

Advanced Network

System

▶ VPN Status

■ IPsec Status Edit

Tunnel Name	Tunnel Scenario	Local Subnet	Local Subnet Mask	Remote IP:FODN	Remote Subnet	Remote Subnet Mask	Status

■ PPTP Server Status Edit

User Name	Peer IP:FODN	Peer Virtual IP	Peer Call ID	Status

■ PPTP Client Status Edit

PPTP Client Name	Interface	Virtual IP	Remote IP:FODN	Default Gateway/Remote Subnet	Status

■ L2TP Server Status Edit

User Name	Peer IP:FODN	Virtual IP	Peer Call ID	Status

■ L2TP Client Status Edit

L2TP Client Name	Interface	Virtual IP	Remote IP:FODN	Default Gateway/Remote Subnet	Status

System Management Status

Wizard

Status

- Network Status
- LAN Client List
- Firewall Status
- VPN Status
- System Mgmt. Status**

Basic Network

Advanced Network

System

▶ System Mgmt. Status

■ SNMP Linking Status

User Name	IP Address	Port	Community	Auth. Mode	Privacy Mode	SNMP Version

■ SNMP Trap Information

Trap Level	Time	Trap Event

■ TR-069 Status

Link Status
Off

■ UPnP Status

Protocol	Internal Port	External Port	Action

17

1800-209-3444 (Toll Free)

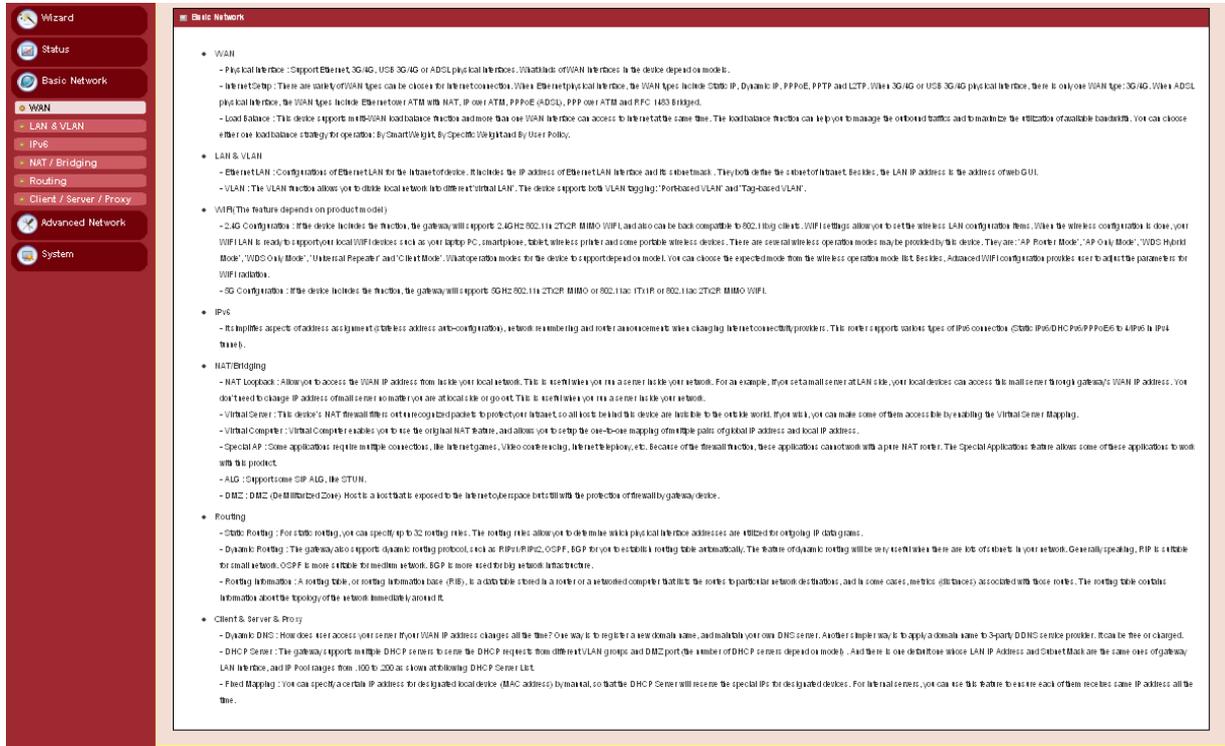
helpdesk@digisol.com

sales@digisol.com

www.digisol.com

3.1 Basic Network

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

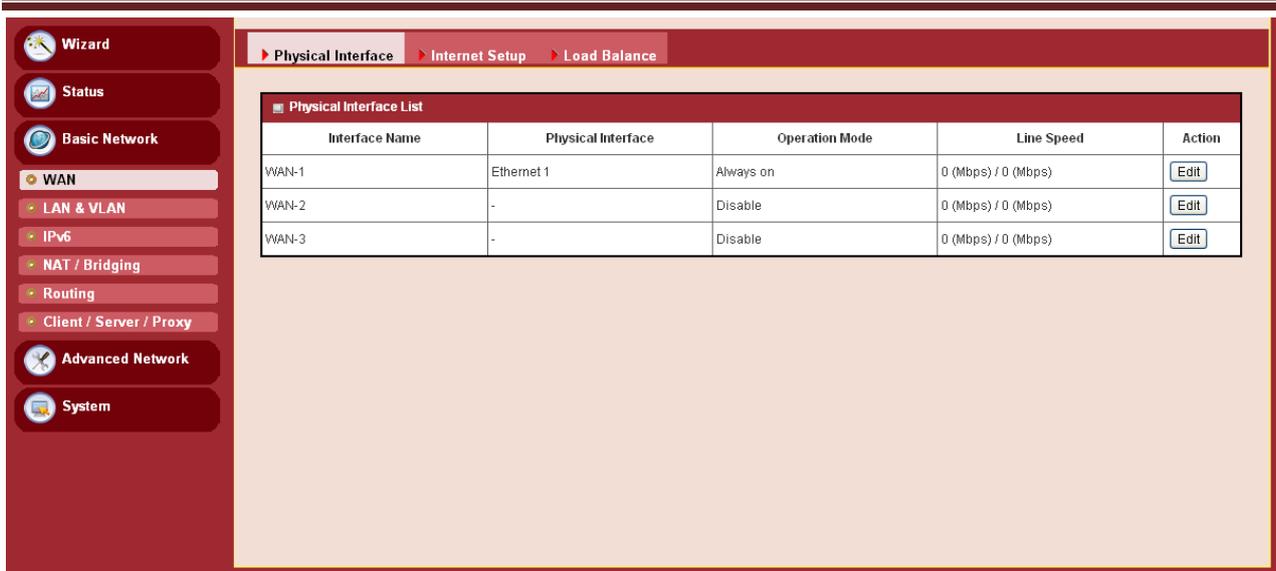


3.1.1 WAN Setup

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

USB 3G/4G WAN: The product has one USB port for 3G/4G access, please plug in your USB 3G/4G modem and follow UI setting to setup.

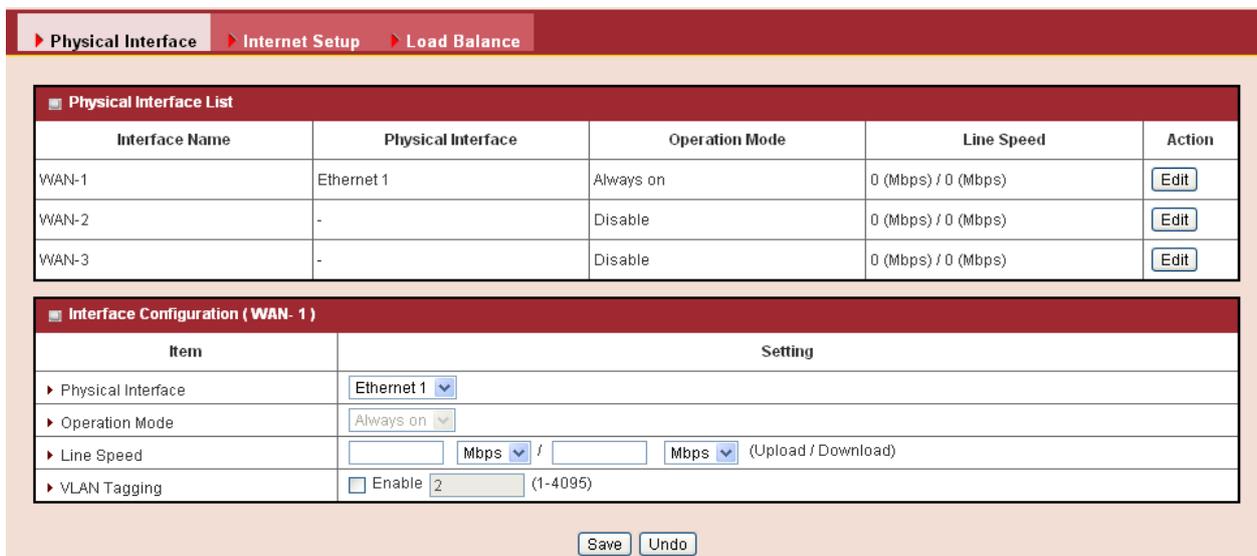
Ethernet WAN: The product has one or two RJ45 Ethernet WAN port(s). Please plug in RJ45 cable from your external DSL modem and follow UI setting to setup.



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.

By default, the WAN-1 interface is forced to “**Always-on**” mode, and operates as the primary internet connection; the interface WAN-2 / WAN-3 are disabled.



1. **Physical Interface:** Select the WAN interface from the available list. For this device, there are “Ethernet 1”, “Ethernet 2” and “3G/4G” items. If you would like the Ethernet WAN1 port to operate as the primary internet connection, Please choose “Ethernet 1”.
2. **Operation Mode:** There are three configurable items “**Always-on**”, “**Fail over**” and “**Disable**” for the operation mode setting. It decides whether the corresponding WAN interface functions as a main access or a failover access connection. If you specified a

certain WAN interface as a “**Fail over**” WAN, you have to further identify which WAN interface(s) is to be failover and fallback.

▶ Physical Interface
▶ Internet Setup
▶ Load Balance

Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet 1	Always on	0 (Mbps) / 0 (Mbps)	Edit
WAN-2	-	Disable	0 (Mbps) / 0 (Mbps)	Edit
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	Edit

Interface Configuration (WAN- 3)

Item	Setting
▶ Physical Interface	<input type="text" value="Ethernet 2"/>
▶ Operation Mode	<input type="text" value="Disable"/>
▶ Line Speed	<input type="text" value=""/> Mbps / <input type="text" value=""/> Mbps (Upload / Download)
▶ VLAN Tagging	<input type="checkbox"/> Enable <input type="text" value="3"/> (1-4095)

3. **Line Speed:** You can specify the downstream / upstream speed (Kbps) 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.
4. **VLAN Tagging:** 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 Internet Setup

There are two or three physical WAN interfaces that you can configure one by one to get proper internet connection setup. They include the Ethernet WAN(s) - the DSL ISP (Dynamic IP, Static IP, PPPoE, PPTP and L2TP connection) and the Wireless WAN - the remote wireless ISP such as 3G/4G (LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS).

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.

Physical Interface ▶ Internet Setup ▶ Load Balance				
Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet 1	Always on	Static IP	Edit
WAN-2	-	Disable	-	Edit
WAN-3	-	Disable	-	Edit
Internet Connection Configuration (WAN - 1)				
Item	Setting			
▶ WAN Type	Dynamic IP ▼			

Dynamic IP Address

Dynamic IP WAN Type Configuration	
Item	Setting
▶ Host Name	<input type="text"/> (Optional)
▶ ISP Registered MAC Address	<input type="text"/> Clone
▶ Connection Control	Auto-reconnect (Always on) ▼
▶ MTU	<input type="text"/> (0 is Auto)
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval <input type="text"/> (seconds) Check Timeout <input type="text"/> (seconds) Latency Threshold <input type="text"/> (ms) Fail Threshold <input type="text"/> (Times) Target1 <input type="text"/> Target2 <input type="text"/>
▶ IGMP	Disable ▼
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text"/>

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

- Host Name:** Optional, required by some ISPs, for example, @Home.
- ISP registered MAC Address:** Some ISP would ask you to register a MAC address for Internet connection. In this case, you need to enter the registered MAC address here, or simply press “Clone” button to copy MAC address of your PC to this field.
- Connection Control:** Select your connection control scheme from the drop list: Auto-Reconnect (always-on), Dial-on-Demand, or Manually. If selecting “Auto-Reconnect (always-on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If

choosing “Dial-on-Demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

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. **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 each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an ethernet link.
7. **WAN IP alias:** The device supports 2 WAN IP addresses for a physical interface, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote users to manage this device.

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

■ Static IP Address

Select this WAN type 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.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	Static IP
Static IP WAN Type Configuration	
Item	Setting
▶ WAN IP Address	121.242.57.56
▶ WAN Subnet Mask	255.255.255.0
▶ WAN Gateway	121.242.57.33
▶ Primary DNS	4.2.2.3
▶ Secondary DNS	4.2.2.2
▶ MTU	0 (0 is Auto)
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval: 3 (seconds) Check Timeout: 3 (seconds) Latency Threshold: 3000 (ms) Fail Threshold: 10 (Times) Target1: DNS1 Target2: None
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

- 1. WAN IP address / Subnet Mask / Gateway:** Enter the IP address, subnet mask, and gateway address, provided to you by your ISP.
- 2. Primary DNS / Secondary DNS:** Input the Primary/Secondary DNS if necessary.
- 3. MTU:** Most ISP offers MTU value to users. The default value is 0 (auto)
- 4. NAT:** If you enable this option, it will act with a non-NAT function.
- 5. 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.
- 6. WAN IP alias:** The device supports 2 WAN IP addresses for a physical interface, 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.

■ PPP over Ethernet

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

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	PPPoE
PPPoE WAN Type Configuration	
Item	Setting
▶ IPv6 Dual Stack	<input type="checkbox"/> Enable
▶ PPPoE Account	<input type="text"/>
▶ PPPoE Password	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Connection Control	Auto-reconnect (Always on)
▶ Service Name	<input type="text"/> (Optional)
▶ Assigned IP Address	<input type="text"/> (Optional)
▶ MTU	0 (0 is Auto)
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval <input type="text" value="3"/> (seconds) Check Timeout <input type="text" value="3"/> (seconds) Latency Threshold <input type="text" value="3000"/> (ms) Fail Threshold <input type="text" value="10"/> (Times) Target1 <input type="text" value="DNS1"/> Target2 <input type="text" value="None"/>
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

- IPv6 Dual Stack:** You can enable this option if your ISP provides not only one IPv4 but also one IPv6 address.
- PPPoE Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.
- Primary DNS / Secondary DNS:** In most cases, ISP will assign DNS server automatically after PPPoE connection is established. Input the IP address of primary and secondary DNS server manually if required.
- Connection Control:** Select your connection control scheme from the drop list: Auto-Reconnect (always-on), Dial-on-Demand, or Manually. If selecting "Auto-Reconnect (always-on)", this gateway will start to establish Internet connection automatically since it's powered on. It's recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing "Dial-on-Demand", this gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect

WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

5. **Service Name / Assigned IP Address:** ISP may ask you to use a specific service name when connecting PPPoE connection. In some cases, ISP can also provide you a fixed IP address with PPPoE connection. For these cases, you need to add that information in this field.
6. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0. (auto)
7. **NAT :** If you enable this option, there will be no NAT mechanism between LAN side and WAN side.
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. **WAN IP alias:** The device supports 2 WAN IP addresses for a physical interface, 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.

■ PPTP

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

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	PPTP
PPTP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address
▶ Server IP Address / Name	
▶ PPTP Account	
▶ PPTP Password	
▶ Connection ID	(Optional)
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	0 (0 is Auto)
▶ MPPE	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval: 3 (seconds) Check Timeout: 3 (seconds) Latency Threshold: 3000 (ms) Fail Threshold: 10 (Times) Target1: DNS1 Target2: None
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

- 1. WAN Type:** Choose “PPTP” 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 “My IP Address”, “My Subnet Mask”, and “Gateway IP” settings provided by your ISP.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	PPTP
PPTP WAN Type Configuration	
Item	Setting
▶ IP Mode	Static IP Address
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<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)
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	0 (0 is Auto)
▶ MPPE	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval <input type="text" value="3"/> (seconds) Check Timeout <input type="text" value="3"/> (seconds) Latency Threshold <input type="text" value="3000"/> (ms) Fail Threshold <input type="text" value="10"/> (Times) Target1 <input type="text" value="DNS1"/> Target2 <input type="text" value="None"/>
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

- 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. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.
- 5. Connection ID:** Optional, input the connection ID if your ISP requires it.
- 6. Connection Control:** Select your connection control scheme from the drop list: Auto-Reconnect (always-on), Dial-on-Demand, or Manually. If selecting "Auto-Reconnect (always-on)", this gateway will start to establish Internet connection automatically since it's powered on. It's recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing "Dial-on-Demand", this gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing "Manually", this gateway won't start to establish WAN connection until you press "Connect" button on web UI. After that, this gateway will disconnect WAN connection

if idle time reaches value of Maximum Idle Time.

7. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0. (auto)
8. **NAT :** If you enable this option, there will be no NAT mechanism between LAN side and WAN side.
9. **MPPE (Microsoft Point-to-Point Encryption):** Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.
10. **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 to each of the interfaces, which multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
11. **WAN IP alias:** The device supports 2 WAN IP addresses for a physical interface, 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.

■ L2TP

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

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	L2TP

L2TP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address
▶ Server IP Address / Name	
▶ L2TP Account	
▶ L2TP Password	
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	0 (0 is Auto)
▶ Service Port	User-defined 1702
▶ MPPE	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval: 3 (seconds) Check Timeout: 3 (seconds) Latency Threshold: 3000 (ms) Fail Threshold: 10 (Times) Target1: DNS1 Target2: None
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

- 1. 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.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	L2TP
L2TP WAN Type Configuration	
Item	Setting
▶ IP Mode	Static IP Address
▶ WAN IP Address	<input type="text"/>
▶ WAN Subnet Mask	<input type="text"/>
▶ WAN Gateway	<input type="text"/>
▶ Server IP Address / Name	<input type="text"/>
▶ L2TP Account	<input type="text"/>
▶ L2TP Password	<input type="text"/>
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	0 (0 is Auto)
▶ Service Port	User-defined 1702
▶ MPPE	<input type="checkbox"/> Enable
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval <input type="text" value="3"/> (seconds) Check Timeout <input type="text" value="3"/> (seconds) Latency Threshold <input type="text" value="3000"/> (ms) Fail Threshold <input type="text" value="10"/> (Times) Target1 <input type="text" value="DNS1"/> Target2 <input type="text" value="None"/>
▶ IGMP	Disable
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text" value="10.0.0.1"/>

2. **Server IP Address / Name:** The IP address of the L2TP server and designated Gateway provided by your ISP.
3. **L2TP Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.
4. **Connection Control:** Select your connection control scheme from the drop list: Auto-Reconnect (always-on), Dial-on-Demand or Manually. If selecting "Auto-Reconnect (always-on)", this gateway will start to establish Internet connection automatically since it's powered on. It's recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing "Dial-on-Demand", this gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing "Manually", this gateway won't start to establish WAN connection until you press "Connect" button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

5. **MTU:** Most ISP offers MTU values to users. The default MTU value is 0 (auto)
6. **MPPE** (Microsoft Point-to-Point Encryption): Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.
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. **WAN IP alias:** The device supports 2 WAN IP addresses for a physical interface, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that lets remote users to manage this device.

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

■ 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.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet 1	Always on	Static IP	Edit
WAN-2	-	Disable	-	Edit
WAN-3	USB 3G/4G	Failover	3G/4G	Edit

Internet Connection Configuration (WAN - 3)	
Item	Setting
▶ WAN Type	3G/4G

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A

Connection with SIM-A Card	
Item	Setting
▶ Dial-up Profile	<input type="radio"/> Auto-detection <input checked="" type="radio"/> Manual-configuration
▶ Country	India
▶ Service Provider	Vodafone
▶ APN	www (Optional)
▶ PIN Code	(Optional)
▶ Dial Number	*99#
▶ Account	(Optional)
▶ Password	(Optional)
▶ Authentication	Auto
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)
▶ Roaming	<input type="checkbox"/> Enable

Connection Common Configuration	
Item	Setting
▶ Time Schedule	(0) Always
▶ MTU	0 (0 is Auto)
▶ NAT	<input checked="" type="checkbox"/> Enable
▶ Network Monitoring	<input checked="" type="checkbox"/> Enable <input type="radio"/> DNS Query <input checked="" type="radio"/> ICMP Checking <input type="checkbox"/> Loading Check Check Interval: 3 (seconds) Check Timeout: 3 (seconds) Latency Threshold: 3000 (ms) Fail Threshold: 10 (Times) Target1: DNS1 Target2: None
▶ WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

- 1. WAN Type:** Choose “3G/4G” from the drop list
- 2. Dial-up Profile:** After you subscribe 3G/4G data service, your operator will provide some information for you to setup connection, such as APN, dialed number, account, or password. If you know this information exactly, you can choose “Manual” setting and type in that information by your own. Otherwise, you can select “Auto-Detection” to let this gateway detect automatically. Even you choose “Manual” setting, this gateway will

show responding information for your reference after you select country and service provider.

3. **Service Provider:** Select the service provider from the drop down list.
4. **PIN Code:** Enter the PIN Code for your SIM card.(Optional)
5. **Dial Number:** Enter the dial number that is provided by your ISP.
6. **Account/Password:** Enter the account / Password that is provided by your ISP(Optional).
7. **Authentication:** Choose “auto”, “PAP”, or “CHAP” according to your ISP’s authentication approach.
8. **Primary / Secondary DNS:** Enter IP address of Domain Name Server (Optional). You can keep them in blank, because most ISP will assign them automatically.
9. **Time Schedule:** This option allows you to limit WAN connection available in a certain time period. You can select “Always” available or “By Schedule” for connection method. If you choose “By Schedule” rule, you need to add a new schedule at **System -> Scheduling** menu.
10. **MTU:** MTU refers to Maximum Transmit Unit. Different WAN types of connection will have different value. You can leave it with 0 (Auto) if you are not sure about this setting.
11. **NAT:** Check mark this fiels to enable this feature.

3.1.1.3 Load Balance

This device supports multi-WAN load balance function and more than one WAN interfaces can access to Internet at a time. The load balance function can help you to manage the outbound traffics and to maximize the utilization of available bandwidth.

Item	Setting
▶ Load Balance	<input type="checkbox"/> Enable
▶ Load Balance Strategy	By Smart Weight ▼

Save Undo

1. **Load Balance:** Enable or disable the load balance function.
2. **Load Balance Strategy:** Once you enabled the load balance function, you have to further configure which strategy is to be applied for load balancing the outbound traffics. There are three load balance strategies: “By Smart Weight”, “By Priority” and “By User Policy”.

By Smart Weight:

Physical Interface > Internet Setup > Load Balance

Configuration	
Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By Smart Weight

Save Undo

If you choose the “**By Smart Weight**” strategy, no other setting is required. This device will automatically allocate the outbound traffics to each WAN interface.

By Priority:

Physical Interface > Internet Setup > Load Balance

Configuration	
Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By Priority

Priority Definition		
WAN ID	Priority (%)	Action
WAN - 1	100%	Edit

Save Undo

1. **Priority:** If you choose the “**By Priority**” strategy, you have to further specify the outbound traffic percentage for each WAN interface. The load balancing mechanism will follow these settings to allocate proper traffic for each WAN to access the internet.

By User Policy:

Physical Interface > Internet Setup > Load Balance

Configuration	
Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By User Policy

User Policy List						
ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

Add Delete

Save Undo

If you choose the “**By User Policy**” strategy, you have to further create the expected policies one by one. Click the “**add**” button to add your load balance policy.

You can manage the outbound traffics flow and the force specific traffics to access Internet through designated WAN interface. For those traffics not covered in the user policy rules, the device will allocate the WAN interface by applying “Smart Weight” mechanism simultaneously.

▶ Physical Interface
▶ Internet Setup
▶ Load Balance

■ Configuration

Item	Setting
▶ Load Balance	<input checked="" type="checkbox"/> Enable
▶ Load Balance Strategy	By User Policy ▼

■ User Policy List
Add Delete

ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions

■ User Policy Configuration

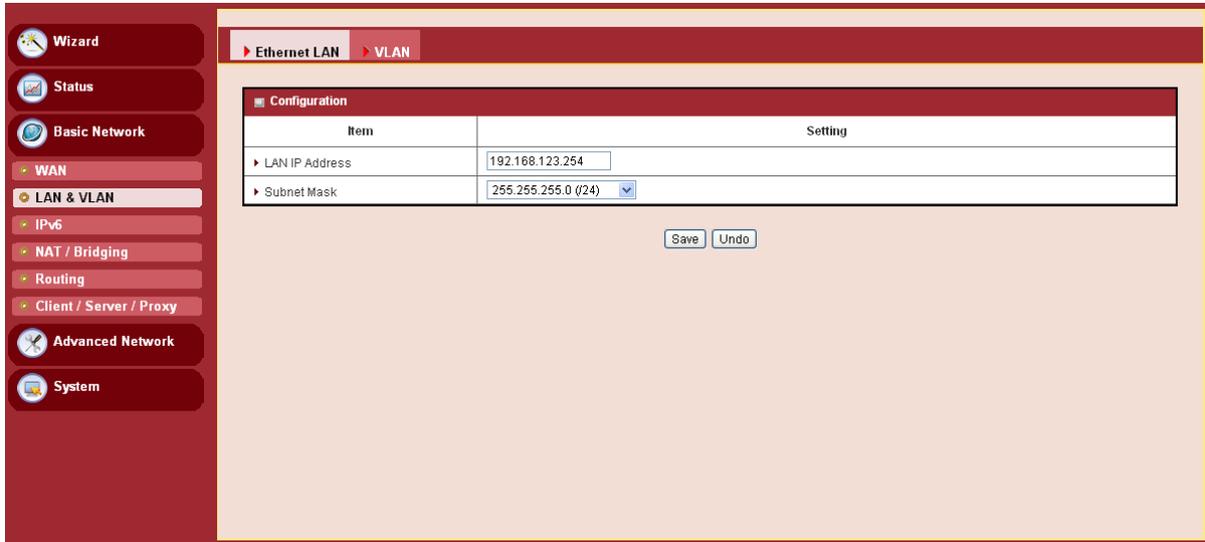
Item	Setting
▶ Source IP Address	Any ▼
▶ Destination IP Address	Any ▼
▶ Destination Port	All ▼
▶ Protocol	Both ▼
▶ WAN Interface	WAN - 1 ▼
▶ Policy	<input type="checkbox"/> Enable

Save
Undo

1. **Source IP Address:** Enter the expected Source IP Address for the load balance policy. It can be “Any”, “Subnet”, “IP Range”, or “Single IP”. Just choose one type of the source IP address, and specify its value as well. If you don’t want to specify a certain source IP address for this policy, just leave it as “Any”.
2. **Destination IP Address:** Enter the expected Destination IP Address and / or the Port number for the load balance policy. It can be “Any”, “Subnet”, “IP Range”, “Single IP”, or “Domain Name”. Just choose one type of the destination IP address, and specify its value as well. If you don’t want to specify a certain destination IP address for this policy, just leave it as “Any”
3. **Destination Port:** Enter the expected Destination Port number for the load balance policy. It can be “All”, “Port Range”, “Single Port”, or “Well-known Applications”. Just choose one type of the destination port, and specify its value as well. If you don’t want to specify a certain destination port for this policy, just leave it as “All”
4. **Protocol:** Enter the expected protocol type for the load balance policy. It can be “TCP”, “UDP”, or “Both”. If you don’t want to specify a certain protocol type for this policy, just leave it as “Both”
5. **WAN Interface:** Identify which WAN interface is to be selected for accessing the Internet if all of above source and destination criteria are matched for the outbound traffics.
6. **Policy:** Enable or disable this user policy.

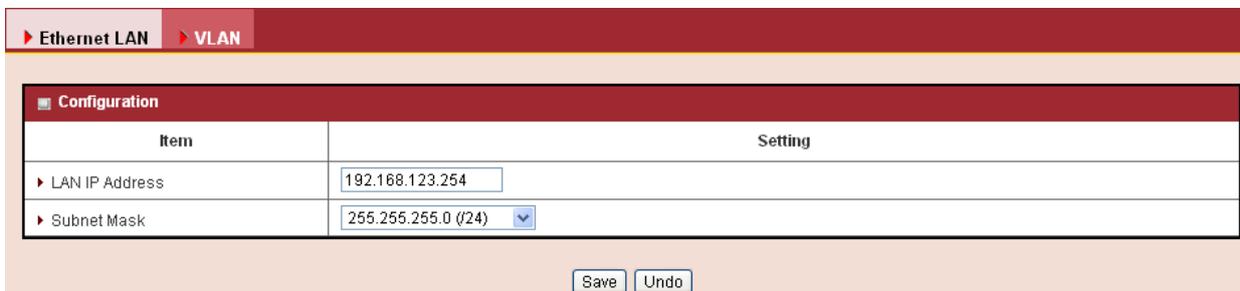
3.1.2 LAN & VLAN Setup

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 Ethernet LAN

Please follow the below mentioned instructions to do IPv4 Network Setup.



1. **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. It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.
2. **Subnet Mask:** Input your Subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0, and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway. So there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

255.0.0.0 (/8)
255.128.0.0 (/9)
255.192.0.0 (/10)
255.224.0.0 (/11)
255.240.0.0 (/12)
255.248.0.0 (/13)
255.252.0.0 (/14)
255.254.0.0 (/15)
255.255.0.0 (/16)
255.255.128.0 (/17)
255.255.192.0 (/18)
255.255.224.0 (/19)
255.255.240.0 (/20)
255.255.248.0 (/21)
255.255.252.0 (/22)
255.255.254.0 (/23)
255.255.255.0 (/24)
255.255.255.128 (/25)
255.255.255.192 (/26)
255.255.255.224 (/27)
255.255.255.240 (/28)
255.255.255.248 (/29)
255.255.255.252 (/30)

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

3.1.2.2 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 forms a logical Ethernet segment. There are four LAN ports for this device, so you can have various VLAN configurations to organize the available LAN ports if required.

▶ Ethernet LAN
▶ VLAN

■ Configuration
[Help]

Item	Setting
▶ VLAN Type	Port-based

■ Port-based VLAN List

Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
Port1	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	3	Edit
Port2	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	Edit
Port3	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	Edit
Port4	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	Edit

■ Port-based VLAN Summary

VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag
1	Port1, Port2, Port3, Port4	NAT	DHCP 1	X	No

Save VLAN Routing Group

By default, all the 4 LAN ports 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. **VLANID:** 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 VID:** The VLAN Tag ID that comes 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.

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 VLANs 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.

▶ Ethernet LAN ▶ VLAN

■ Configuration [Help]

Item	Setting
▶ VLAN Type	Tag-based ▼

■ Tag-based VLAN List Add Delete

VLAN ID	Internet	Port	DHCP Server	Actions
None	<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4	DHCP 1	Edit

<< Previous
Next >>

■ Tag-based VLAN Summary

Port	VLAN IDs
Port1	
Port2	
Port3	
Port4	

Apply

By default, all the LAN ports and virtual APs belong to one VLAN, and this VLAN ID is forced to “1”. It is a special tag based VLAN for device to operate, 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 packets will be un-tagged before it is forwarded to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forwarded that the destination belongs to this configuring VLAN group.
3. **Port 1 ~ Port 4:** Specify whether it belongs 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.

3.1.3 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 what type of IPv6 is supported before you proceed with IPv6 setup.**

3.1.3.1 Static IPv6

The screenshot shows the following configuration details:

Item	Setting
IPv6	<input checked="" type="checkbox"/> Enable
WAN Connection Type	Static IPv6

Static IPv6 WAN Type Configuration	
IPv6 Address	<input type="text"/>
Subnet Prefix Length	<input type="text"/>
Default Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
MLD Snooping	<input checked="" type="checkbox"/> Enable

WAN Connection Options	
DS-Lite	<input checked="" type="checkbox"/> Enable AFTR IPv6 Address <input type="radio"/> Static <input type="text"/> <input checked="" type="radio"/> Dynamic

LAN Configuration	
Global Address	<input type="text"/> /64
Link-local Address	<input type="text"/>

Address Auto-configuration	
Auto-configuration	<input checked="" type="checkbox"/> Enable
Auto-configuration Type	Stateless
Router Advertisement Lifetime	200 (seconds)

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

WAN IPv6 address settings:

- 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”

2. **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.
3. **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.
4. **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.
5. **MLD Snooping:** Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.
6. **Ds-Lite:** Dual-Stack Lite (DS-Lite, allows a service provider to share existing IPv4 address space and support both IPv6 and IPv4 clients utilizing an IPv6 infrastructure. This allows for preservation of the IPv4 address space by reclaiming addresses from the access network as it migrates to IPv6, and sharing the existing IPv4 addresses among its customer base. Unlike other migration strategies, DS-Lite combines both tunneling and network address translation technologies, and decouples the service provider's access network from the public internet. These features can simplify the migration to IPv6 by allowing incremental IPv6 deployment within the service provider's network while continuing to support legacy IPv4 clients.
7. **Global Address:** is assigned to a computer or modem by an internet service provider and can be communicated with from anywhere on the internet. Global IP addresses are unique and assigned only to a single computer or device.
8. **Link local address:** A link-local address is a network address that is valid only for communications within the network segment (link) or the broadcast domain that the host is connected to.

Address auto configuration settings:

7. **Auto-configuration:** Disable or enable this auto configuration setting.
8. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
9. **Router advertisement Lifetime:** You can set the time for the period that the router sends (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.

3.1.3.2 DHCP v6

Configuration	
IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	<input checked="" type="checkbox"/> Enable
▶ WAN Connection Type	DHCPv6
DHCPv6 WAN Type Configuration	
▶ DNS	<input checked="" type="radio"/> From Server <input type="radio"/> Specific DNS
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable
WAN Connection Options	
▶ DS-Lite	<input type="checkbox"/> Enable AFTR IPv6 Address <input type="radio"/> Static <input type="text"/> <input checked="" type="radio"/> Dynamic
LAN Configuration	
▶ Global Address	<input type="text"/>
▶ Link-local Address	<input type="text"/>
Address Auto-configuration	
▶ Auto-configuration	<input checked="" type="checkbox"/> Enable
▶ Auto-configuration Type	Stateless
▶ Router Advertisement Lifetime	200 (seconds)

Save Undo

When “DHCPv6” is selected you need to do the following settings:

- 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.
- LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

Address auto configuration settings:

3. **Auto-configuration:** Disable or enable this auto configuration setting.
4. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
5. **Router advertisement Lifetime:** You can set the time for the period that the router sends (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.

3.1.3.3 PPPoEv6

▶ Configuration

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	<input checked="" type="checkbox"/> Enable
▶ WAN Connection Type	PPPoEv6 ▾

PPPoEv6 WAN Type Configuration	
▶ Account	<input type="text"/>
▶ Password	<input type="text"/>
▶ Service Name	<input type="text"/>
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

LAN Configuration	
▶ Global Address	<input type="text"/>
▶ Link-local Address	<input type="text"/>

Address Auto-configuration	
▶ Auto-configuration	<input checked="" type="checkbox"/> Enable
▶ Auto-configuration Type	Stateless ▾
▶ Router Advertisement Lifetime	<input type="text" value="200"/> (seconds)

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

WAN IPv6 address settings:

1. **Account:** Enter the Username that you got from your ISP
2. **Password:** Enter the Password that you got from your ISP
3. **Service Name:** Enter the Service Name that you got from your ISP
4. **Connection Control:** Leave the setting as “Auto Reconnect (always-on)”
5. **MTU (Maximum Transmission Unit):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
6. **MLD Snooping:** Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.
7. **LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

Address auto configuration settings:

8. **Auto-configuration:** Disable or enable this auto configuration setting.
9. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
10. **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.

3.1.3.4 6 to 4

▶ Configuration

■ IPv6 Configuration
[Help]

Item	Setting
▶ IPv6	<input checked="" type="checkbox"/> Enable
▶ WAN Connection Type	6to4

■ 6to4 WAN Type Configuration

▶ 6 to 4 Address	
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable

■ LAN Configuration

▶ Global Address	2002:0:0: <input type="text"/> ::1
▶ Link-local Address	

■ Address Auto-configuration

▶ Auto-configuration	<input checked="" type="checkbox"/> Enable
▶ Auto-configuration Type	Stateless
▶ Router Advertisement Lifetime	<input type="text" value="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 you need to send Router advertisement messages periodically.

3.1.3.5 IPv6 in IPv4 Tunnel

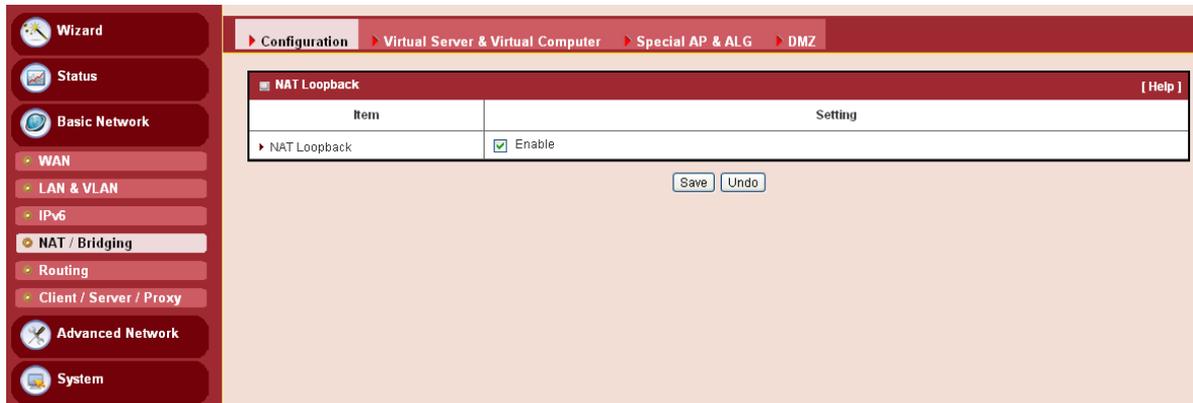
Configuration	
IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	<input checked="" type="checkbox"/> Enable
▶ WAN Connection Type	6in4
6in4 WAN Type Configuration	
▶ Remote IPv4 Address	<input type="text"/>
▶ Local IPv4 Address	0.0.0.0
▶ Local IPv6 Address	<input type="text"/> /64
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ MLD Snooping	<input type="checkbox"/> Enable
LAN Configuration	
▶ Global Address	<input type="text"/> /64
▶ Link-local Address	<input type="text"/>
Address Auto-configuration	
▶ Auto-configuration	<input checked="" type="checkbox"/> Enable
▶ Auto-configuration Type	Stateless
▶ Router Advertisement Lifetime	200 (seconds)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

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

- 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.
- LAN IPv6 address setting:** LAN IPv6 address and LAN IPv6 Link-Local address.
- 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.

3.1.4 NAT/Bridging

3.1.4.1 NAT Loopback



Allows you to access the WAN IP address from inside your local network. This is useful when you run a server inside your network. For an example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's WAN IP address. You don't need to change the IP address of mail server no matter you are at local side or go out. This is useful when you run a server inside your network.

3.1.4.2 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 users more flexibility on Access control. For the details, please refer to **Scheduling Rule**.

Configuration > Virtual Server & Virtual Computer > Special AP & ALG > DMZ

Virtual Server Rule Configuration

Item	Setting
Public Port	User-defined Service <input type="text"/>
Server IP	<input type="text"/>
Private Port	<input type="text"/>
Protocol	Both
Time Schedule	Always
Rule	<input type="checkbox"/> Enable

Save Undo Back

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.

3.1.4.3 Virtual Computers

Virtual Computer List Add Delete

ID	Global IP	Local IP	Enable	Actions
	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	

Virtual Computer Rule Configuration [Help]

Global IP	Local IP	Enable
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save

Save Undo

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.

- 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.

3.1.4.4 Special AP

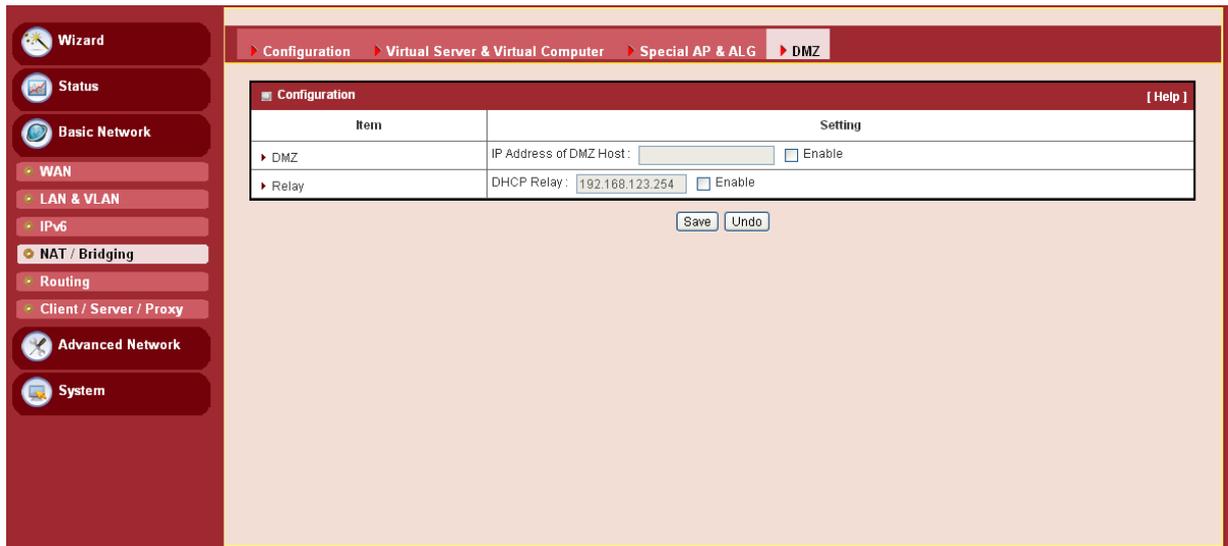
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. 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 Port:** 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. **Time Schedule:** Each special AP setting can be turned 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.

3.1.4.5 DMZ



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. Otherwise, if specific application is blocked by NAT mechanism, you can indicate the LAN computer as a DMZ host to solve this problem.

NOTE: This feature should be used only when needed.

3.1.5 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.

The screenshot shows the 'Static Routing' configuration page. The left sidebar has a 'Routing' menu item highlighted. The main content area has a breadcrumb trail: Static Routing > Dynamic Routing > Routing Information. Below this is a 'Configuration' section with a table:

Item	Setting
Static Routing	<input type="checkbox"/> Enable

Below the configuration table is a 'Static Routing Rule List' section with 'Add' and 'Delete' buttons. It contains a table with the following columns: ID, Destination IP, Subnet Mask, Gateway, Interface, Metric, Enable, and Actions. Below the table are 'Save' and 'Undo' buttons.

3.1.5.1 Static Routing

The screenshot shows the 'Static Routing Rule Configuration' page. The breadcrumb trail is: Static Routing > Dynamic Routing > Routing Information. The main content area has a 'Static Routing Rule Configuration' section with a table:

Item	Setting
Destination IP	<input type="text"/>
Subnet Mask	<input type="text"/>
Gateway IP	<input type="text"/>
Interface	Auto <input type="button" value="v"/>
Metric	<input type="text"/>
Rule	<input type="checkbox"/> Enable

Below the table are 'Save', 'Undo', and 'Back' buttons.

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 datagrams. 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.

1. **Destination:** Enter the subnet network of routed destination.
2. **Subnet Mask:** Input your Subnet mask. Subnet mask defines the range of IP address in destination network.
3. **Gateway IP:** The IP address of gateway that you want to route for this destination subnet network. The assigned gateway needs in the same subnet of LAN side or WAN

side.

- Metric:** The number of router/gateway between this device and assigned gateway.

Static Routing Rule List Add Delete							
ID	Destination IP	Subnet Mask	Gateway	Interface	Metric	Enable	Actions
1	10.10.10.0	255.255.255.0	192.168.123.254	Auto	1	<input checked="" type="checkbox"/>	Edit Select

Save Undo

With above example, every packet goes to IP addresses 10.10.10.1~10.10.10.254 will be sent to 192.168.123.250 first.

3.1.5.2 Dynamic Routing

The feature of static route is for you to maintain routing table manually. In addition, this gateway also supports dynamic routing protocol, such as RIPv1/RIPv2, OSPF, BGP for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

Static Routing Dynamic Routing Routing Information

Static Routing Dynamic Routing Routing Information

RIP Configuration [Help]

Item	Setting
▶ RIP	Disable

OSPF Configuration

Item	Setting
▶ OSPF	<input checked="" type="checkbox"/> Enable
▶ Backbone Subnet	<input type="text"/>

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions

BGP Configuration
BGP Neighbor List Add Delete
BGP Neighbor Configuration
Save Undo

- RIP:** 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.

- 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.

OSPF Configuration	
Item	Setting
▶ OSPF	<input checked="" type="checkbox"/> Enable
▶ Backbone Subnet	<input type="text"/>

OSPF Area List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Area Subnet	Area ID	Enable	Actions

You can enable the OSPF routing function by clicking 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.

- 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.

BGP Configuration	
Item	Setting
▶ BGP	<input checked="" type="checkbox"/> Enable
▶ Self ID	<input type="text"/>

BGP Neighbor List <input type="button" value="Add"/> <input type="button" value="Delete"/>				
ID	Neighbor IP	Neighbor ID	Enable	Actions

BGP Neighbor Configuration	
Item	Setting
▶ Neighbor IP	<input type="text"/>
▶ Neighbor ID	<input type="text"/>
▶ Neighbor	<input type="checkbox"/> Enable

You can enable the BGP routing function by clicking 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.

3.1.5.3 Routing Information

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.

3.1.6 Client/Server/Proxy

Domain Name	IP Address	Definition Enable	Actions
[Add] [Delete]			

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

[Save] [Undo]

3.1.6.1 Dynamic DNS

How does user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to 3-party DDNS service provider. It can be free or charged.

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.

Dynamic DNS > DHCP Server

Pre-defined Domain Name List

Domain Name	IP Address	Definition Enable	Actions
Dynamic DNS [Help]			
Item	Setting		
DDNS	<input checked="" type="checkbox"/> Enable		
Provider	DynDNS.org(Dynamic) ▾		
Host Name	<input type="text"/>		
Username / E-mail	<input type="text"/>		
Password / Key	<input type="text"/>		

- DDNS:** Select enable if you would like to trigger this function.
 - 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.
 - Host Name:** Register a domain name to the DDNS provider. The full domain name is concatenated with hostname(you specify) and a suffix(DDNS provider specifies).
 - Username/E-mail:** Input username or E-mail based on the DDNS provider you select.
 - 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.

3.1.6.2 DHCP Server

Dynamic DNS > DHCP Server

DHCP Server List

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Server Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>

- DHCP Server:** Choose DHCP Server to **Enable**. If you enable the DHCP Server function, this gateway will assign IP address to LAN computers or devices through DHCP protocol. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
- LAN IP Address:** Specify the local IP address of the enabled DHCP Server. It’s the LAN IP address of this gateway. Normally, this IP address will be also the default gateway of local computers and devices.

3. Subnet Mask: Input your Subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0, and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

255.0.0.0 (/8)
255.128.0.0 (/9)
255.192.0.0 (/10)
255.224.0.0 (/11)
255.240.0.0 (/12)
255.248.0.0 (/13)
255.252.0.0 (/14)
255.254.0.0 (/15)
255.255.0.0 (/16)
255.255.128.0 (/17)
255.255.192.0 (/18)
255.255.224.0 (/19)
255.255.240.0 (/20)
255.255.248.0 (/21)
255.255.252.0 (/22)
255.255.254.0 (/23)
255.255.255.0 (/24)
255.255.255.128 (/25)
255.255.255.192 (/26)
255.255.255.224 (/27)
255.255.255.240 (/28)
255.255.255.248 (/29)
255.255.255.252 (/30)

4. 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. Please note the number of IP addresses in this IP pool must be less than the maximum number of subnet network as per the subnet mask you set.

5. Lease Time: DHCP lease time to the DHCP client.

6. Domain Name: Optional, this information will be passed to the clients.

7. Primary DNS/Secondary DNS: Optional. This feature allows you to assign a DNS Server.

8. Primary WINS/Secondary WINS: Optional. This feature allows you to assign a WINS Server.

9. Gateway: Optional. Gateway address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your local computer when DHCP server offers IP address. For an example, this gateway will assign IP address to local computers, but local computers will go to Internet through another gateway.

Click on “Add” and the following screen will appear.

Dynamic DNS > DHCP Server

DHCP Server Configuration

Item	Setting
▶ DHCP Server Name	DHCP 2
▶ LAN IP Address	192.168.2.254
▶ Subnet Mask	255.0.0.0 (/8)
▶ IP Pool	Starting Address: <input type="text"/> Ending Address: <input type="text"/>
▶ Lease Time	86400 seconds
▶ Domain Name	<input type="text"/>
▶ Primary DNS	<input type="text"/>
▶ Secondary DNS	<input type="text"/>
▶ Primary WINS	<input type="text"/>
▶ Secondary WINS	<input type="text"/>
▶ Gateway	<input type="text"/>
▶ Server	<input type="checkbox"/> Enable

Save Undo Back

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. For internal servers, you can use this feature to ensure each of them receives same IP address all the time.

Dynamic DNS > DHCP Server

Fixed Mapping [Help]

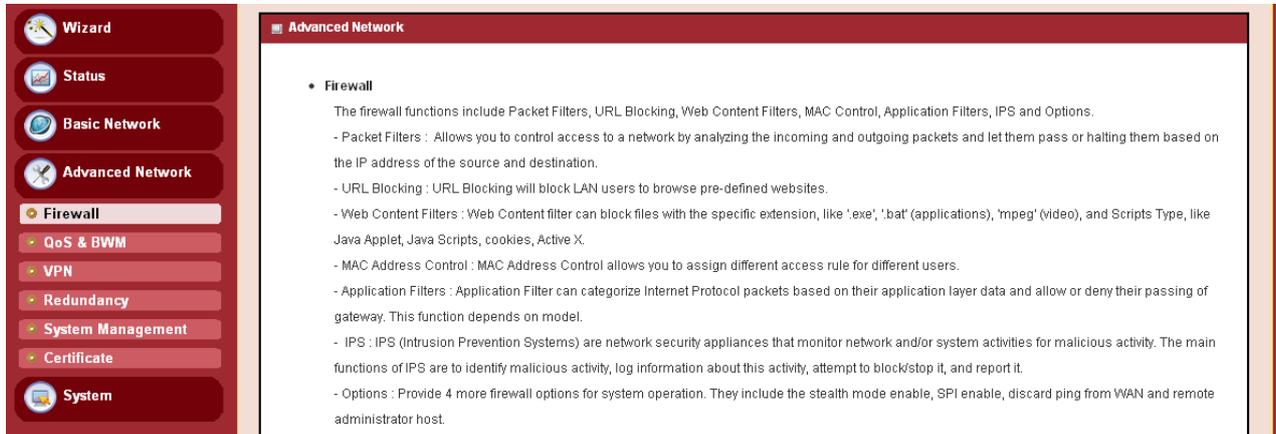
DHCP clients: 192.168.123.100 (savina) Copy to ID 1

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

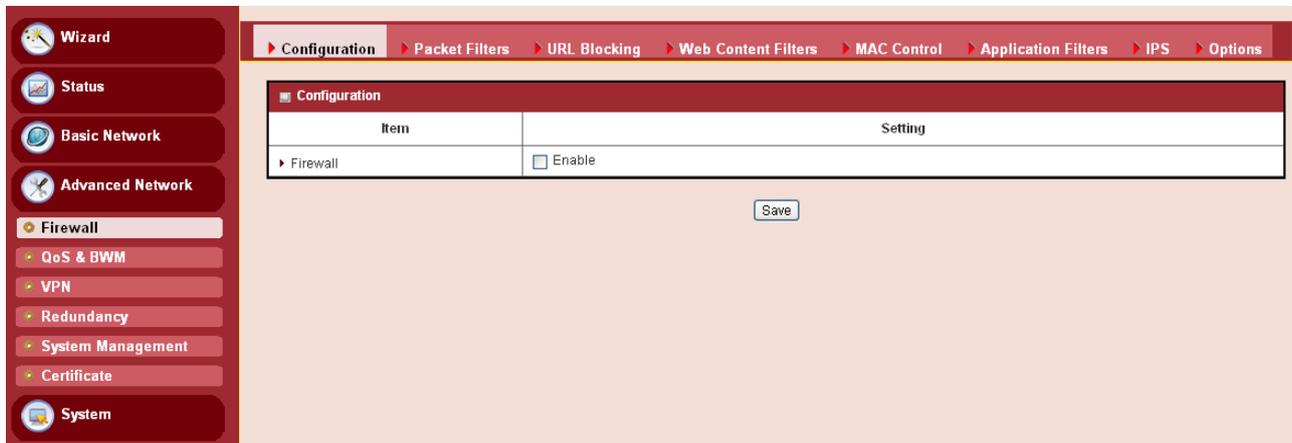
3.2 Advanced Network

This device also supports many advanced network features, such as Firewall, QoS, VPN 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, MAC Control, Application Filters, IPS and Options.



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 are destined to virtual servers or DMZ host only. You can select one of the two filtering policies:

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

Item	Setting
Packet Filters	<input checked="" type="checkbox"/> Enable
Black List / White List	Allow all to pass except those match the following rules. ▾
Log Alert	<input type="checkbox"/> Enable

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions

Save Undo MAC Level

1. **Packet Filters:** Check if you want to enable Packet Filter function.
2. **Black List / White List:** Select one of the two filtering policies for the defined rules.
Black List - Allow all to pass except those that match the specified rules.
White List - Deny all to pass except those that match the specified rules
3. **Log Alert:** Enable Log Alert will record events that are blocked by these rules.

Rule Definition:

You can enter the **Source IP**, **destination IP / Port**, **Protocol**, and **Schedule** settings for each packet filter rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

4. **Source IP:** Specify the source IP range for the rule. 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.
5. **Destination IP / Destination Ports:** Specify the Destination IP and Port range for the rule. 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). An empty implies all port addresses.
6. **Protocol:** Specify which packet protocol is to be filtered. It can be TCP, UDP, or Both.
7. **Time Schedule:** The rule can be turned off according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu.

8. **Enable:** Check if you want to enable the rule. Each rule can be enabled or disabled individually.
9. **Actions:** Click on the “Reset” button to clear the existing settings for the specified rule, and you can easily delete or overwrite a rule with new rule settings.

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

Item	Setting
▶ URL Blocking	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Allow all to pass except those match the following rules. ▼
▶ Log Alert	<input type="checkbox"/> Enable
▶ Invalid Access Web Redirection	<input type="checkbox"/> Enable

ID	Rule Name	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions
----	-----------	-----------------------------	------------------	---------------	--------	---------

1. **URL Blocking:** Check if you want to enable URL Blocking.
2. **Black List / White List:** Select one of the two filtering policies for the defined rules.
 Black List - Allow all to pass except those that match the specified rules.
 White List - Deny all to pass except those that match the specified rules
3. **Log Alert:** Enable Log Alert will record events that are blocked by these rules.
4. **Invalid Access Web Redirection:** Users will see a specific web page to know their access is blocked by rule.

Click on “Add”. The following screen will appear.

Item	Setting
▶ Rule Name	Rule1
▶ URL / Domain Name / Keyword	
▶ Destination Port	-
▶ Time Schedule	(0) Always ▼
▶ Rule	<input type="checkbox"/> Enable

5. **Rule Name:** Give an appropriate name to the rule.
6. **URL/Domain Name/Keyword:** 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".
7. **Destination Port:** Enter the destination port.
8. **Time Schedule:** The rule can be turn off according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu. 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.

The screenshot displays the configuration interface for Web Content Filters. It includes a navigation bar, a configuration table, a list of filters, and a detailed configuration form for a specific rule.

Item	Setting
Web Content Filters	<input checked="" type="checkbox"/> Enable
Popular File Extension List	<input type="checkbox"/> Cookie <input type="checkbox"/> Java <input type="checkbox"/> ActiveX
Log Alert	<input type="checkbox"/> Enable

ID	Rule Name	User-defined File Extension List	Time Schedule	Enable	Actions

Rule Name	User-defined File Extension List (Use ; to Concatenate)	Time Schedule	Enable
Rule1		Always	<input type="checkbox"/>

1. **Web Content Filters:** Check if you want to enable Web Content Filter.
2. **Popular File Extension List:** Check which extension types, Cookie, Java, ActiveX, are to be blocked
3. **User-defined File Extension List:** You can enter up to 10 file extensions in a rule to be blocked.
4. **Time Schedule:** The rule can be turned off according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu.

- 5. Enable:** Check if you want to enable the rule. Each rule can be enabled or disabled individually.

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

3.2.1.4 MAC Control

MAC Control allows you to assign different access rights for different users based on device’s MAC address.

- 1. MAC Control:** Check “Enable” to enable the “MAC Control”. All of the settings in this page will take effect only when “Enable” is checked.
- 2. Black List / White List:** Select one of the two filtering policies for the defined rules.
Black List - Allow all to pass except those that match the specified rules.
White List - Deny all to pass except those that match the specified rules.
- 3. Log Alert:** Enable Log Alert will record events that are blocked by these rules.
- 4. Known MAC from LAN PC List:** You can see all of connected clients from this list, and copy their MAC address to the control table below.
- 5. MAC Address:** Input the MAC address of local device. You can input manually or copy it from **Known MAC from LAN PC List**. Please note the format of MAC address is like “xx:xx:xx:xx:xx:xx”. “x” is a hexadecimal digit.
- 6. Time Schedule:** The rule can be turn off according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu.
- 7. Enable:** Check if you want to enable the rule. Each rule can be enabled or disabled individually.

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

3.2.1.5 Application Filters

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

The screenshot displays the 'Application Filters' configuration page in the Digisol management interface. The breadcrumb trail at the top indicates the path: Configuration > Packet Filters > URL Blocking > Web Content Filters > MAC Control > Application Filters > IPS > Options. The left sidebar contains navigation options: Wizard, Status, Basic Network, Advanced Network, Firewall (selected), QoS & BWM, VPN, Redundancy, System Management, Certificate, and System.

The main configuration area is divided into several sections, each with a table of items and their settings:

- Configuration:**

Item	Setting
Application Filters	<input checked="" type="checkbox"/> Enable
Log Alert	<input type="checkbox"/> Enable
Schedule	(0) Always
- Chat Software:**

QQ	<input type="checkbox"/> Enable
Facebook	<input type="checkbox"/> Enable
Skype	<input type="checkbox"/> Enable
Aliww	<input type="checkbox"/> Enable
- P2P Software:**

BT(BitTorrent, BitSpirit, BitComet)	<input type="checkbox"/> Enable
eDonkey/eMule/Shareaza	<input type="checkbox"/> Enable
HTTP Multiple Thread Download	<input type="checkbox"/> Enable
Thunder	<input type="checkbox"/> Enable
Baofeng	<input type="checkbox"/> Enable
- Proxy:**

HTTP proxy	<input type="checkbox"/> Enable
SOCKS 4/5 proxy	<input type="checkbox"/> Enable
- Streaming:**

MMS	<input type="checkbox"/> Enable
RTSP	<input type="checkbox"/> Enable
PPStream	<input type="checkbox"/> Enable
PPLive(PPTV)	<input type="checkbox"/> Enable
Qvod	<input type="checkbox"/> Enable

At the bottom right of the configuration area, there are 'Save' and 'Undo' buttons.

3.2.1.6 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.

Item	Setting
▶ IPS	<input checked="" type="checkbox"/> Enable
▶ Log Alert	<input type="checkbox"/> Enable

Item	Setting
▶ SYN Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ UDP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ ICMP Flood Defense	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)
▶ Port Scan Detection	<input type="checkbox"/> Enable <input type="text" value="200"/> Packets/second (10~10000)
▶ Block Land Attack	<input type="checkbox"/> Enable
▶ Block Ping of Death	<input type="checkbox"/> Enable
▶ Block IP Spoof	<input type="checkbox"/> Enable
▶ Block TCP Flag Scan	<input type="checkbox"/> Enable
▶ Block Smurf	<input type="checkbox"/> Enable
▶ Block Traceroute	<input type="checkbox"/> Enable
▶ Block Fraggle Attack	<input type="checkbox"/> Enable
▶ ARP Spoofing Defence	<input type="checkbox"/> Enable <input type="text" value="300"/> Packets/second (10~10000)

Save Undo

3.2.1.7 Options

Item	Setting
▶ Stealth Mode	<input type="checkbox"/> Enable
▶ SPI	<input checked="" type="checkbox"/> Enable
▶ Discard Ping from WAN	<input type="checkbox"/> Enable
▶ Remote Administrator Hosts (IP / Mask : Port)	<input type="text" value="0.0.0.0"/> / <input type="text" value="0"/> : <input type="text" value="80"/> <input type="checkbox"/> Enable

Save Undo

- Stealth Mode:** Enable this feature, this device will not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet.
 - SPI:** When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.
- 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.

The screenshot displays the configuration page for Rule-based QoS. The left sidebar contains navigation options: Wizard, Status, Basic Network, Advanced Network, Firewall, QoS & BWM (selected), VPN, Redundancy, System Management, Certificate, and System. The main content area is titled 'Configuration' and 'Rule-based QoS'. It features two configuration tables:

System Resource Configuration		[Help]
Item	Setting	
Total Priority Queues of All WANs	<input type="text" value="6"/>	
WAN Interface	WAN - 1	

WAN Interface Resource		
Item	Setting	
Bandwidth of Upstream	<input type="text" value="0"/>	Mbps
Bandwidth of Downstream	<input type="text" value="0"/>	Mbps
Total Connection Sessions	<input type="text" value="30000"/>	

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

3.2.2.1 QoS Configuration

Before QoS function can work correctly, this gateway needs to know available bandwidth of WAN connection.

System Resource Configuration	
Item	Setting
Total Priority Queues of All WANs	6
WAN Interface	WAN - 1

WAN Interface Resource	
Item	Setting
Bandwidth of Upstream	0 Mbps
Bandwidth of Downstream	0 Mbps
Total Connection Sessions	30000

Save Undo

- Bandwidth of Upstream:** Input the maximum bandwidth of uplink in Mbps/Kbps.
- Bandwidth of Downstream:** Input the maximum bandwidth of downlink in Mbps/Kbps.

3.2.2.2 Rule-based QoS

This gateway provides lots of flexible rules for you to set QoS policies. Basically, you need to know three parts of information before you create your own policies. First, “who” needs to be managed. Second, “what” kind of service needs to be managed. The last part is “how” you prioritize. Once you get this information, you can continue to learn more details in this section.

Configuration	
Item	Setting
Rule-based QoS	<input checked="" type="checkbox"/> Enable
Flexible Bandwidth Management	<input type="checkbox"/> Enable

QoS Rule List									
Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
Save Undo									

- Enable Rule-based QoS:** Check the “**Enable**” check box to enable the rule-based QoS function.
- Flexible Bandwidth Management:** It’s strongly recommended to enable this option to exploit maximum bandwidth effectively.

3. **Add :** After you enabled the rule-based QoS function, you can click on the “Add” button to create a new QoS rule.

Item	Setting
▶ Interface	All WANs
▶ Group	Src. MAC Address
▶ Service	All
▶ Resource	Bandwidth
▶ Control Function	Set MINR & MAXR
▶ QoS Direction	Outbound
▶ Sharing Method	Group Control
▶ Time Schedule	(0) Always
▶ Rule	<input type="checkbox"/> Enable

For creating a rule-QoS rule, please refer to the following sub-sections.

2. **Rule List:** Once you saved a QoS rule, it will be displayed in the **Rule Lists** area as below.

Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
All WANs	192.168.123.10/32	DSCP:BE	Bandwidth	2-3 Mbps	Inbound	Group	(0) Always	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Select"/>

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.

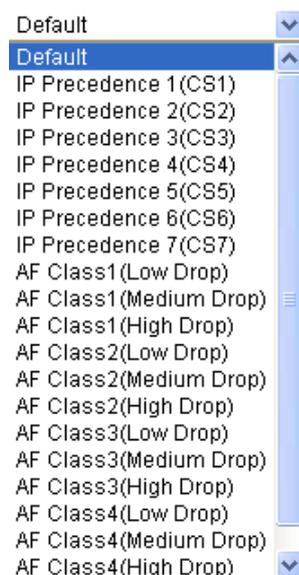
3. **Restart:** Press “Restart” button to re-initiate all QoS rules again.
4. **Reset QoS Rule:** Press “Reset QoS Rule” button to delete all created QoS rules.

3.2.2.2.1 Creating a QoS Rule based on IP Grouping

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs
▶ Group	IP 192.168.123.10 Subnet Mask : 255.255.255.255 (/32)
▶ Service	DSCP ▶ DiffServ CodePoint Default
▶ Resource	Bandwidth
▶ Control Function	Set MINR & MAXR --- Mbps
▶ QoS Direction	Inbound
▶ Sharing Method	Group Control
▶ Time Schedule	(0) Always
▶ Rule	<input checked="" type="checkbox"/> Enable

- 1. Rule:** Enable the rule setting first.
- 2. Group:** Choose **IP** from the list, and indicate single IP address or a segment IP range in following field. As the example above, this rule applies on IP address from 192.168.123.10 to 192.168.123.20.
- 3. Service:** Define “what” kinds of service need to be managed. There are four options for service recognition. They are **DSCP**, **TOS**, **User-Defined service** and **well-known service**.

DSCP: DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags. The DSCP categories that this gateway can detect are as below. You need to choose a correct one according to your device’s specification.



4. **Control Function:** In this field, you will decide what action will be taken on those selected traffics. Set the corresponding control types for the selected service type as below.

DSCP Marking: This option is only available when “**DSCP**” is chosen in “**Service**” field. The purpose of this option is changing original DSCP tag to a new value. This option won’t prioritize data packets.

PRI: Set priority for data packets of selected traffics. The value is from 1 to 6. “1” is with highest priority, and “6” is with least priority.

MAXR: Indicate the maximum bandwidth for selected traffics. The measurement unit can be Kbps or Mbps.

MINR: Indicate the minimum bandwidth for selected traffics. The measurement unit can be Kbps or Mbps.

SESSION: This option is only available when “**Connection Sessions**” is chosen in “**Service**” field. The maximum number of session is 20000.

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

Direction	
IN	For In-bond data
OUT	For Out-bond data
BOTH	In-bond and Out-bond

6. **Sharing Method:** This option is only available when “**MAXR**”, “**MINR**”, or “**SESSION**” is chosen in “**Control**” field. If you want to apply the value of **Control** setting on each selected host, then you need to select “**Single**”. Otherwise, if the value of **Control** setting is applying on all selected hosts, then you need to select “**Grouping**”. For example, you set MAXR to 2Mbps and select “**Single**”. Then it means the maximum bandwidth of each selected host can be up to 2Mbps. If changing to “**Grouping**”, then it means the maximum bandwidth of all selected hosts can be up to 2Mbps.
7. **Time Schedule:** The rule can be turned off according to the schedule rule you specified, and give user more flexibility on QoS function. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.

Example for adding a “DSCP” type QoS rule

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs
▶ Group	IP Subnet Mask: 255.255.255.255 (/32)
▶ Service	DSCP ▶ DiffServ CodePoint IP Precedence 4(CS4)
▶ Resource	Bandwidth
▶ Control Function	Set MINR & MAXR Mbps
▶ QoS Direction	Outbound
▶ Sharing Method	Group Control
▶ Time Schedule	(0) Always
▶ Rule	<input type="checkbox"/> Enable

Group: Select “IP” and entry IP range.

Service: Select “DSCP” which DiffServ CodePoint is set as CS4.

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

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

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

This rule means IP packets from WAN interface to LAN IP address 192.168.12.10 ~ 192.168.12.40 which with DiffServ value of “IP Precedence 4(CS4)” will be modified with DSCP Marking of “AF Class 2(High Drop)”.

Example for adding a “Connection Session” type QoS rule

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs
▶ Group	IP 192.168.123.10 Subnet Mask: 255.255.255.255 (/32)
▶ Service	DSCP ▶ DiffServ CodePoint IP Precedence 4(CS4)
▶ Resource	Connection Sessions
▶ Control Function	Set Session Limitation 200
▶ QoS Direction	Outbound
▶ Sharing Method	Individual Control
▶ Time Schedule	(0) Always
▶ Rule	<input checked="" type="checkbox"/> Enable

Group: Select “IP” and entry IP range.

Service: Select “Connection Sessions”.

Control Function: Select “SESSION”, and set session number to 200.

QoS 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” from the list.

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

This rule defines that each single host, 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.

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.

The products support following tunneling technologies to establish secure tunnels for data communication, including IPsec, PPTP, L2TP (over IPsec) and GRE.

The screenshot displays the Digisol configuration web interface. On the left is a dark red sidebar with navigation icons and labels: Wizard, Status, Basic Network, Advanced Network, Firewall, QoS & BWM, VPN (highlighted), Redundancy, System Management, Certificate, and System. The main content area has a breadcrumb trail: Configuration > IPsec > PPTP > L2TP > GRE. Below this is a 'Configuration' table with two columns: 'Item' and 'Setting'. The table contains one row: 'VPN' with a checked checkbox in the 'Setting' column. Below the table are 'Save' and 'Undo' buttons.

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable

3.2.3.1 IPSec

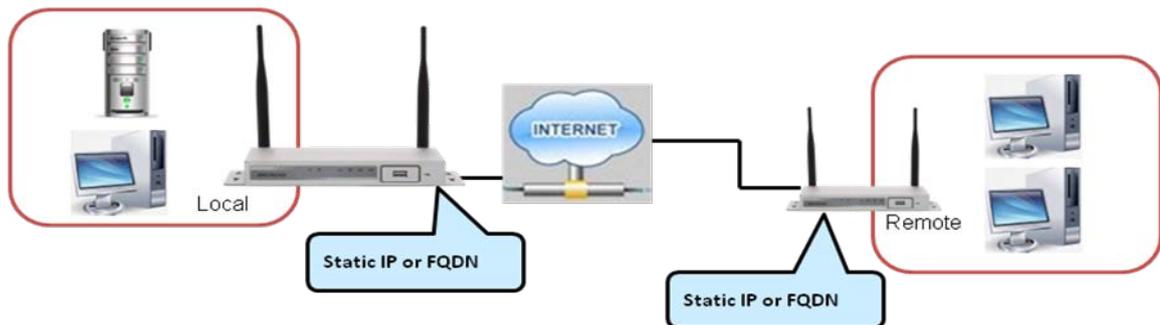
Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

3.2.3.1.1 IPSec VPN Tunnel Scenarios

There are some common IPSec VPN connection scenarios as follows:

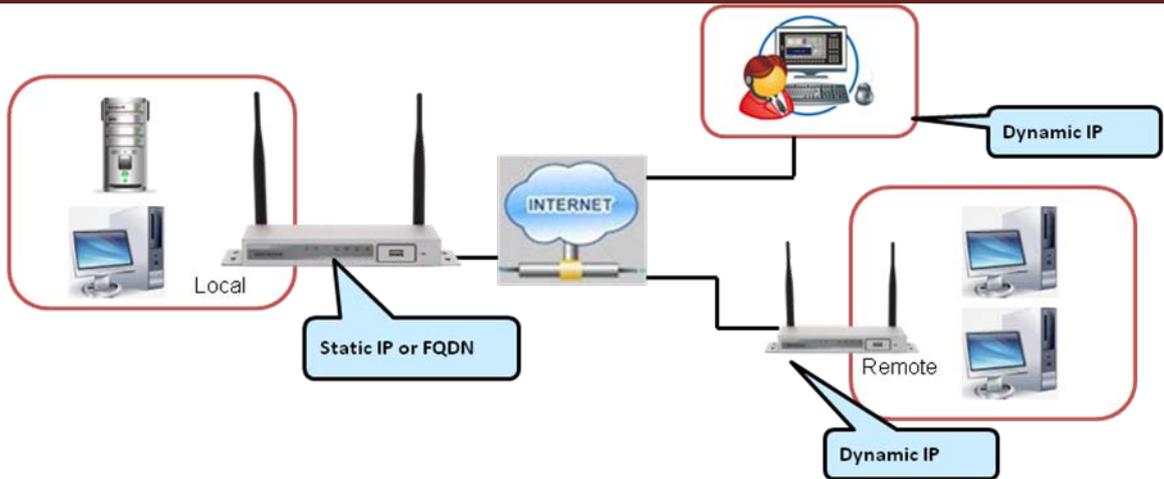
- Site to Site

Description: The unit establishes IPSec VPN tunnels with security gateway in head quarter or branch offices. Either local or remote DG-LB1054UV gateway which can be recognized by a static IP address or a FQDN can initiate the establishment of an IPSec VPN tunnel. Two peers of the tunnel have their own Intranets and the secure tunnel serves between these two subnets of hosts for data communication.



- Dynamic VPN

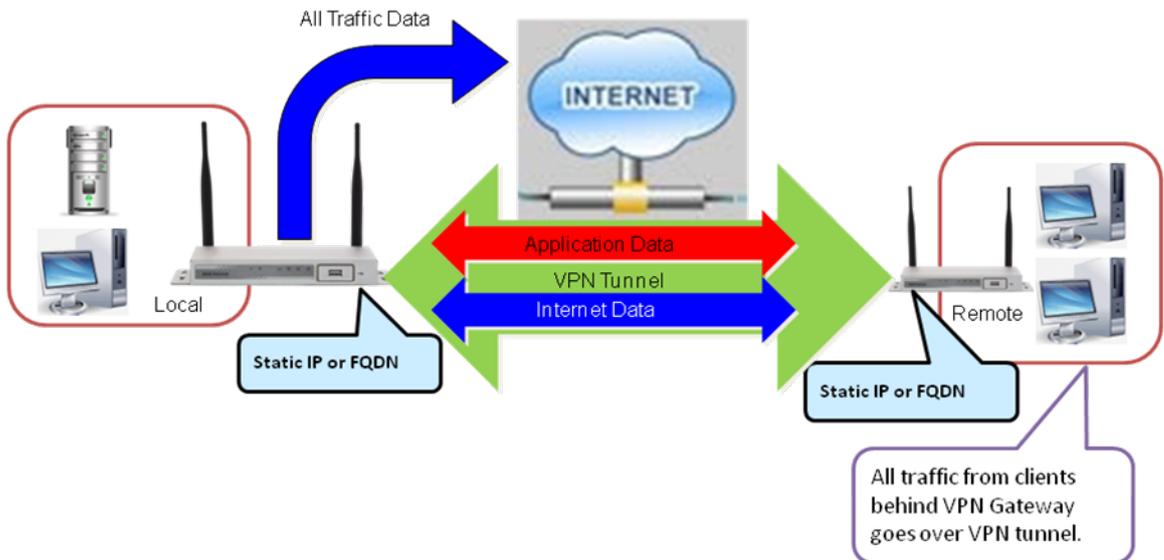
Description: DG-LB1054UV supports remote peers without fixed IP address to establish an IPSec VPN tunnel with itself. The remote peer can be a client host or a network site with its Intranet. It must be noted that the remote peer has to initiate the tunnel establishing process first.



There is one more advanced IPSec VPN application:

- Site to Site – Support Full Tunnel Application

Description: When Full Tunnel function of remote VPN gateway is enabled, all data traffic from remote clients behind remote VPN gateway will go over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote VPN gateway, all application packets and private data packets from the PC will be transmitted securely in the VPN tunnel to access the resources behind local VPN gateway. As a result, every time the user surfs the web for shopping or searching data on Internet, checking personal emails, or accessing company servers, all are done in a secure way through local VPN gateway.



3.2.3.1.2 IPsec Configuration

Item	Setting
▶ IPsec	<input checked="" type="checkbox"/> Enable
▶ NetBIOS over IPsec	<input type="checkbox"/> Enable
▶ NAT Traversal	<input type="checkbox"/> Enable
▶ Max. Concurrent IPsec Tunnels	32

ID	Interface	Tunnel Scenario	Tunnel Name	Remote Address	Gateway	Status	Enable	Actions
----	-----------	-----------------	-------------	----------------	---------	--------	--------	---------

- 1. IPsec:** You could trigger the function of IPsec VPN if you check “**Enable**”.
- 2. NetBIOS over IPsec:** If you would like two Intranets behind two VPN gateways to receive the NetBIOS packets from Network Neighborhood, you have to check “**Enable**”.
- 3. NAT Traversal:** Some NAT routers will block IPsec packets if they don’t support IPsec pass through. If your VPN gateway connects to this kind of NAT router which doesn’t support IPsec pass through, you need to activate this option in your VPN gateway.
- 4. Max. Concurrent IPsecTunnels:** The device supports up to 32 IPsec tunnels, but you can specify it with the number of maximum current activated IPsec tunnels that is smaller or equal to 32.

You can add new, edit or delete some IPsec tunnels in Tunnel List & Status as follows.

3.2.3.1.3 Tunnel List & Status

ID	Interface	Tunnel Scenario	Tunnel Name	Remote Address	Gateway	Status	Enable	Actions
----	-----------	-----------------	-------------	----------------	---------	--------	--------	---------

- 1. Add:** You can add one new IPsec tunnel with Site to Site scenario by clicking the “Add” button.
- 2. Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking the “Delete” button.
- 3. Tunnel:** Check the “Enable” box to activate the IPsec tunnel.
- 4. Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

Note: Tunnel ID1 is only for Dynamic VPN.

3.2.3.1.4 Tunnel Configuration

Tunnel Configuration	
Item	Setting
▶ Tunnel	<input type="checkbox"/> Enable
▶ Tunnel Name	IPSec #1
▶ Interface	WAN 1
▶ Tunnel Scenario	Site to Site
▶ Operation Mode	Always on
▶ Encapsulation Protocol	ESP
▶ Keep-alive	<input type="checkbox"/> Enable Ping IP <input type="text"/> Interval 30 (seconds)

- Tunnel Name:** Enter Tunnel Name.
- Interface:** Decide the WAN Interface to establish the tunnel.
- Tunnel Scenario:** Support “Site to Site” and “Dynamic VPN”.
- Operation Mode:** Default is “Always on” and options depend on product models.
- Encapsulation Protocol:** Default is ESP and options depend on product models.
- Keep-alive:** Check “Enable” box to keep alive the tunnel. By default, keep-alive method is “Ping IP” and other options depend on product models. Input the IP address of remote host that exist in the opposite side of the VPN tunnel (Ex. You can input the LAN IP address of remote VPN gateway). The Interval is specified with the time interval between two ping requests, and by default, it is 30 seconds. Now, the device will start to ping remote host when there is no traffic within the VPN tunnel. If the device can't get ICMP response from remote host anymore, it will terminate the VPN tunnel automatically.

3.2.3.1.5 IPsec Phase

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	28800 (seconds) (Max. 86400)

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 VPN peers.

3.2.3.1.6 IPSec Proposal Definition

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto	SHA1	Group 2	<input checked="" type="checkbox"/> Enable
2	AES-auto	MD5		<input checked="" type="checkbox"/> Enable
3	DES	SHA1		<input checked="" type="checkbox"/> Enable
4	3DES	SHA1		<input checked="" type="checkbox"/> Enable

There are 4 IPSec proposals can be defined by you and used in IPSec tunnel establishing.

- Encryption:** There are six algorithms that can be selected: DES, 3DES, AES-auto, AES-128, AES-192 and AES-256.
- Authentication:** There are five algorithms that can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.
- PFS Group:** There are nine groups which can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18. Once the PFS Group is selected in one IPSec proposal, the one in the other 3 IPSec proposals uses the same choice.
- Definition:** Check this box to enable the IKE Proposal during tunnel establishment.

3.2.3.2 PPTP

The VPN gateway can behave as a PPTP server and a PPTP client at the same time.

Item	Setting
PPTP	<input checked="" type="checkbox"/> Enable
Client/Server	Server

- PPTP:** Check the “Enable” box to activate PPTP client and server functions.
- Client/Server:** Choose Server or Client to configure corresponding role of VPN gateway beneath the choosing.

3.2.3.2.1 PPTP Server

When VPN gateway plays the PPTP server role, it will allow remote hosts to access LAN servers behind the PPTP server. The device can support upto four authentication methods: PAP, CHAP, MSCHAP (v1) and MSCHAP (v2). Users can also enable MPPE encryption when using MSCHAP.

Item	Setting
PPTP	<input checked="" type="checkbox"/> Enable
Client/Server	Server

Item	Setting
PPTP Server	<input type="checkbox"/> Enable
Server Virtual IP	192.168.0.1
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-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits

User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

ID	User Name	Password	Enable	Actions
----	-----------	----------	--------	---------

Save

- PPTP Server Configuration:** Enable or Disable PPTP server function.
- 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.
- IP Pool Starting Address:** This device will assign an IP address to remote PPTP client.

This value indicates the beginning of IP pool.

4. **IP Pool Ending 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 :** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method. You can choose encryption length of MPPE encryption
7. **PPTP Server Status:** The connected PPTP user & connection information will be shown in this table.
8. **User Account List:** You can input up to 10 different user accounts for the PPTP server.

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

3.2.3.2.2 PPTP Client

Configuration [Help]	
Item	Setting
▶ PPTP	<input checked="" type="checkbox"/> Enable
▶ Client/Server	Client ▾

PPTP Client Configuration	
Item	Setting
▶ PPTP Client	<input type="checkbox"/> Enable

PPTP Client List & Status Add Delete Refresh								
ID	PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/ Gateway/Remote Subnet	Status	Enable	Actions
<input type="button" value="Save"/>								

1. **PPTP Client Configuration:** Enable or Disable PPTP client function.
2. **PPTP Client List & Status:** You can input upto 10 different user accounts for PPTP clients, and define each user account settings by clicking on the corresponding “Edit” button and then check the “Enable” checkbox to enable it.

PPTP Client Configuration	
Item	Setting
▶ PPTP Client Name	<input type="text" value="PPTP #1"/>
▶ Interface	<input type="text" value="WAN 1"/>
▶ Operation Mode	<input type="text" value="Always on"/>
▶ Remote IP/FQDN	<input type="text"/>
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Default Gateway/Remote Subnet	<input type="text" value="Remote Subnet"/> <input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ NAT before Tunneling	<input type="checkbox"/> Enable
▶ LCP Echo Type	<input type="text" value="Auto"/>
	Interval <input type="text"/> seconds Max. Failure Time <input type="text"/> times
▶ Tunnel	<input type="checkbox"/> Enable

3. **PPTP Client Name:** The name of this rule.
4. **Interface:** Select the interface from the list.
5. **Operation Mode:** Support “Always on”
6. **Remote IP/FQDN:** Enter the IP/FQDN of the remote PPTP server.
7. **User Name:** The user name which is provided by remote PPTP server.
8. **Password:** The password which is provided by remote PPTP server.
9. **Default Gateway/Remote Subnet:** You can check the “Enable” checkbox to set this tunnel as the default gateway for WAN connection.
10. **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.
11. **MPPE Encryption:** If you enable MPPE, then this L2TP tunnel will be encrypted.
12. **NAT before tunneling:** It can go to access the Server internal data.
13. **LCP Echo Type:** Choose the way to do connection keep alive.

3.2.3.3 L2TP

The VPN gateway can behave as a L2TP server and a L2TP client at the same time.

Configuration [Help]	
Item	Setting
▶ L2TP	<input type="checkbox"/> Enable
▶ Client/Server	Server

- L2TP:** Check the “Enable” box to activate L2TP client and server functions.
- Client/Server:** Choose Server or Client to configure corresponding role of VPN gateway beneath the choosing.

3.2.3.3.1 L2TP Server

When VPN gateway plays the L2TP server role, it will allow remote hosts to access LAN servers behind the L2TP server. The device can support four authentication methods: PAP, CHAP, MSCHAP(v1) and MSCHAP(v2). Users can also enable MPPE encryption when using MSCHAP.

Configuration [Help]	
Item	Setting
▶ L2TP	<input checked="" type="checkbox"/> Enable
▶ Client/Server	Server

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	<input checked="" type="checkbox"/> Enable
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshare Key <input type="text"/> (Min. 8 characters)
▶ Server Virtual IP	<input type="text" value="192.168.10.1"/>
▶ IP Pool Starting Address	<input type="text" value="10"/>
▶ IP Pool Ending Address	<input type="text" value="100"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable <input type="text" value="40 bits"/>
▶ Service Port	<input type="text" value="1701"/>

L2TP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

User Account List Add Delete				
ID	User Name	Password	Enable	Actions
Save				

- L2TP Server Configuration:** Enable or Disable L2TP server function.
- 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.

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 :** Check this checkbox to enable MPPE encryption. Please note that MPPE needs to work with MSCHAP-v1 or MSCHAP-v2 authentication method. You can choose encryption length of MPPE encryption.
8. **Service Port:** Enter the service port.
9. **L2TP Server Status:** The connected L2TP user & connection information will be shown in this table.
10. **User Account List:** You can input upto 10 different user accounts for the L2TP server.

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

3.2.3.3.2 L2TP Client

1. **L2TP Client Configuration:** Enable or Disable L2TP client function.

2. **L2TP Client List & Status:** You can input upto 10 different user accounts for L2TP clients, and define each user account settings by clicking on the corresponding “Edit” button and then check the “Enable” checkbox to enable it.

L2TP Client Configuration	
Item	Setting
▶ L2TP Client Name	L2TP #1
▶ Interface	WAN 1
▶ Operation Mode	Always on
▶ L2TP over IPsec	<input type="checkbox"/> Enable Preshare Key <input type="text"/> (Min. 8 characters)
▶ Remote LNS IP/FQDN	<input type="text"/>
▶ Remote LNS Port	1701
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ Tunneling Password (Optional)	<input type="text"/>
▶ Default Gateway/Remote Subnet	Remote Subnet <input type="text"/>
▶ Authentication Protocol	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE Encryption	<input type="checkbox"/> Enable
▶ NAT before Tunneling	<input type="checkbox"/> Enable
▶ LCP Echo Type	Auto Interval <input type="text"/> 30 seconds Max. Failure Time <input type="text"/> 6 times
▶ Service Port	Auto <input type="text"/> 0
▶ Tunnel	<input type="checkbox"/> Enable

1. **L2TP Client Name:** The name of this rule.
2. **Interface:** Select the interface from the drop down list.
3. **Operation Mode:** Supports “Always on”.
4. **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.
5. **Remote LNS IP/FQDN:** Enter the IP/FQDN of the remote PPTP server.
6. **User Name:** The user name which is provided by remote L2TP server.
7. **Password:** The password which is provided by remote L2TP server.
8. **Tunneling Password:** Enter the tunneling password.
9. **Default Gateway/Remote Subnet:** You can check the “Enable” checkbox to set this tunnel as the default gateway for WAN connection.
10. **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.
11. **MPPE Encryption:** If you enable MPPE, then this L2TP tunnel will be encrypted.
12. **NAT before tunneling:** It can go to access the Server internal data.
13. **LCP Echo Type:** Choose the way to do connection keep alive.
14. **Service Port:** Enter the service port.

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

3.2.3.4 GRE Tunnel

3.2.3.4.1 GRE Configuration

Configuration > IPSec > PPTP > L2TP > GRE

Configuration [Help]

Item	Setting
GRE Tunnel	<input checked="" type="checkbox"/> Enable

GRE Tunnel List Add Delete

ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Default Gateway/Remote Subnet	Enable	Actions
----	-------------	-----------	----------------	-----------	-----------	-----	-----	------------	-------------------------------	--------	---------

Save Undo

1. **GRE Tunnel:** You could trigger the function of GRE Tunnel if you check “**Enable**”.
2. **Default Gateway:** You can choose a tunnel as the default gateway for WAN connection.

3.2.3.4.2 GRE Tunnel Definitions

1. **Add:** You can add one new IPSec tunnel with Site to Site scenario by clicking the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the IPSec tunnel.
4. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

3.2.3.4.3 GRE rule Configuration

GRE Rule Configuration [Help]	
Item	Setting
▶ Tunnel Name	GRE #1
▶ Interface	WAN 1
▶ Operation Mode	Always on
▶ Tunnel IP	
▶ Remote IP	
▶ Key	
▶ TTL	
▶ Keep-alive	<input type="checkbox"/> Enable Ping IP <input type="text"/> Interval <input type="text" value="5"/> (seconds)
▶ Default Gateway/Remote Subnet	Default Gateway <input type="text" value="0.0.0.0/0"/>
▶ DMVPN Spoke	<input type="checkbox"/> Enable
▶ IPsec Pre-shared Key	<input type="text"/> (Min. 8 characters)
▶ Tunnel	<input type="checkbox"/> Enable

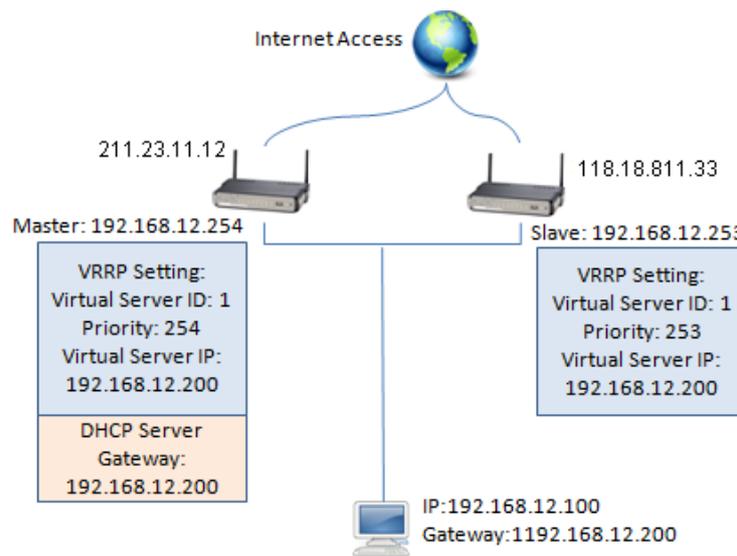
1. **Tunnel Name:** The name of this GRE tunnel.
2. **Interface:** Select the interface form the drop down list.
3. **Operation Mode:** Supports “Always on”.
4. **Tunnel IP:** Assign a virtual IP address of this tunnel.
5. **Remote IP:** Enter the IP address of remote host that you want to connect.
6. **Key:** Enter the password to establish GRE tunnel with remote host.
7. **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.
8. **Keep alive:** Enter the ping IP and the interval.
9. **Default Gateway/Remote Subnet:** You can choose a tunnel as the default gateway for WAN connection. Or enter the local subnet of remote host. If a packet wants to go to this subnet, the GRE tunnel will be established automatically.
10. **DMVPN Spoke:** Selects device as device which connects to central HUB.
11. **IPsec Pre-Shared Key:** Enter the preshared key.
12. **Tunnel:** Enable or Disable this GRE tunnel.

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

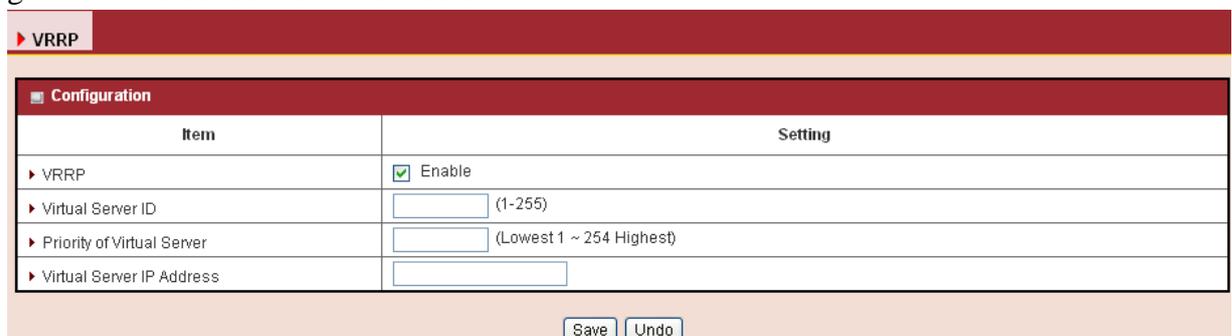
3.2.4 Redundancy

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. **VRRP:** 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 System Management

3.2.5.1 TR-069

Item	Setting
▶ TR-069	<input checked="" type="checkbox"/> Enable
▶ Interface	WAN-1
▶ ACS URL	<input type="text"/>
▶ ACS UserName	<input type="text"/>
▶ ACS Password	<input type="text"/>
▶ ConnectionRequest Port	8099
▶ ConnectionRequest UserName	<input type="text"/>
▶ ConnectionRequest Password	<input type="text"/>
▶ Inform	<input checked="" type="checkbox"/> Enable Interval <input type="text" value="900"/>

[Save] [Undo]

TR-069 is a customized feature for ISP, It is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help.

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.

TR-069
SNMP
Telnet with CLI
UPnP

Configuration
[Help]

Item	Setting
SNMP Enable	<input type="checkbox"/> LAN <input type="checkbox"/> WAN
Supported Versions	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input type="checkbox"/> v3
Get/ Set Community	<input type="text"/> / <input type="text"/>
Trap Event Receiver 1	<input type="text"/>
Trap Event Receiver 2	<input type="text"/>
Trap Event Receiver 3	<input type="text"/>
Trap Event Receiver 4	<input type="text"/>
WAN Access IP Address	<input type="text"/>

User Privacy Definition

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
2			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
3			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
4			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
5			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit

Save Undo

1. **SNMP Enable:** You can check “Local(LAN)”, “Remote(WAN)” or both to enable SNMP function. If “Local(LAN)” is checked, this device will respond to the request from LAN. If “Remote(WAN)” is checked, this device will respond to the request from WAN.
2. **Supported Versions:** Supports SNMP V1, V2c and V3.
3. **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.
4. **Set Community:** The community of SetRequest that this device will accept.
5. **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.
6. **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.

3.2.5.3 Telnet with CLI

The screenshot shows a configuration page with a breadcrumb trail: TR-069 > SNMP > Telnet with CLI > UPnP. The main content area is titled 'Configuration' and contains a table with two columns: 'Item' and 'Setting'.

Item	Setting
▶ Telnet with CLI	LAN <input checked="" type="checkbox"/> Enable WAN <input type="checkbox"/> Enable
▶ Connection Type	Telnet : Service Port <input type="text" value="23"/> <input checked="" type="checkbox"/> Enable SSH : Service Port <input type="text" value="22"/> <input type="checkbox"/> Enable

At the bottom of the configuration area, there are two buttons: 'Save' and 'Undo'.

3.2.5.4 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.

The screenshot shows a configuration page with a breadcrumb trail: TR-069 > SNMP > Telnet with CLI > UPnP. The main content area is titled 'Configuration' and contains a table with two columns: 'Item' and 'Setting'.

Item	Setting
▶ UPnP	<input checked="" type="checkbox"/> Enable

At the bottom of the configuration area, there are two buttons: 'Save' and 'Undo'. A '[Help]' link is visible in the top right corner of the configuration table.

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

3.2.6 Certificate

3.2.6.1 My Certificates

My Certificates Trusted Certificates Issue Certificates					
Root CA <input type="button" value="Generate"/>					
ID	Name	Subject	Issuer	Vaild To	Action
Local Certificate List <input type="button" value="Generate"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>					
ID	Name	Subject	Issuer	Vaild To	Action

Root CA Certificate Configuration

Root CA Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/>
▶ Key	Key Type : <input type="text" value="RSA"/> Key Length : <input type="text" value="1024-bits"/>
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> E-mail : <input type="text"/>
▶ Validity	Expired : <input type="text" value="10-years"/>

Local Certificate Configuration

Local Certificate Configuration	
Item	Setting
▶ Name	<input type="text"/> Self-signed : <input type="checkbox"/>
▶ Key	Key Type : <input type="text" value="RSA"/> Key Length : <input type="text" value="1024-bits"/>
▶ Subject Name	Country(C) : <input type="text"/> State(ST) : <input type="text"/> Location(L) : <input type="text"/> Organization(O) : <input type="text"/> Organization Unit(OU) : <input type="text"/> Common Name(CN) : <input type="text"/> E-mail : <input type="text"/>

3.2.6.2 Trusted Certificates

My Certificates Trusted Certificates Issue Certificates						
Trusted CA Certificate List <input type="button" value="Import"/> <input type="button" value="Delete"/>						
ID	Name	Subject	Issuer	Valid To	Action	
Trusted Client Certificate List <input type="button" value="Import"/> <input type="button" value="Delete"/>						
ID	Name	Subject	Issuer	Valid To	Action	

Import trusted CA Certificate

My Certificates Trusted Certificates Issue Certificates	
Trusted CA Certificate Import from a File	
<input type="button" value="Choose File"/> No file chosen <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	
Trusted CA Certificate Import from a PEM	
<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Import Trusted Client Certificate

Trusted Client Certificate Import from a File
<input type="button" value="Choose File"/> No file chosen <input type="button" value="Apply"/> <input type="button" value="Cancel"/>
Trusted Client Certificate Import from a PEM
<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>

3.2.6.3 Issue Certificates

My Certificates
Trusted Certificates
Issue Certificates

Certificate Signing Request (CSR) Import from a File
Sign

No file chosen

Certificate Signing Request (CSR) Import from a PEM
Sign

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 settings.

- Wizard
- Status
- Basic Network
- Advanced Network
- System
- System Related**
- Scheduling
- Grouping
- External Servers
- MMI

System

- **System Related**
 System Related sub-section includes 'Change Password', 'System Information', 'System Status' and 'System Tools'. Change Password is to change the password of administrator for configuring the device by using Web UI. System Tools support system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup. You also can check the system information and system status log here.
 - Change Password : You can change the System Password here. We strongly recommend you to change the system password for security reason.
 - System Information : You can view the System Information in this page. It includes the WAN Type, Display Time and Modem Information. But the modem information will be existed only at the models with embedded modems, like ADSL modem and 3G/LTE modem.
 - System Status : You can view the System Logs in Web UI. You also can send the logs to specific email accounts periodically or instantly by clicking on the 'Email Now' command button.
 - System Tools : The device supports many system tools, including system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup.
- **Scheduling**
 About Scheduling, you can define some time scheduling rules here to be applied at various applications in the device system. Whatever one application needs a time schedule, like the Work Hours is defined as AM8:00-PM5:00 from Monday to Friday, the time schedule object can be defined in this sub-section.
- **User Management* (The feature depends on product model)**
 User Management function provides you to manage user accounts, group them and define their properties based on user groups. You can manage user account in this section, including user list, user profile and user group. User List shows out all user accounts and User Profile can let you add one new profile or edit it. User Group offers you to collect several user accounts to one group to own same properties and bound services. Certainly, one individual user account also can be a unique group, like 'Administrator' group.
- **Grouping**
 Except for user group, the device also provides you to group some kinds of objects to be several groups, including host grouping, extension file grouping and L7 application grouping.
- **External Servers**
 About External Servers, you can define some external server objects here to be applied at various applications in the device system. Whatever one application needs an external server, like a RADIUS server, the external server object can be defined in this sub-section. These server objects include

3.3.1 System Related

Change Password

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

Change Password	
Item	Setting
▶ Old Password	<input type="password"/>
▶ New Password	<input type="password"/>
▶ New Password Confirmation	<input type="password"/>

System Information

You can view the System Information in this page. It includes the WAN Type and Display Time.

System Information	
Item	Setting
▶ WAN Type	Static IP
▶ Display Time	Tue, 01 Jan 2013 09:23:44 +0530

System Status

You can view the system status in this page. You also can send the logs to specific email accounts..

System Web Log	
Item	Setting
▶ Web Log	<input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input type="checkbox"/> Debug Categories
▶ Email Alert	<input type="checkbox"/> Enable Server List: <input type="text" value="--- Option ---"/> <input type="button" value="AddObject"/> E-mail Addresses: <input type="text"/> E-mail Subject: <input type="text"/>
▶ Syslogd	<input type="checkbox"/> Enable Server List: <input type="text" value="--- Option ---"/> <input type="button" value="AddObject"/>

Web Log: It displays web logs.

Email Alert: To get email alerts, check mark the enable box and enter the email addresses with an email subject.

Syslog: It displays the system log.

System Tools

Click on system tools to refer to the system time, perform the firmware upgrade, do the ping test, tracert test, reboot from the web, reset to default settings and take a back up of the config file. The 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.

▶ Change Password
▶ System Information
▶ System Status
▶ System Tools

System Tools	
Item	Setting
▶ System Time	<input type="button" value="Configure"/> <input type="button" value="Sync with Time Server"/> <input type="text" value="Sync with my PC (Tuesday March 31, 2015 12:25:11)"/>
▶ FW Upgrade	<input type="button" value="Via Web UI"/> <input type="button" value="FW Upgrade"/>
▶ Ping Test	Host IP: <input type="text"/> Interface: <input type="button" value="Auto"/> <input type="button" value="Ping"/>
▶ Tracert Test	Host IP: <input type="text"/> Interface: <input type="button" value="Auto"/> <input type="button" value="UDP"/> <input type="button" value="Traceroute"/>
▶ Reboot	<input type="button" value="Now"/> <input type="button" value="Reboot"/>
▶ Reset to Default	<input type="button" value="Reset"/>
▶ Wake on LAN	<input type="text"/> <input type="button" value="Wake up"/>
▶ Backup Configuration Settings	<input type="button" value="Backup"/>

3.3.2 Scheduling

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

Schedule Settings

Configuration

Item	Setting
Time Scheduling	<input type="checkbox"/> Enable

Time Schedule List Add Delete

ID	Rule Name	Actions
1	test	<input type="button" value="Edit"/> <input type="checkbox"/>
2	test1	<input type="button" value="Edit"/> <input type="checkbox"/>

1. **Enable:** Enable or disable the scheduling function.
2. **Add:** To create a schedule rule, click the “Add” button. When the next dialog popped out you can edit the **Rule Name, Policy** and set the schedule time (**Week day, Start Time and End Time**).

Time Schedule Configuration

Item	Setting
Rule Name	<input type="text"/>
Rule Policy	<input type="button" value="Inactivate"/> the Selected Days and Hours Below.

Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
2	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
3	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
4	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
5	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
6	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
7	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>
8	-- choose one -- <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

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

3.3.3 Grouping

Except for user group, the device also provides you to group some kinds of objects to be several groups, including host grouping, extension file grouping and L7 application grouping.

Configuration

▶ Configuration ▶ Host Grouping ▶ File Extension Grouping ▶ L7 Application Grouping

Configuration	
Item	Setting
▶ Grouping	<input checked="" type="checkbox"/> Enable

Host Grouping

▶ Configuration ▶ Host Grouping ▶ File Extension Grouping ▶ L7 Application Grouping

Host Group List						
ID	Group Name	Group Type	Member List	Bound Services	Enable	Actions
<input type="button" value="Refresh"/>						

Host Group Configuration	
Item	Setting
▶ Group Name	<input type="text"/>
▶ Member List	
▶ Multiple Bound Services	<input type="checkbox"/> Firewall <input type="checkbox"/> QoS
▶ Member Type	IP Address-based <input type="button" value="v"/>
▶ Member to Join	<input type="text"/> <input type="button" value="Join"/>
▶ Group	<input type="checkbox"/> Enable

File Extension Grouping

▶ Configuration ▶ Host Grouping ▶ File Extension Grouping ▶ L7 Application Grouping

File Extension Group List					
ID	Group Name	File Extension Group List	Bound Services	Enable	Actions
<input type="button" value="Refresh"/>					

File Extension Group Configuration	
Item	Setting
▶ Group Name	<input type="text"/>
▶ File Extension Group List	
▶ Multiple Bound Services	<input type="checkbox"/> Firewall
▶ Member to Join	Image <input type="text" value="Image"/> .bmp <input type="text" value=".bmp"/> <input type="button" value="Join"/>
▶ Group	<input type="checkbox"/> Enable

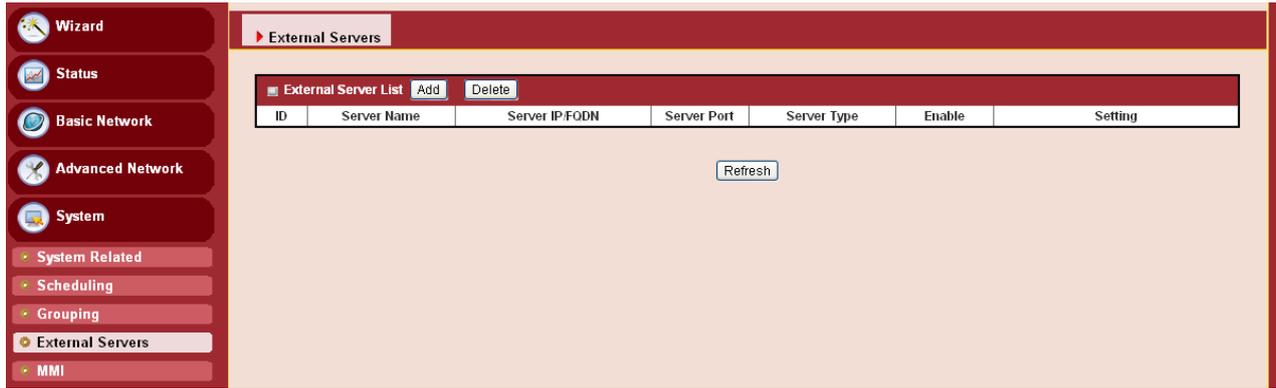
L7 Application Grouping

Configuration ▶ Host Grouping ▶ File Extension Grouping ▶ L7 Application Grouping					
L7 Application Group List <input type="button" value="Add"/> <input type="button" value="Delete"/>					
ID	Group Name	L7 Application Group List	Bound Services	Enable	Actions
<input type="button" value="Refresh"/>					

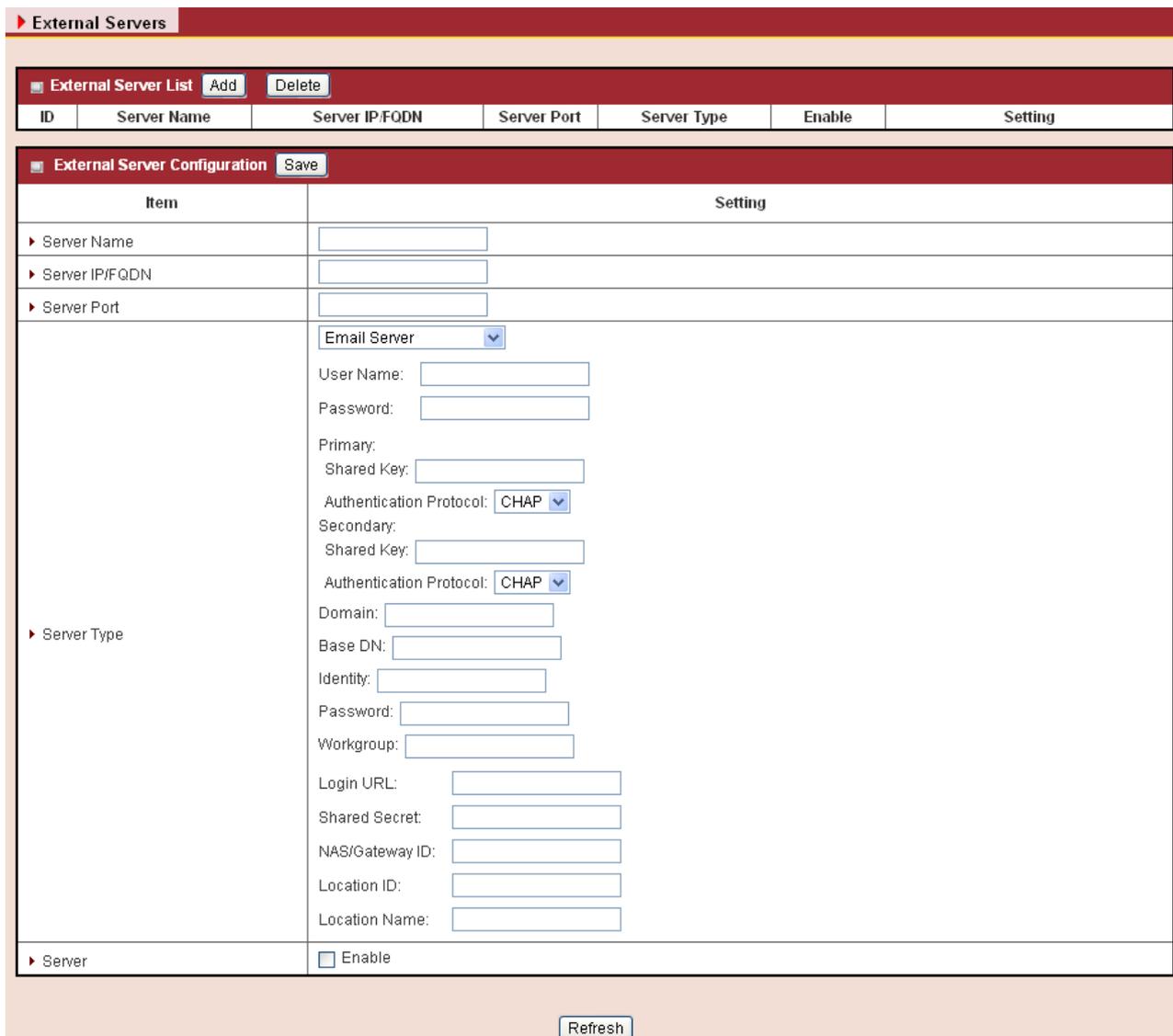
L7 Application Group Configuration	
Item	Setting
▶ Group Name	<input type="text"/>
▶ L7 Application List	
▶ Multiple Bound Services	<input type="checkbox"/> Firewall
▶ L7 Application to Join	Chat <input type="text" value="Chat"/> QQ <input type="text" value="QQ"/> <input type="button" value="Join"/>
▶ Group	<input type="checkbox"/> Enable

3.3.4 External Servers

About External Servers, you can define some external server objects here to be applied at various applications in the device system. Whatever one application needs an external server, like a RADIUS server, the external server object can be defined in this sub-section. These server objects include Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. (Some objects' supporting depends on product model.)



Click on “Add“. Whatever one application needs an external server, like a RADIUS server, the external server object can be defined in this sub-section.



3.3.5 MMI

3.3.5.1 Web UI

About MMI (Man-Machine Interface), it means the Web-based GUI. User can set the administrator timeout of Web UI surfing during configuring the device by the administrator. You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

Web UI	
Others [Help]	
Item	Setting
▶ Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

CHAPTER 4 Troubleshooting

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

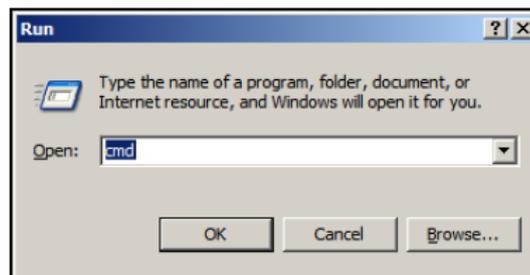
1 Why can't I configure the router even when the cable is plugged and the LED is lit?

Do a **Ping test** to make sure that the load balancing 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 load balancing 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 **Wired 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?

1. Make sure the RJ45 cable connects with the router.
2. Ensure that the setting on your Network Interface Card adapter is **“Enabled”**.
3. 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.
4. If the connection still doesn't work properly, then you can reset it to default.

3 How to reset to default?

1. Ensure the load balancing 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 Router reboots, it gets back to the factory**default** settings.

This product comes with One Year warranty. For further details about warranty policy and Product Registration, please visit support section of www.digisol.com