



# **DG-WU2005V**

WIRELESS ACCESS CONTROLLER, 5GE

LAN, 2GE WAN, 1GE DMZ, USB

## **User Manual**

**V1.0**

**2015-08-26**

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

---

## TABLE OF CONTENTS

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>8</b>
1.1 PACKAGE CONTENTS .....	9
1.2 HARDWARE INSTALLATION.....	9
1.2.1 ATTENTION .....	9
1.2.2 SYSTEM REQUIREMENTS .....	10
1.2.3 Hardware Configuration .....	11
1.2.4 LED Indicators.....	12
<b>CHAPTER 2 GETTING STARTED .....</b>	<b>13</b>
2.1 CONNECT YOUR DEVICE .....	13
2.2 EASY SETUP BY CONFIGURING WEB UI.....	13
2.2.1 Wizard .....	14
2.2.1.1 Configure with the Network Setup Wizard.....	14
2.2.1.2 Configure with the VPN Setup Wizard .....	20
2.2.2 Status.....	26
2.2.2.1 Network Status .....	27
2.2.2.2 LAN Client List.....	29
2.2.2.3 Firewall Status.....	29
2.2.2.4 VPN Status .....	30
2.2.2.5 System Management Status.....	31
2.2.2.6 DDNS Status .....	32
2.2.2.7 UPnP Status.....	33
2.2.2.8 Storage Status.....	33
3.1 BASIC NETWORK.....	38
3.1.1 WAN Setup.....	38
3.1.1.1 Physical Interface .....	39
3.1.1.2 Internet Setup.....	40
3.1.1.2.1 Ethernet WAN.....	41
3.1.1.2.2 Wireless WAN – 3G/4G.....	50
3.1.1.3 Load Balance.....	51
3.1.2 LAN & VLAN .....	54
3.1.2.1 Ethernet LAN .....	54
3.1.2.2 VLAN.....	55
3.1.2.2.1 VLAN Scenarios .....	56
3.1.2.2.2 Port-Based VLAN.....	61

---

3.1.2.2.3	Tag-Based VLAN.....	63
3.1.3	IPv6 Setup .....	66
3.1.3.1	6 to 4.....	66
3.1.3.2	6 in 4.....	67
3.1.4	NAT / Bridging.....	69
3.1.4.1	Configuration .....	69
3.1.4.2	Virtual Server & Virtual Computer.....	70
3.1.4.2.1	Virtual Server .....	70
3.1.4.2.2	Virtual Computer.....	71
3.1.4.3	Special AP & ALG .....	71
3.1.4.3.1	ALG .....	71
3.1.4.3.2	Special AP .....	72
3.1.4.4	DMZ .....	72
3.1.5	Routing.....	73
3.1.5.1	Static Routing.....	73
3.1.5.2	Dynamic Routing.....	75
3.1.5.3	Routing Information.....	77
3.1.6	Client/Server/Proxy.....	78
3.1.6.1	Dynamic DNS.....	78
3.1.6.2	DHCP Server.....	79
3.1.6.2.1	DHCP Server List .....	79
3.1.6.2.2	DHCP Server Configuration .....	80
3.1.6.2.4	Fixed Mapping .....	82
3.2	ADVANCED NETWORK.....	83
3.2.1	Firewall.....	84
3.2.1.1	Configuration .....	84
3.2.1.2	Packet Filters.....	84
3.2.1.2.1	Configuration .....	85
3.2.1.2.2	Packet Filter List .....	85
3.2.1.2.3	Packet Filter Rule Configuration .....	85
3.2.1.3	URL Blocking.....	87
3.2.1.3.1	Configuration .....	87
3.2.1.3.2	URL Blocking Rule List .....	88
3.2.1.3.3	URL Blocking Rule Configuration .....	88
3.2.1.4	Web Content Filters.....	89
3.2.1.4.1	Configuration .....	89
3.2.1.4.2	Web Content Filter Rule List .....	90
3.2.1.4.3	Web Content Filter Configuration.....	90

---

3.2.1.5	MAC Control .....	91
3.2.1.5.1	Configuration .....	91
3.2.1.5.2	MAC Control Rule List.....	92
3.2.1.5.3	MAC Control Rule Configuration .....	92
3.2.1.6	Application Filters .....	92
3.2.1.6.1	Configuration .....	93
3.2.1.7	IPS.....	94
3.2.1.8	Options .....	94
3.2.2	QoS & BWM .....	95
3.2.2.1	Configuration .....	96
3.2.2.2	Rule-based QoS .....	97
3.2.2.2.1	Configuration .....	98
3.2.2.2.2	QoS Rule List.....	99
3.2.2.2.3	QoS Rule Configuration.....	100
3.2.3	VPN Setup.....	104
3.2.3.1	IPSec .....	105
3.2.3.1.1	IPSec VPN Tunnel Scenarios .....	105
3.2.3.1.2	IPSec Configuration .....	107
3.2.3.1.3	Tunnel List & Status .....	108
3.2.3.1.4	Tunnel Configuration .....	108
3.2.3.1.5	Local & Remote Configuration.....	109
3.2.3.1.6	Authentication.....	110
3.2.3.1.7	IKE Phase.....	110
3.2.3.1.8	IKE Proposal Definition.....	111
3.2.3.1.9	IPSec Phase .....	112
3.2.3.1.10	IPSec Proposal Definition.....	112
3.2.3.2	PPTP.....	113
3.2.3.2.1	PPTP / L2TP VPN Tunnel Scenarios .....	113
3.2.3.2.1	PPTP Server Configuration .....	114
3.2.3.2.2	PPTP Server Status.....	115
3.2.3.2.3	User Account List.....	115
3.2.3.2.4	User Account Configuration .....	116
3.2.3.2.5	PPTP Client.....	116
3.2.3.2.6	PPTP Client List & Status.....	116
3.2.3.2.7	PPTP Client Configuration .....	117
3.2.3.3	L2TP .....	118
3.2.3.3.1	L2TP Server Configuration .....	118
3.2.3.3.2	L2TP Server Status.....	119

---

3.2.3.3.3	User Account List.....	119
3.2.3.3.4	User Account Configuration .....	120
3.2.3.3.5	L2TP Client.....	120
3.2.3.3.6	L2TP Client List & Status.....	121
3.2.3.3.7	L2TP Client Configuration .....	121
3.2.3.4	GRE .....	123
3.2.3.4.1	GRE VPN Tunnel Scenario.....	123
3.2.3.4.2	GRE Configuration .....	123
3.2.3.4.3	GRE Tunnel Definition.....	124
3.2.3.4.4	GRE rule Configuration .....	124
3.2.3.4.5	SSL VPN .....	125
3.2.4	Redundancy.....	126
3.2.4.1	VRRP .....	126
3.2.5	System Management .....	128
3.2.5.1	TR-069.....	128
3.2.5.2	SNMP .....	128
3.2.5.3	Telnet with CLI .....	130
3.2.5.4	UPnP.....	131
3.2.6	Certificate .....	131
3.3	APPLICATIONS.....	133
3.3.1	AP Management.....	134
3.3.1.1	Configuration .....	134
3.3.1.1.1	AP Management Configuration .....	134
3.3.1.1.2	AP Configuration Proposal List.....	134
3.3.1.2	AP List.....	135
3.3.1.2.1	Trusted AP List & Status.....	135
3.3.1.3	AP Configuration.....	136
3.3.1.3.1	AP Configuration .....	136
3.3.2	Captive Portal .....	137
3.3.2.1	Captive Portal Configuration.....	137
3.4	SYSTEM.....	138
3.4.1	System Related.....	140
3.4.1.1	Change Password .....	140
3.4.1.2	System Information.....	141
3.4.1.3	System Status .....	141
3.4.1.4	System Tools.....	142
3.4.2	Scheduling .....	145
3.4.3	User Management .....	146

---

---

3.4.3.1	User List.....	147
3.4.3.2	User Profile.....	147
3.4.3.3	User Group .....	148
3.4.4	<i>Grouping</i> .....	149
3.4.4.1	Grouping Configuration.....	149
3.4.4.2	Host Grouping .....	149
3.4.4.2.1	Host Group List.....	149
3.4.4.2.2	Host Group Configuration .....	150
3.4.4.3	File Extension Grouping .....	151
3.4.4.3.1	File Extension Group List.....	151
3.4.4.3.2	File Extension Group Configuration.....	151
3.4.4.4	L7 Application Grouping .....	152
3.4.4.4.1	L7 Application Group List.....	152
3.4.4.3.2	L7 Application Group Configuration.....	152
3.4.5	<i>External Servers</i> .....	153
3.4.5.1	External Server List.....	153
3.4.5.2	External Server Configuration.....	154
3.4.6	<i>MMI</i> .....	155
3.4.6.1	Web UI.....	155
<b>CHAPTER 4 TROUBLESHOOTING .....</b>		<b>156</b>

## 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-WU2005V Multi-Service Gateway with WLAN Controller. The product series, the multi-service security gateway comes with fruitful functions to meet SMB fast growing intranet access requirement. Multi-WAN NAT function allows multiple clients to have high speed access. VPN technology can enable secure access within intranet. By AP controller function, it is easy to deploy WiFi access infrastructure. Firewall and access control can prevent from hackers attack and avoid unproductive activity. Friendly setting and professional network management function, supervisor can easily take control of whole intranet. Besides being used for SMB corporate, when combined with various gateway series, it is also quite suitable for commercial, mobile office, hotspot deployment, and M2M-IoT application. For optimal IT investment, this device will guarantee maximum ROI and highest reliability.

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

The following items should be present in your package:

- DG-WU2005V Wireless Access Controller
- Power Cord (1 No.)
- Patch Cord (1 No.)
- Rack Mount Kit
- Installation Guide CD (includes User Manual & QIG)

Make sure that the package contains above items. If any of the listed items is damaged or missing, please contact your retailer immediately.

## 1.2 Hardware Installation

### 1.2.1 ATTENTION



#### **Attention**

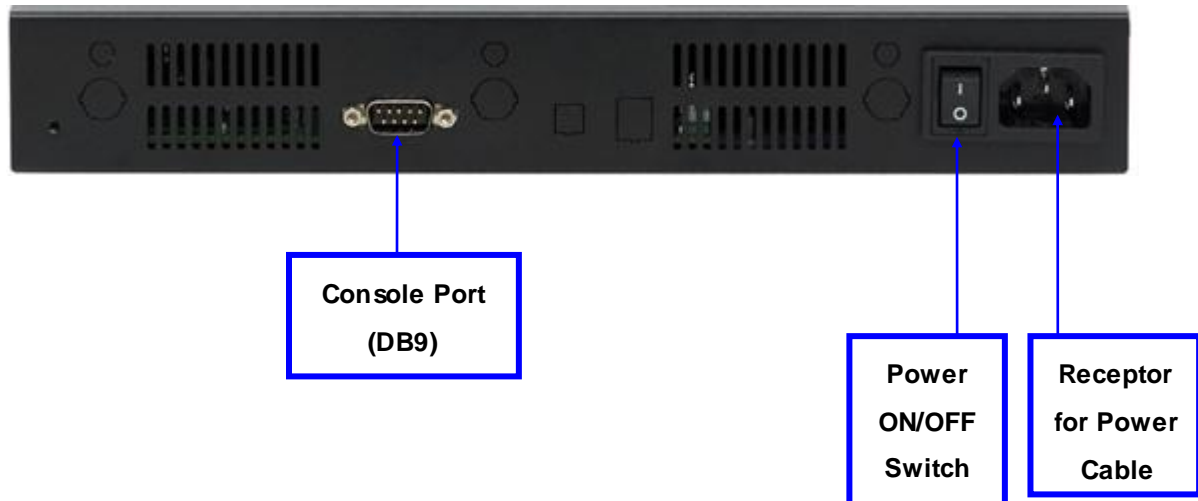
- Do not use the product in high humidity or high temperatures.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the product.
- Do not open or repair the case yourself. If the Product is too hot, turn off the power immediately and have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

## 1.2.2 SYSTEM REQUIREMENTS

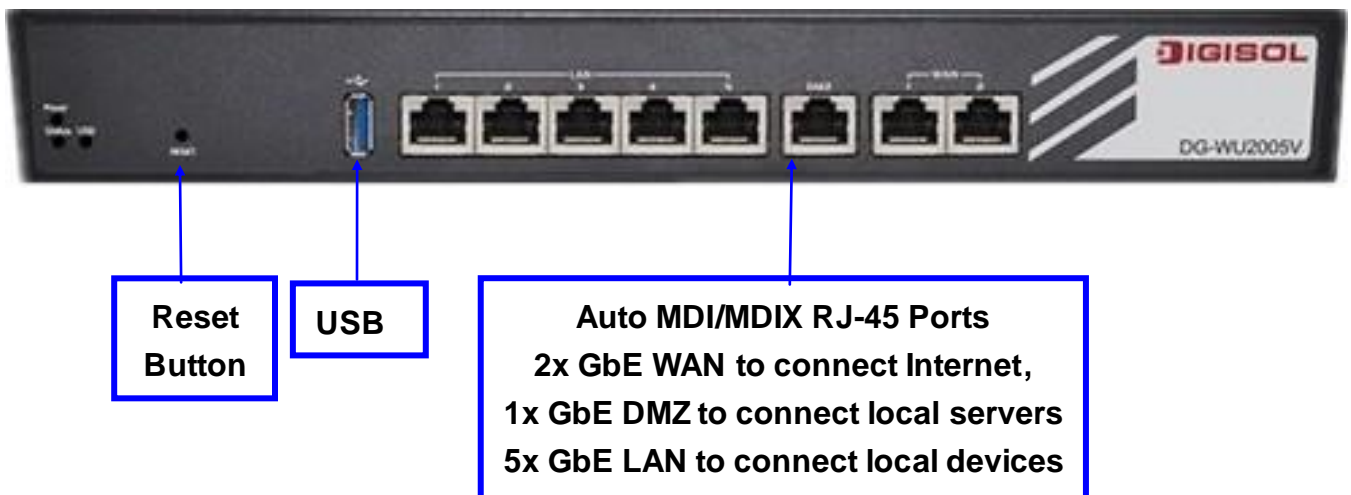
<b>Network Requirements</b>	<ul style="list-style-type: none"><li>• An Ethernet RJ45 cable or DSL modem</li><li>• 10/100/1000 Ethernet adapter on PC / NB.</li></ul>
<b>Web-based Configuration Utility Requirements</b>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"><li>• Windows®, Macintosh, or Linux-based operating system.</li><li>• An installed Ethernet adapter.</li></ul> <p><b>Browser Requirements:</b></p> <ul style="list-style-type: none"><li>• Internet Explorer 6.0 or higher</li><li>• Chrome 2.0 or higher</li><li>• Firefox 3.0 or higher</li><li>• Safari 3.0 or higher.</li></ul>
<b>CD Installation Wizard Requirements</b>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"><li>• Windows® 7 / 8, Vista®, or XP with Service Pack 2.</li><li>• An installed Ethernet adapter.</li><li>• CD-ROM drive.</li></ul>

### 1.2.3 Hardware Configuration

#### Rear View:



#### Front View:



## 1.2.4 LED Indicators



LED	Description
Power	OFF: Device is powered down.
	Green: Device is powered on.
Status	Green in flash: Device is in normal operation.
	Green in fast flash: Device is in recovery mode or abnormal state.
USB (for 3G/4G)	OFF: USB 3G/4G connection is not established.
	Green: USB 3G/4G connection is established.
	Green in flash: data packet transferred via USB 3G/4G
LAN-1 ~ LAN-5 / DMZ	Green: Ethernet connection is established.
	Green in flash: Data packet transferred via Ethernet.
	OFF: No Ethernet cable attached or Device not linked.
WAN-1 / WAN-2	Green: Ethernet connection is established.
	Green in flash: Data packet transferred through WAN.
	OFF: No Ethernet cable attached or Device not linked.

## Chapter 2 Getting Started

### 2.1 Connect Your Device

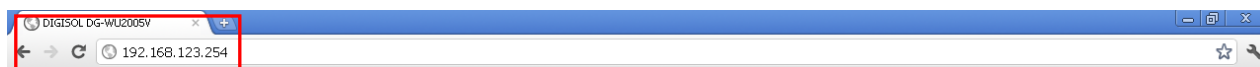
Before you can use this product, you need to connect your PC or NB to this gateway first. You can connect your PC to one of the LAN1~LAN5 ports through an Ethernet cable.

### 2.2 Easy Setup by Configuring Web UI

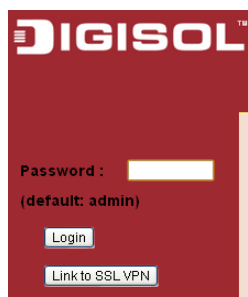
You can browse web UI to configure the device. Firstly you need to launch the Setup Wizard browser first and then the Setup Wizard will guide you step-by-step to finish the basic setup process.

#### **Browse to Activate the Setup Wizard**

Type in the IP Address (<http://192.168.123.254>)<sup>1</sup>



When you see the login page, type the password '**admin**' (Refer note2) and then click '**login**' button.



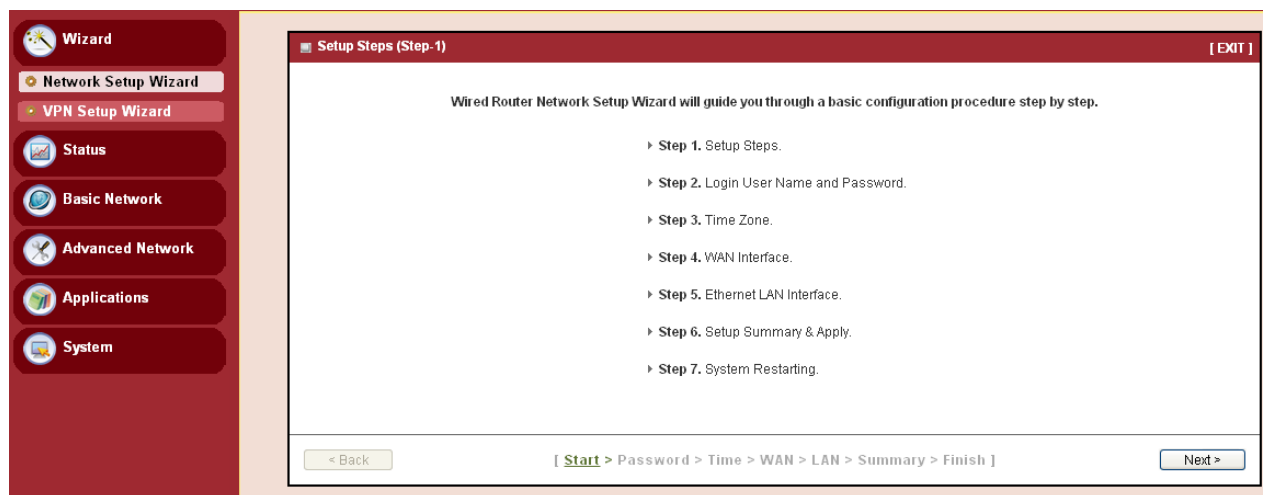
After login, select your language from the list.



- 
- 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.

## 2.2.1 Wizard

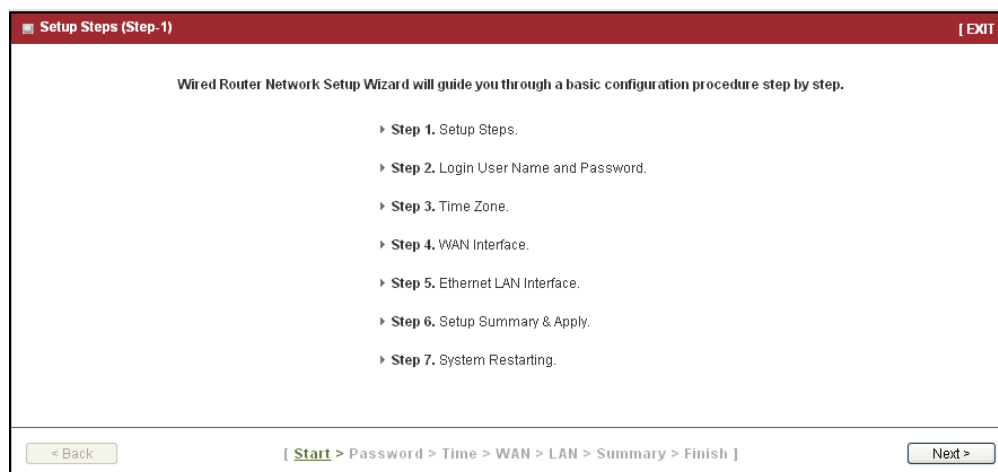
Select “**Wizard**” for basic network settings and VPN settings in a simple way. Or, you can go to **Basic Network** / **Advanced Network** / **Applications** / **System** to setup the configuration by your own selection.



### 2.2.1.1 Configure with the Network Setup Wizard

#### Step 1

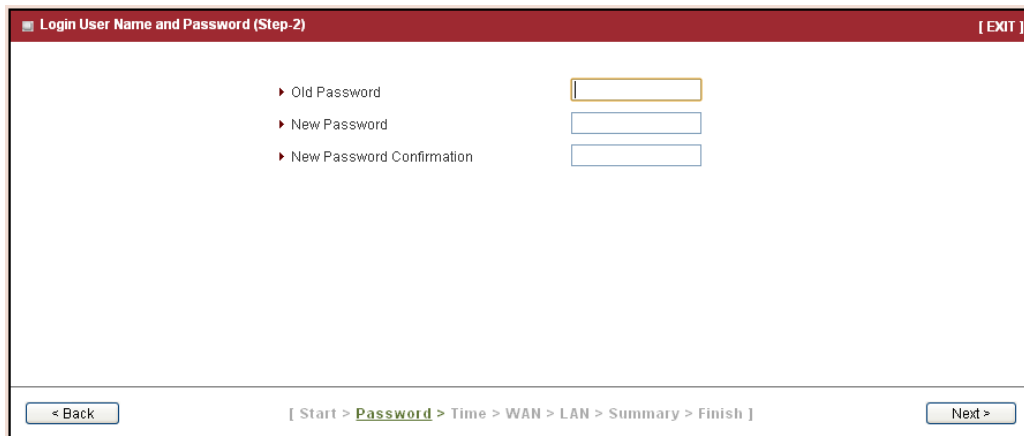
The network setup wizard will guide you to finish some basic settings, including login password, time zone, WAN interface and LAN interface. One “**Exit**” button at the upper-right corner of each window is provided for you to quit the setup process.



Press “**Next**” to start the wizard.

## Step 2: Change Password

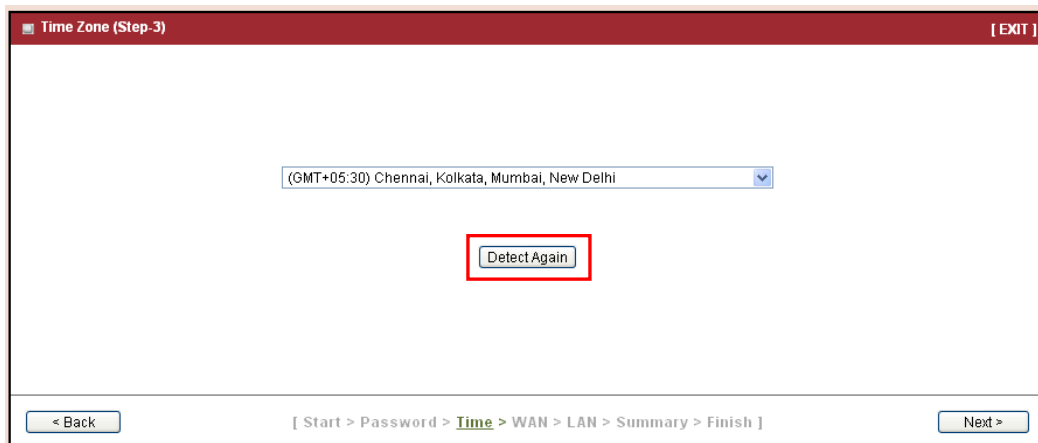
Password setting. You can change the login password of web UI here. It's strongly recommended that you change this login password from default value.



Press “**Next**” to continue.

## Step 3: Time Zone

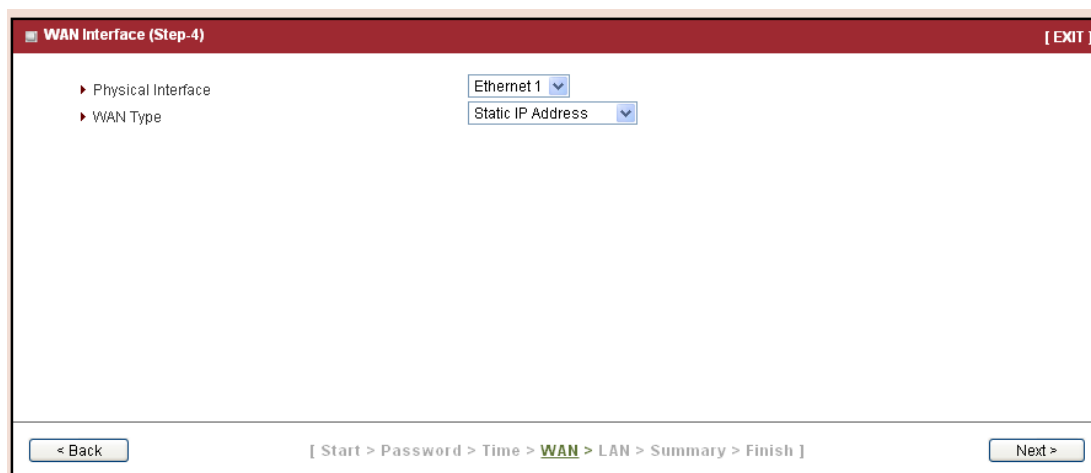
Time Zone setting. It will detect your time zone automatically. If the result of auto detection is not correct, you can press “**Detect Again**” button or select manually.



Press “**Next**” to continue.

## Step 4: WAN

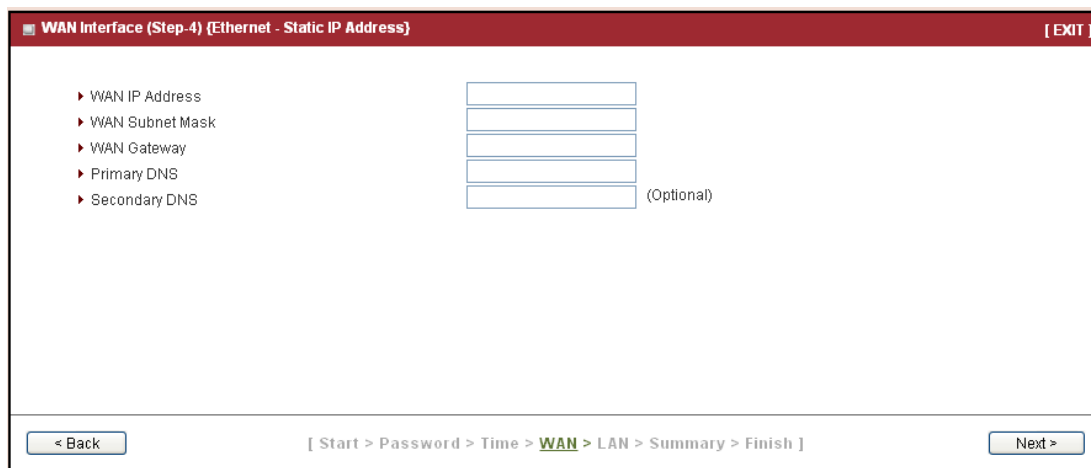
WAN Interface setting. Choose the type of WAN connection. You can select Ethernet WAN if you want to connect to Internet through fixed line. Or select USB 3G/4G if you want to connect to Internet through 3G/4G network. A variety of WAN types are available for Ethernet WAN connection.



Press “**Next**” to continue.

### Step 4-1: Ethernet (Static IP Address)

If you choose **Ethernet->Static IP Address**, you need to input all IP address that you get from ISP (Internet Service Provider) manually. This Static IP WAN Type option is usually chosen when you get a fixed IP address from ISP.



Press “**Next**” to continue.



### Step 4-2: Ethernet (Dynamic IP Address)

If you choose **Ethernet->Dynamic IP Address**, you can input host name or registered MAC address when your ISP requests it. In most cases, you can leave them as blank and go to next. This Dynamic IP WAN Type option is usually chosen when you get a dynamic IP address from ISP.

The screenshot shows a configuration window titled "WAN Interface (Step-4) (Ethernet - Dynamic IP Address)" with an "[EXIT]" button in the top right corner. The window contains two input fields: "Host Name" (with "(Optional)" text) and "ISP Registered MAC Address" (with a "Clone" button next to it). At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[ Start > Password > Time > WAN > LAN > Summary > Finish ]", and a "Next >" button.

Press “**Next**” to continue.

### Step 4-3: Ethernet (PPPoE)

If you choose **Ethernet->PPP over Ethernet** (so-called PPPoE), you need to input account and password that you get from ISP. For other fields, you can leave them as blank in most cases. This PPPoE WAN Type option is usually chosen when you use ADSL for WAN connection.

The screenshot shows a configuration window titled "WAN Interface (Step-4) (Ethernet - PPP over Ethernet)" with an "[EXIT]" button in the top right corner. The window contains six input fields: "PPPoE Account", "PPPoE Password", "Primary DNS", "Secondary DNS", "Service Name", and "Assigned IP Address". The last three fields have "(Optional)" text next to them. At the bottom, there is a navigation bar with a "< Back" button, a breadcrumb trail "[ Start > Password > Time > WAN > LAN > Summary > Finish ]", and a "Next >" button.

Press “**Next**” to continue.

### Step 4-4: Ethernet (PPTP)

If you choose **Ethernet->PPTP**, you need to input required dial-up information that you get from ISP. This PPTP WAN Type option is usually chosen when your ISP requests it.

The screenshot shows a web-based configuration window titled "WAN Interface (Step-4) (Ethernet - PPTP)" with an "[EXIT]" button in the top right corner. The window contains a list of configuration items on the left and corresponding input fields on the right:

- IP Mode: Dynamic IP Address (dropdown menu)
- WAN IP Address: [Empty text box]
- WAN Subnet Mask: [Empty text box]
- WAN Gateway: [Empty text box]
- Server IP Address / Name: [Empty text box]
- PPTP Account: [Empty text box]
- PPTP Password: [Empty text box]

At the bottom, there is a navigation bar with a "< Back" button, a progress indicator "[ Start > Password > Time > **WAN** > LAN > Summary > Finish ]", and a "Next >" button.

Press "**Next**" to continue.

### Step 4-5: Ethernet (L2TP)

If you choose **Ethernet->L2TP**, you need to input required dial-up information that you get from ISP. This L2TP WAN Type option is usually chosen when your ISP requests it.

The screenshot shows a web-based configuration window titled "WAN Interface (Step-4) (Ethernet - L2TP)" with an "[EXIT]" button in the top right corner. The window contains a list of configuration items on the left and corresponding input fields on the right:

- IP Mode: Dynamic IP Address (dropdown menu)
- WAN IP Address: [Empty text box]
- WAN Subnet Mask: [Empty text box]
- WAN Gateway: [Empty text box]
- Server IP Address / Name: [Empty text box]
- L2TP Account: [Empty text box]
- L2TP Password: [Empty text box]

At the bottom, there is a navigation bar with a "< Back" button, a progress indicator "[ Start > Password > Time > **WAN** > LAN > Summary > Finish ]", and a "Next >" button.

Press "**Next**" to continue.

## Step 5: LAN

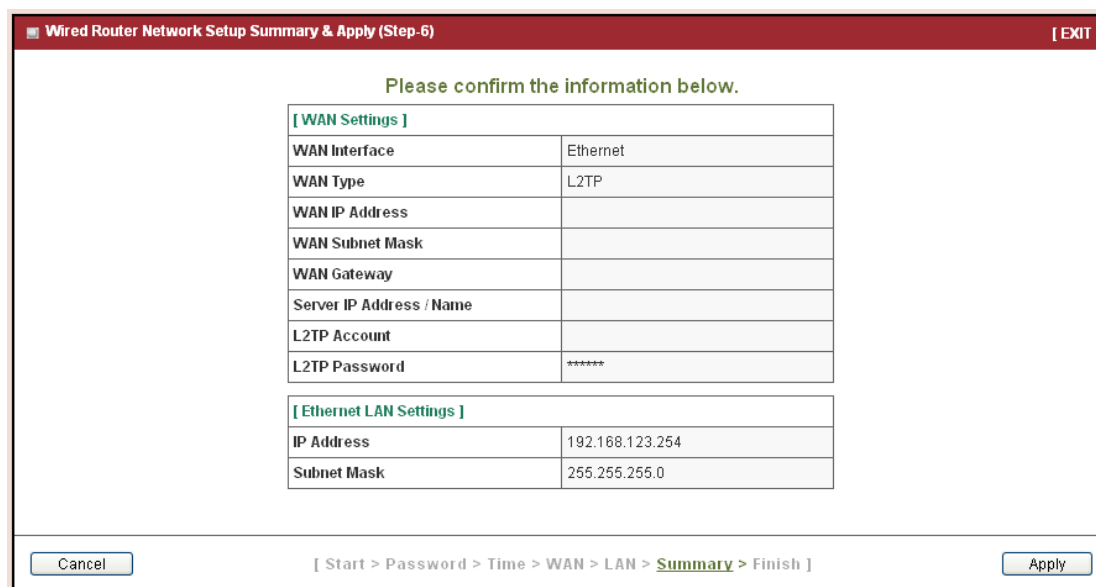
LAN Interface setting. Change the LAN IP address and subnet mask of this gateway. You can keep the default setting and go to next step.



Press “**Next**” to continue.

## Step 6: Confirm and Apply

Check the new settings again. If all information is correct, please press “**Apply**” button to save new settings. Then it will take 95 seconds to restart this gateway and make new settings effective.



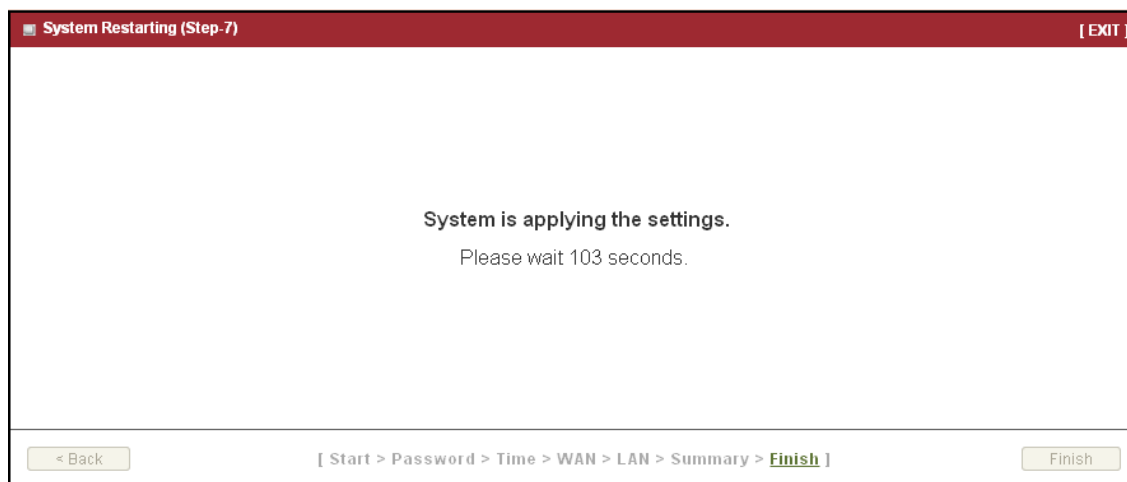
[ WAN Settings ]	
WAN Interface	Ethernet
WAN Type	L2TP
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Server IP Address / Name	
L2TP Account	
L2TP Password	*****

[ Ethernet LAN Settings ]	
IP Address	192.168.123.254
Subnet Mask	255.255.255.0

## Step 7: Counting Down

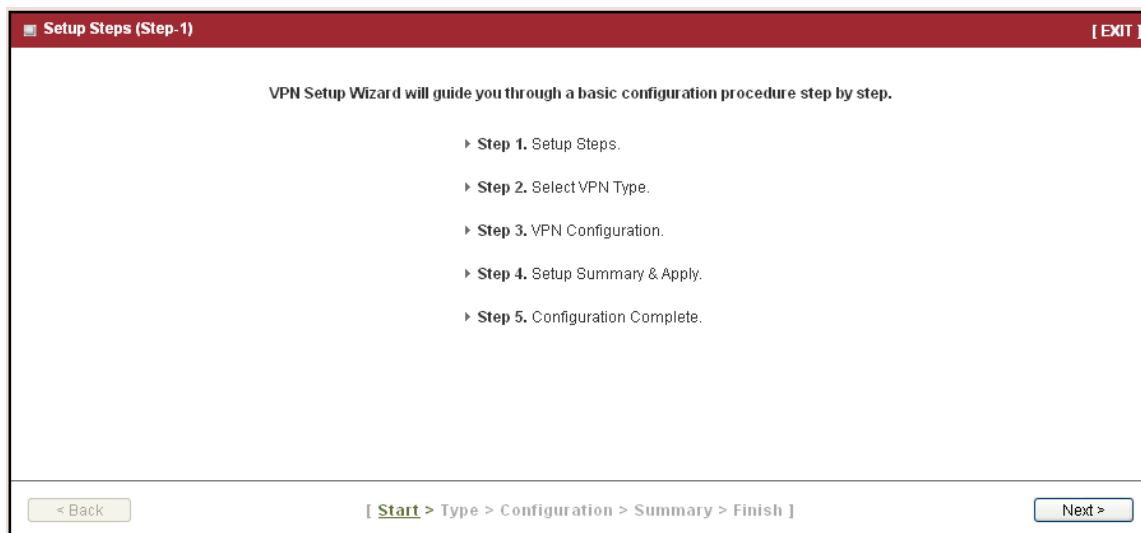
Configuration is completed. Press “**Finish**” button to close Setup Wizard and browser counts down for 65 seconds and provides you with “**Click here**” button to reconnect to the device.



## 2.2.1.2 Configure with the VPN Setup Wizard

### Step 1

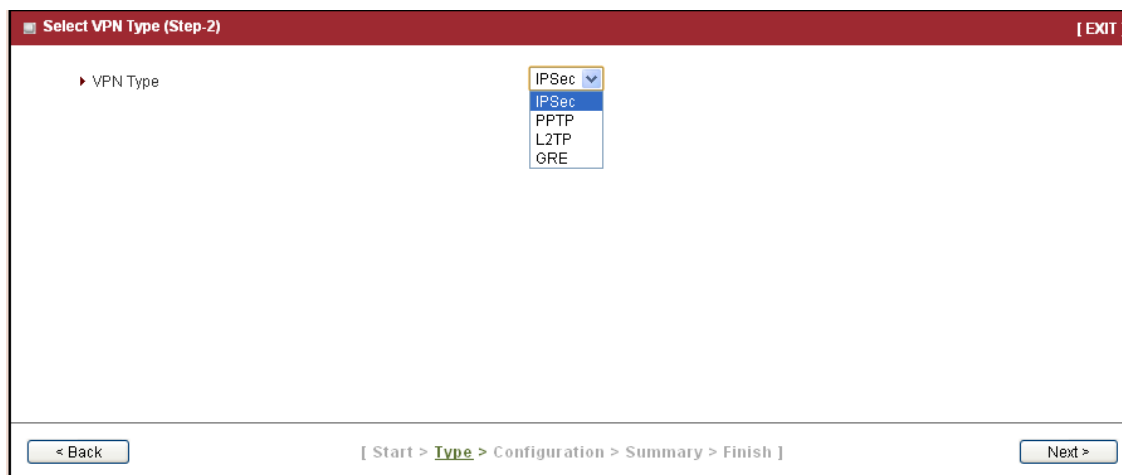
The VPN setup wizard will guide you to finish profiles of IPSec, PPTP and L2TP VPN connection quickly.



Press “**Next**” to start the wizard.

## Step 2: VPN Type

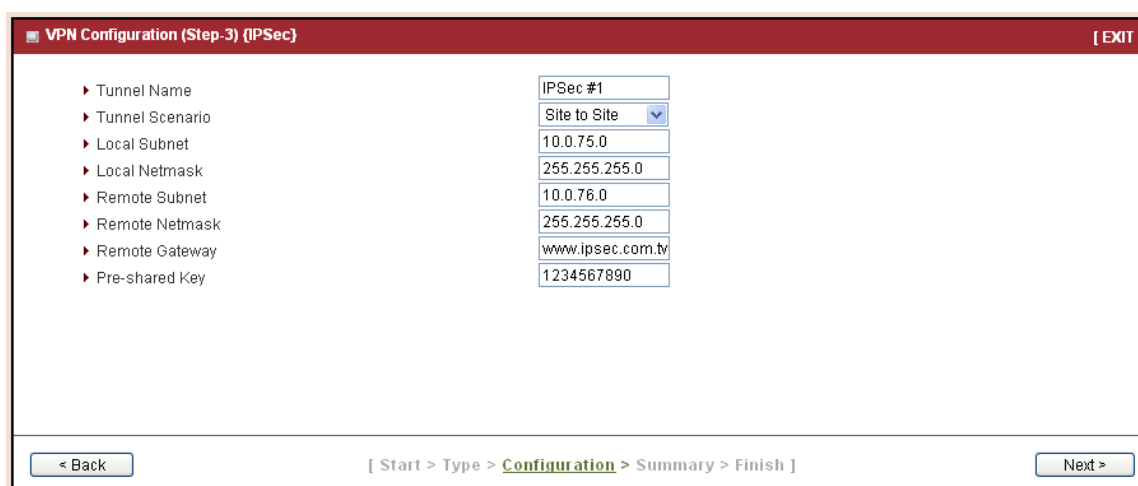
Select type of VPN connection you want to create. Here you can choose IPSec, PPTP, L2TP or GRE.



Press “Next” to continue.

## Step 2-1: IPSec

If you choose IPSec, there are five options of tunnel scenario which can be chosen. “Site to Site” is for two offices to create a VPN tunnel. “Site to Host” is for one office to create a VPN tunnel to the control center. “Host to Site” is for the device as the control center to create a VPN tunnel to a branch office. “Host to Host” is for creating a peer to peer secure tunnel.



“Dynamic VPN” is for remote users to connect to the device securely. For other options, please go to **Advanced Network >> VPN** to setup. Input the required network information and

pre-shared key for VPN connection.

For Dynamic VPN, you don't need to input network information of remote subnet and remote gateway.

VPN Configuration (Step-3) (IPSec) [EXIT]

▶ Tunnel Name

▶ Tunnel Scenario

▶ Local Subnet

▶ Local Netmask

▶ Remote Subnet

▶ Remote Netmask

▶ Remote Gateway

▶ Pre-shared Key

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

## Step 2-2: PPTP

If you choose PPTP, there are two options of modes can be chosen. Choose “**Client**” if you want this device to connect to another PPTP server. Or choose “**Server**” if you want other PPTP clients to connect to it.

Select VPN Type (Step-2) [EXIT]

▶ VPN Type

PPTP Server

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

If you choose PPTP Client, please input tunnel name, IP/FQDN of PPTP server, username/password, authentication and MPPE options. Please make sure these settings are

accepted by PPTP server. Otherwise, remote PPTP server will reject the connection.

Select VPN Type (Step-2) [EXIT]

VPN Type PPTP Client

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

If you choose PPTP Server, please select options of authentication and MPPE. You also need to create a set of username and password for PPTP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to **Advanced Network >> VPN >> PPTP** to add more users.

VPN Configuration (Step-3) (PPTP Server) [EXIT]

Authentication Protocol ☐ PAP ☐ CHAP ☐ MS\_CHAP ☐ MS\_CHAPv2

MPPE Encryption ☐ Enable 40bits

User Account Account: Password:

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

### Step 2-3: L2TP

If you choose L2TP, there are two options of mode that can be chosen. Choose “**Client**” if you want this device to connect to another L2TP server. Or choose “**Server**” if you want other L2TP clients to connect to it.

Select VPN Type (Step-2) [EXIT]

VPN Type

L2TP Client

Client

Server

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

If you choose L2TP Client, please input tunnel name, IP/FQDN of L2TP server, username/password, authentication and MPPE options. Please make sure these settings are accepted by L2TP server. Otherwise, remote L2TP server will reject the connection.

VPN Configuration (Step-3) {L2TP Client} [EXIT]

L2TP Client Name

Peer IP/FQDN

User Account

Default Gateway/Remote Subnet

Authentication Protocol

MPPE Encryption

L2TP #1

Account Password:

Remote Subnet

☐ PAP ☐ CHAP ☐ MS\_CHAP ☐ MS\_CHAPv2

☐ Enable

< Back [ Start > Type > Configuration > Summary > Finish ] Next >

Press “**Next**” to continue.

If you choose L2TP Server, please select options of authentication and MPPE. You also need to create a set of username and password for L2TP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to **Advanced Network >> VPN >> L2TP** to add more users.



VPN Configuration (Step-3) (L2TP Server)
[EXIT]

▶ Authentication Protocol
▶ MPPE Encryption
▶ User Account

☐ PAP
☐ CHAP
☐ MS\_CHAP
☐ MS\_CHAPv2  
☐ Enable
40bits  
Account:
Password:

< Back
[ Start > Type > Configuration > Summary > Finish ]
Next >

Press “**Next**” to continue.

### Step 3: Confirm and Apply

Confirm new settings. If all new settings are correct, please press “**Apply**” button to save these new settings and make them effective.

Setup Summary & Apply (Step-4)
[EXIT]

Please confirm the information below.

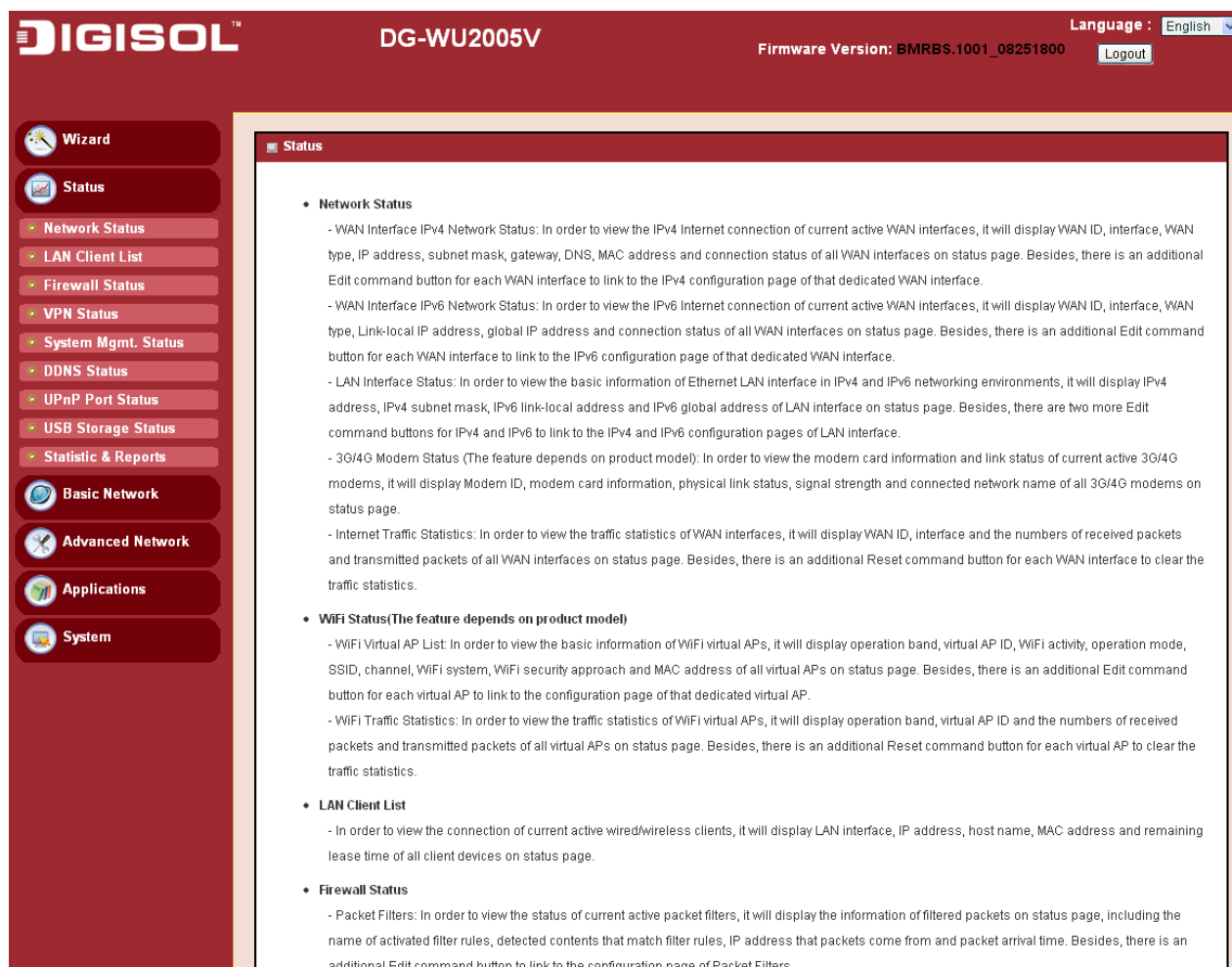
[ VPN Type ]	
VPN Type	IPSec

[ VPN Settings ]	
Tunnel Name	IPSec #1
Tunnel Scenario	Site to Site
Local Subnet	10.0.75.0
Local Netmask	255.255.255.0
Remote Subnet	10.0.76.0
Remote Netmask	255.255.255.0
Remote Gateway	www.ipsec.com.tw
Pre-shared Key	1234567890

Cancel
[ Start > Type > Configuration > Summary > Finish ]
Apply

## 2.2.2 Status

There are 4 kinds of system status to be shown at this window. They are Network Status, LAN Client list, Firewall Status, VPN Status and System Management Status.



**DIGISOL™** **DG-WU2005V** Firmware Version: BMRBS.1001\_08251800 Language: English Logout

**Status**

- Network Status**
  - WAN Interface IPv4 Network Status: In order to view the IPv4 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, IP address, subnet mask, gateway, DNS, MAC address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv4 configuration page of that dedicated WAN interface.
  - WAN Interface IPv6 Network Status: In order to view the IPv6 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, Link-local IP address, global IP address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv6 configuration page of that dedicated WAN interface.
  - LAN Interface Status: In order to view the basic information of Ethernet LAN interface in IPv4 and IPv6 networking environments, it will display IPv4 address, IPv4 subnet mask, IPv6 link-local address and IPv6 global address of LAN interface on status page. Besides, there are two more Edit command buttons for IPv4 and IPv6 to link to the IPv4 and IPv6 configuration pages of LAN interface.
  - 3G/4G Modem Status (The feature depends on product model): In order to view the modem card information and link status of current active 3G/4G modems, it will display Modem ID, modem card information, physical link status, signal strength and connected network name of all 3G/4G modems on status page.
  - Internet Traffic Statistics: In order to view the traffic statistics of WAN interfaces, it will display WAN ID, interface and the numbers of received packets and transmitted packets of all WAN interfaces on status page. Besides, there is an additional Reset command button for each WAN interface to clear the traffic statistics.
- WiFi Status(The feature depends on product model)**
  - WiFi Virtual AP List: In order to view the basic information of WiFi virtual APs, it will display operation band, virtual AP ID, WiFi activity, operation mode, SSID, channel, WiFi system, WiFi security approach and MAC address of all virtual APs on status page. Besides, there is an additional Edit command button for each virtual AP to link to the configuration page of that dedicated virtual AP.
  - WiFi Traffic Statistics: In order to view the traffic statistics of WiFi virtual APs, it will display operation band, virtual AP ID and the numbers of received packets and transmitted packets of all virtual APs on status page. Besides, there is an additional Reset command button for each virtual AP to clear the traffic statistics.
- LAN Client List**
  - In order to view the connection of current active wired/wireless clients, it will display LAN interface, IP address, host name, MAC address and remaining lease time of all client devices on status page.
- Firewall Status**
  - Packet Filters: In order to view the status of current active packet filters, it will display the information of filtered packets on status page, including the name of activated filter rules, detected contents that match filter rules, IP address that packets come from and packet arrival time. Besides, there is an additional Edit command button to link to the configuration page of Packet Filters.

## 2.2.2.1 Network Status

In Network Status page, you can review lots of information of network status, including a connection diagram, WAN IPv4 status, WAN IPv6 status, LAN status, 3G/4G modem status and Internet Traffic Statistics. You can also check the device time at the bottom of this page.

### Connection Diagram



1. 3G/4G Icon: Indicates if 3G/4G connection is established or not.
2. XDSL/Cable Icon: Indicates if Ethernet WAN connection is established or not.
3. Wired Client Icon: Indicates how many Ethernet clients are connected now.

### WAN Interface IPv4 Network Status

Displays WAN type, IPv4 information, subnet mask, gateway, DNS, MAC information and connection status of multiple WAN interfaces in IPv4 networking. Press “**Edit**” button if you want to change settings.

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	L2TP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:17:7C:4B:A8:73	Disconnected	<a href="#">Connect</a> <a href="#">Edit</a>
WAN-2		Disable							<a href="#">Edit</a>
WAN-3		Disable							<a href="#">Edit</a>

### WAN Interface IPv6 Network Status

Display WAN type, IPv6 information, and connection status of multiple WAN interfaces in IPv6 networking. Press “**Edit**” button if you want to change the settings.

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				<a href="#">Edit</a>

## **LAN Interface Status**

Displays IPv4 and IPv6 information of local network. Press “**Edit**” button if you want to change the settings.

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	<a href="#">Edit IPv4</a> <a href="#">Edit IPv6</a>

## **3G/4G Modem Status**

Displays modem card information, link status, signal strength and network (carrier) name of 3G/4G connection.

3G/4G Modem Status <a href="#">Refresh</a>					
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
USB 3G/4G	N/A	Disconnected	N/A	N/A	<a href="#">Detail</a>

## **Internet Traffic Statistics**

Displays number of transmitted packets and received packets of each WAN interface.

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

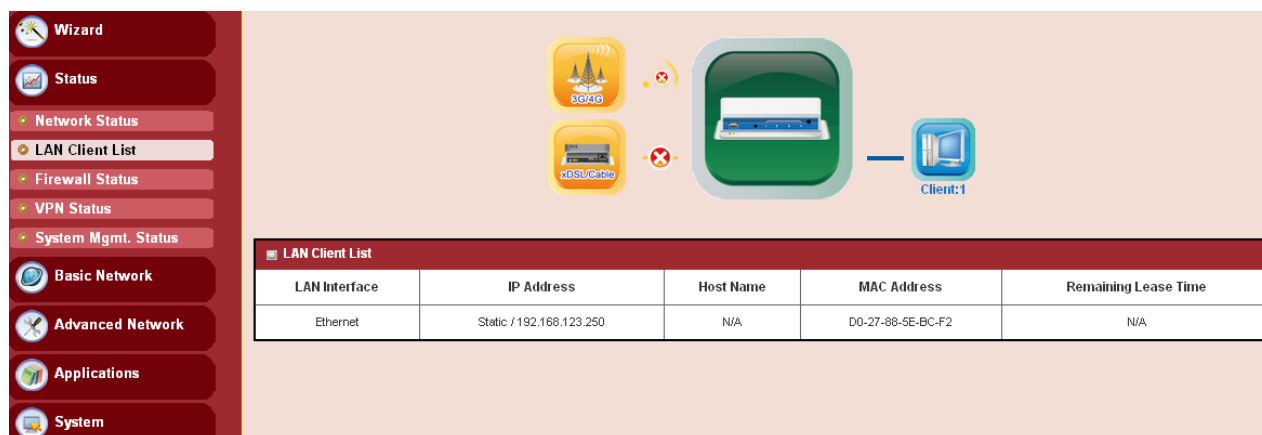
## **Device Time**

Display current time information of device.

Device Time: Tue, 01 Jan 2013 06:12:13 +0530

### 2.2.2.2 LAN Client List

Displays the LAN client information like IP address, host name, MAC address and remaining lease time.



LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Static / 192.168.123.250	N/A	D0-27-88-5E-BC-F2	N/A

### 2.2.2.3 Firewall Status

In Firewall Status page, you can review information of filter status, including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and other options of firewall.

#### Packet Filters

Displays all detected contents of firing activated packet filter rules.

Firewall Status			
Packet Filters <span>Edit</span> <span>[+]</span>			
Activated Filter Rule	Detected Contents	IP	Time

#### URL Blocking

Displays all blocked URLs of firing activated URL blocking rules.

URL Blocking <span>Edit</span> <span>[+]</span>			
Activated Blocking Rule	Blocked URL	IP	Time

#### Web Content Filters

Displays all detected contents of firing activated Web content filter rules.

Web Content Filters <span>Edit</span> <span>[+]</span>			
Activated Filter Rule	Detected Contents	IP	Time

## MAC Control

Displays all blocked MAC addresses of firing activated MAC control rules.

MAC Control <span>Edit</span> <span>[+]</span>			
Activated Control Rule	Blocked MAC Addresses	IP	Time

## Application Filters

Displays all filtered applications of firing activated application filter rules.

Application Filters <span>Edit</span> <span>[+]</span>			
Filtered Application Category	Filtered Application Name	IP	Time

## IPS

Displays all events of firing activated rules of IPS.

IPS <span>Edit</span> <span>[+]</span>		
Detected Intrusion	IP	Time

## Options

Display option settings of fire wall.

Options <span>Edit</span> <span>[+]</span>			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

### 2.2.2.4 VPN Status

In VPN Status page, you can review information of VPN status, including IPSec status, PPTP Server status, PPTP Client status, L2TP Server status, L2TP Client status and SSL VPN Server status.

## IPSec Status

Displays the status of all activated tunnels of IPSec.

IPSec Status <span>Edit</span>					
Tunnel Name	Tunnel Scenario	Local Subnets	Remote IP/FQDN	Remote Subnets	Status

## PPTP Server Status

Displays the status of all activated accounts of PPTP server.

PPTP Server Status <span>Edit</span>				
User Name	Peer IP/FQDN	Peer Virtual IP	Peer Call ID	Status

### **PPTP Client Status**

Displays the status of all activated PPTP clients.

PPTP Client Status <span>Edit</span>					
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

### **L2TP Server Status**

Displays the status of all activated accounts of L2TP server.

L2TP Server Status <span>Edit</span>				
User Name	Peer IP/FQDN	Virtual IP	Peer Call ID	Status

### **L2TP Client Status**

Displays the status of all activated L2TP clients.

L2TP Client Status <span>Edit</span>					
L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

### **SSL VPN Server Status**

Displays the status of all activated accounts of SSL VPN server.

SSL VPN Server Status <span>Edit</span>			
User Name	Remote IP/FQDN	Virtual IP	Status

## **2.2.2.5 System Management Status**

In System Management Status page, you can review information of SNMP and TR-069 status.

### **SNMP Linking Status**

Displays information of SNMP linking.

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

### **SNMP Trap Information**

Displays information of SNMP traps.

SNMP Trap Information		
Trap Level	Time	Trap Event

## TR-069 Status

Displays link status of TR-069.

TR-069 Status	
Link Status	
Off	

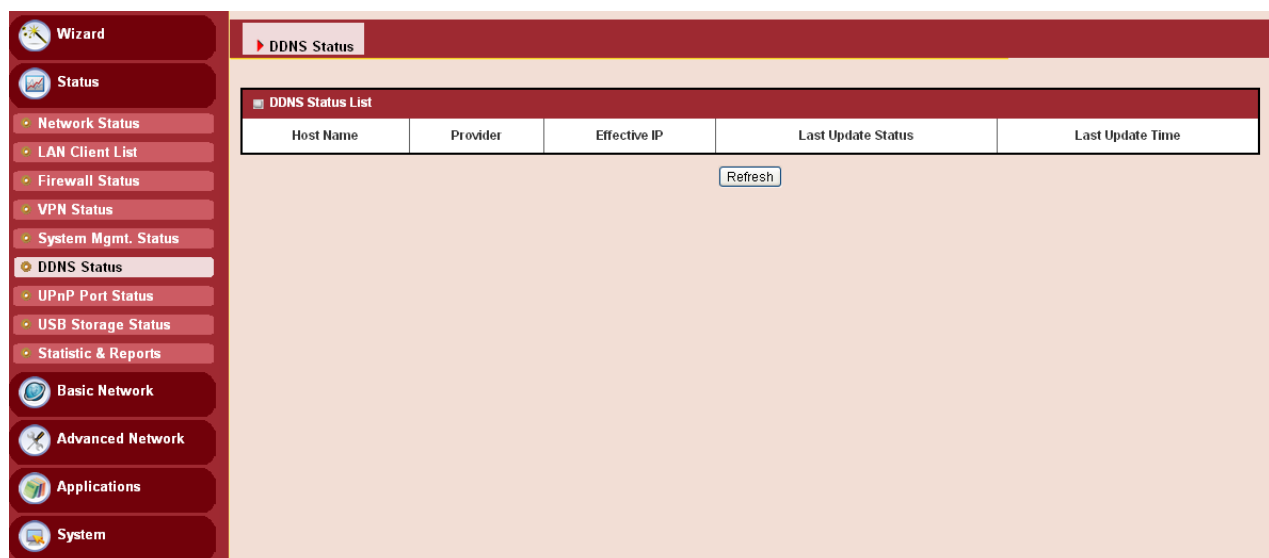
## UPnP Status

Displays UPnP status.

UPnP Status			
Protocol	Internal Port	External Port	Action

## 2.2.2.6 DDNS Status

In DDNS Status page, you can review information of DDNS status.

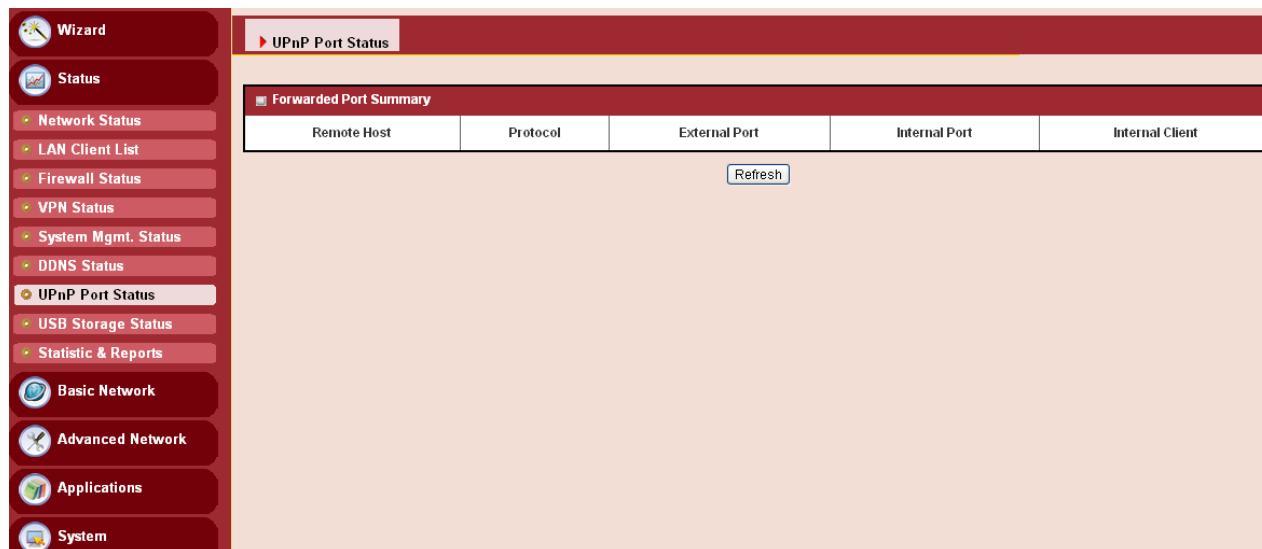


DDNS Status List				
Host Name	Provider	Effective IP	Last Update Status	Last Update Time
Refresh				



## 2.2.2.7 UPnP Status

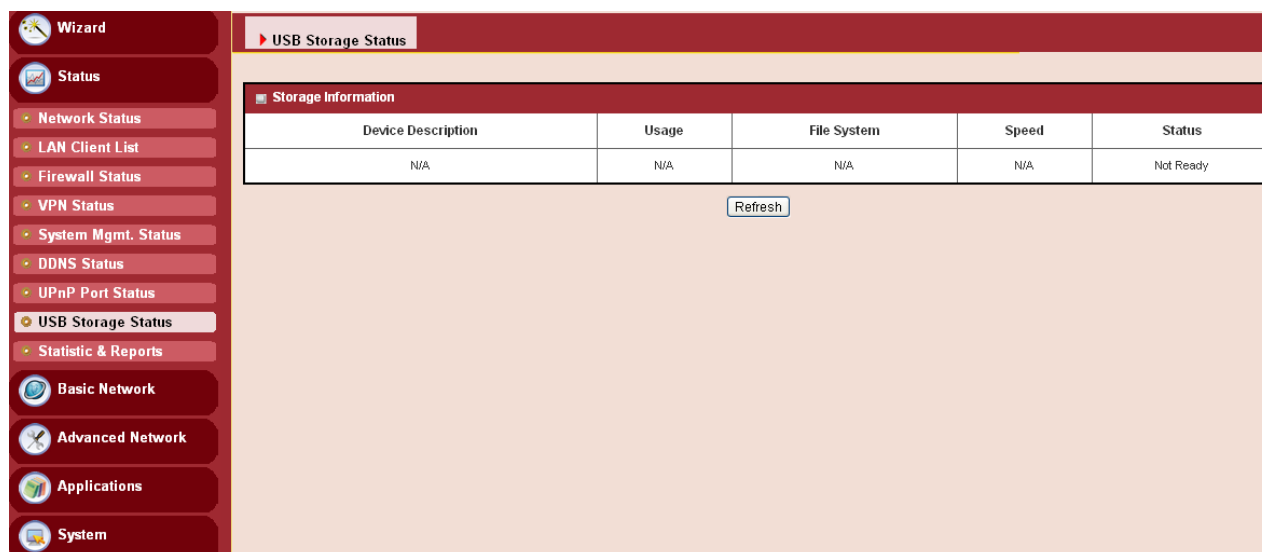
In UPnP Status page, you can review information of UPnP status.



Remote Host	Protocol	External Port	Internal Port	Internal Client
Refresh				

## 2.2.2.8 Storage Status

In Storage status page, you can review information of storage status, including device description, usage, file system, speed and status.



Device Description	Usage	File System	Speed	Status
N/A	N/A	N/A	N/A	Not Ready

Refresh

## 2.2.2.9 Statistics and Reports

In Statistics and reports status page, you can review information of statistics and reports.

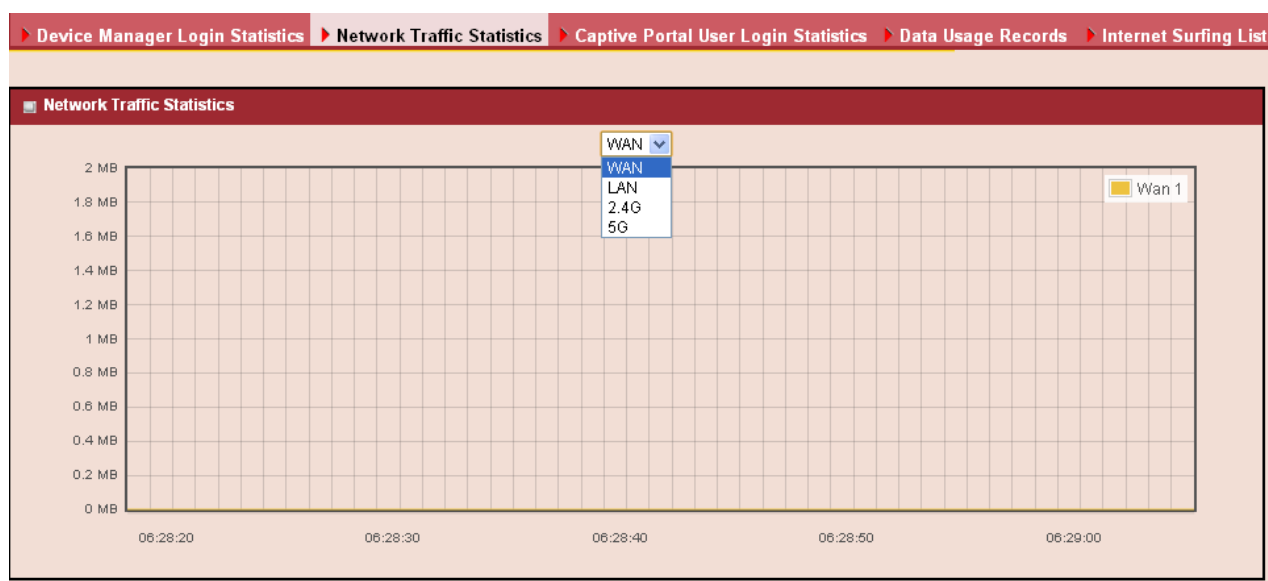
### Device Manager Login Status

Displays device management status like, user name, protocol type, IP address, user level and duration time.

<a href="#">Device Manager Login Statistics</a> <a href="#">Network Traffic Statistics</a> <a href="#">Captive Portal User Login Statistics</a> <a href="#">Data Usage Records</a> <a href="#">Internet Surfing List</a>				
Device Manager Login Statistics				
User Name	Protocol Type	IP Address	User Level	Duration Time
admin	http/https	192.168.123.250	Admin	2013/01/01/00/39~
<a href="#">Previous</a> <a href="#">Next</a> <a href="#">First</a> <a href="#">Last</a> <a href="#">Export (.xml)</a> <a href="#">Export (.csv)</a> <a href="#">Refresh</a>				

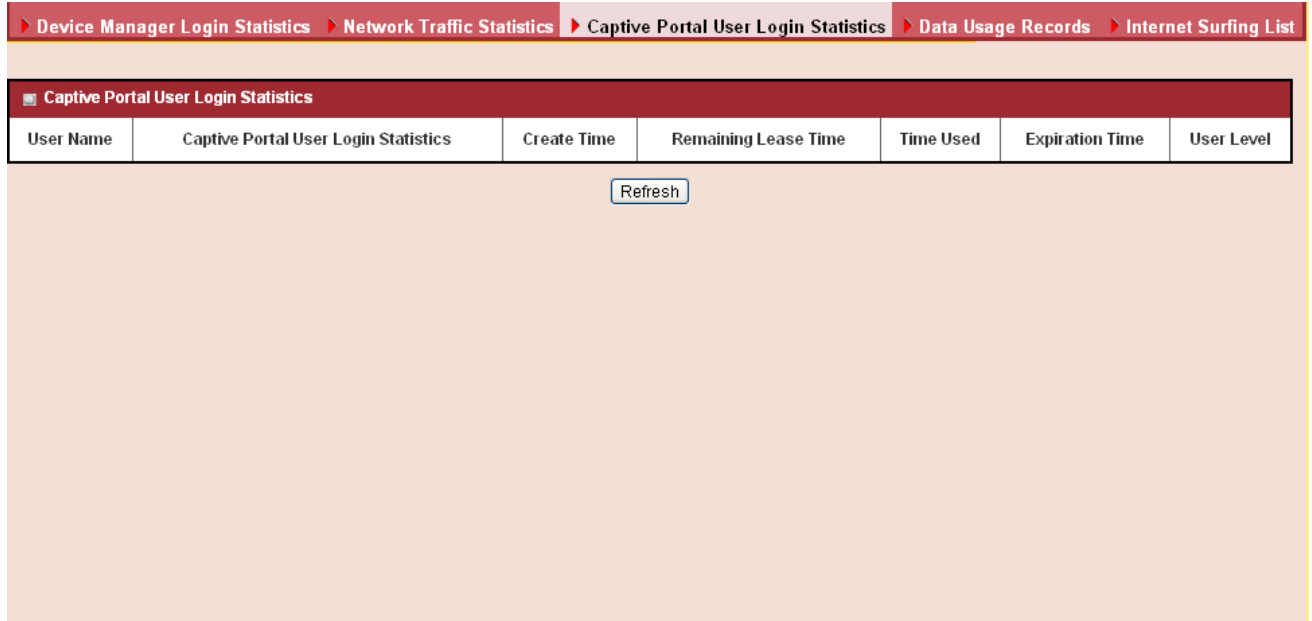
### Network Traffic Statistics

Displays network traffic status of the WAN, LAN, 2.4G and 5G networks.



## Captive portal user login Statistics

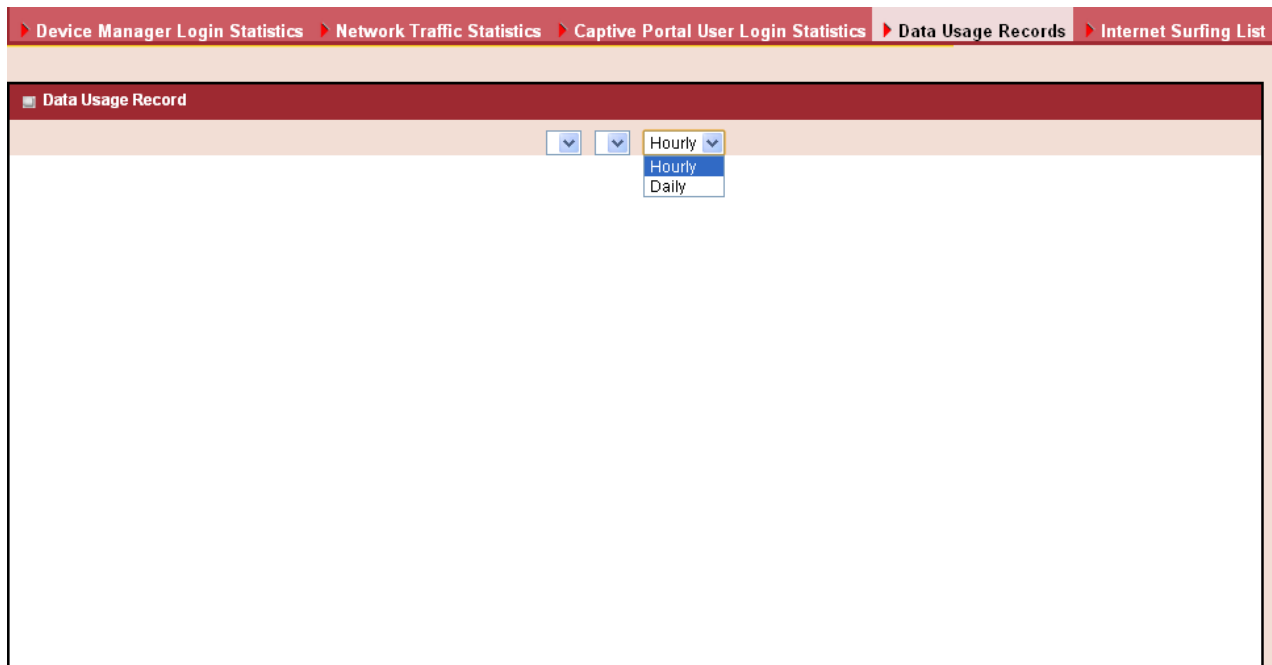
Displays captive portal user login status, including user name, captive portal user login statistics, create time, remaining lease time, time used, expiration time and user level.



User Name	Captive Portal User Login Statistics	Create Time	Remaining Lease Time	Time Used	Expiration Time	User Level
Refresh						

## Data usage record

Displays the data usage records.



## **Internet surfing list**

Displays the internet surfing list including, user name, protocol, internet IMP and port, MAC, external IMP & port and Duration time.

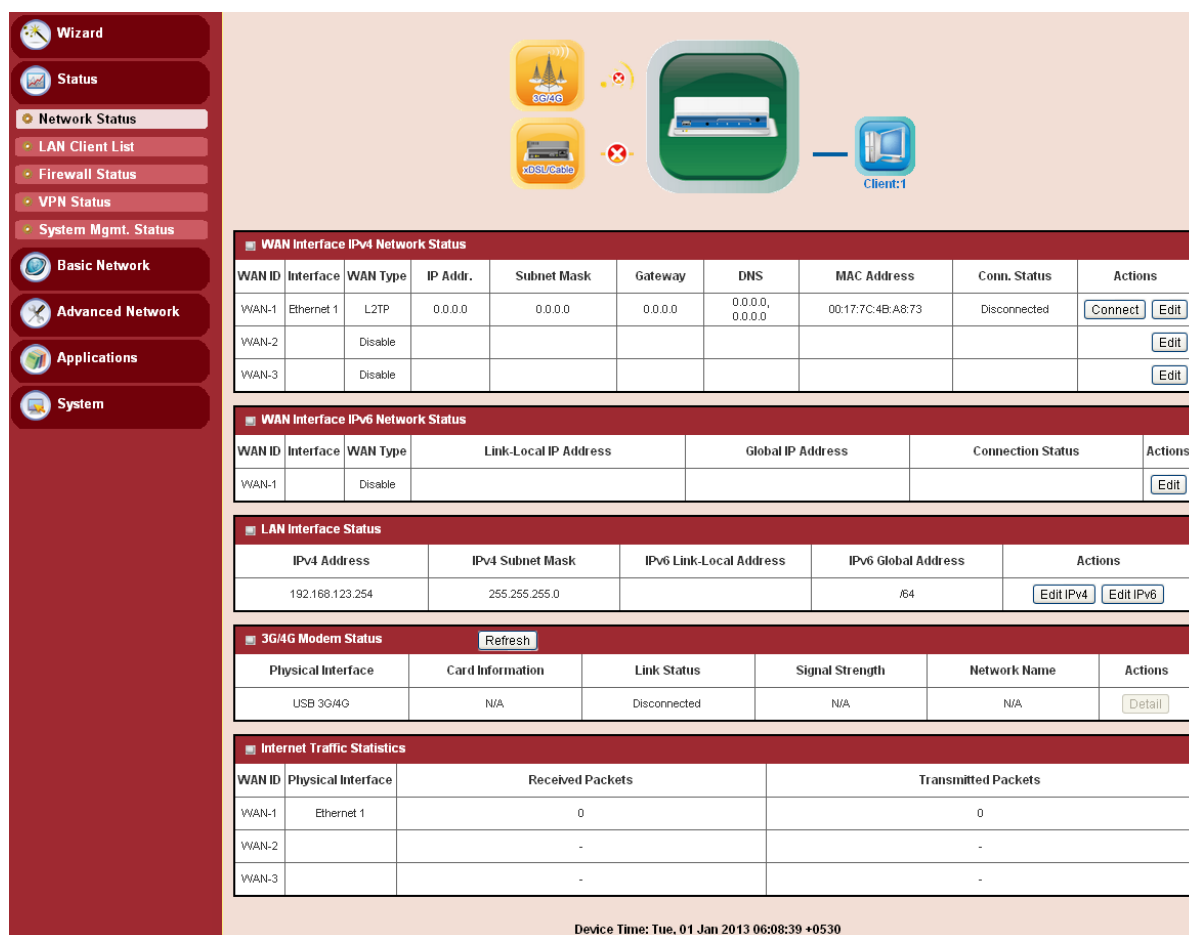
▶ Device Manager Login Statistics ▶ Network Traffic Statistics ▶ Captive Portal User Login Statistics ▶ Data Usage Records ▶ Internet Surfing List					
Internet Surfing List					
User Name	Protocol	Internal IP & Port	MAC	External IP &Port	Duration Time
	TCP	192.168.123.250:3009	d0:27:88:5e:bc:f2	192.168.123.254:80	2013/01/01/01/22~
<div>PreviousNextFirstLastExport (.xml)Export (.csv)Refresh</div>					

## 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.



**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	L2TP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	00:17:C:4B:A8:73	Disconnected	<a href="#">Connect</a> <a href="#">Edit</a>
WAN-2		Disable							<a href="#">Edit</a>
WAN-3		Disable							<a href="#">Edit</a>

**WAN Interface IPv6 Network Status**

WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				<a href="#">Edit</a>

**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	<a href="#">Edit IPv4</a> <a href="#">Edit IPv6</a>

**3G/4G Modem Status** [Refresh](#)

Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
USB 3G/4G	N/A	Disconnected	N/A	N/A	<a href="#">Detail</a>

**Internet Traffic Statistics**

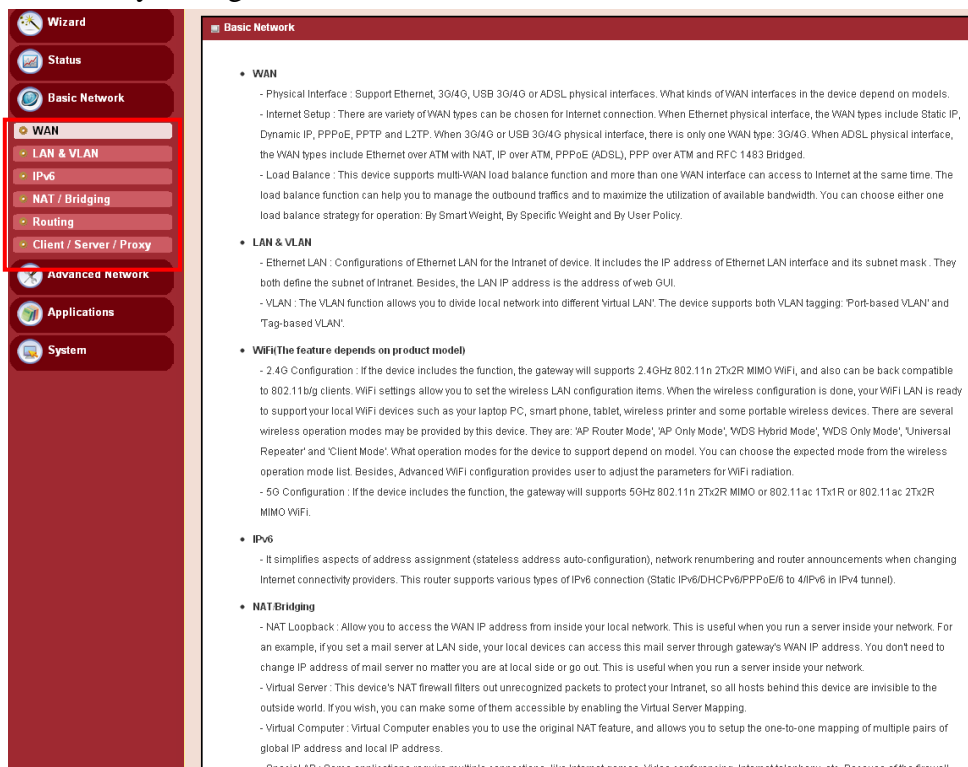
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	Ethernet 1	0	0
WAN-2		-	-
WAN-3		-	-

Device Time: Tue, 01 Jan 2013 06:08:39 +0530

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

## 3.1 Basic Network

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

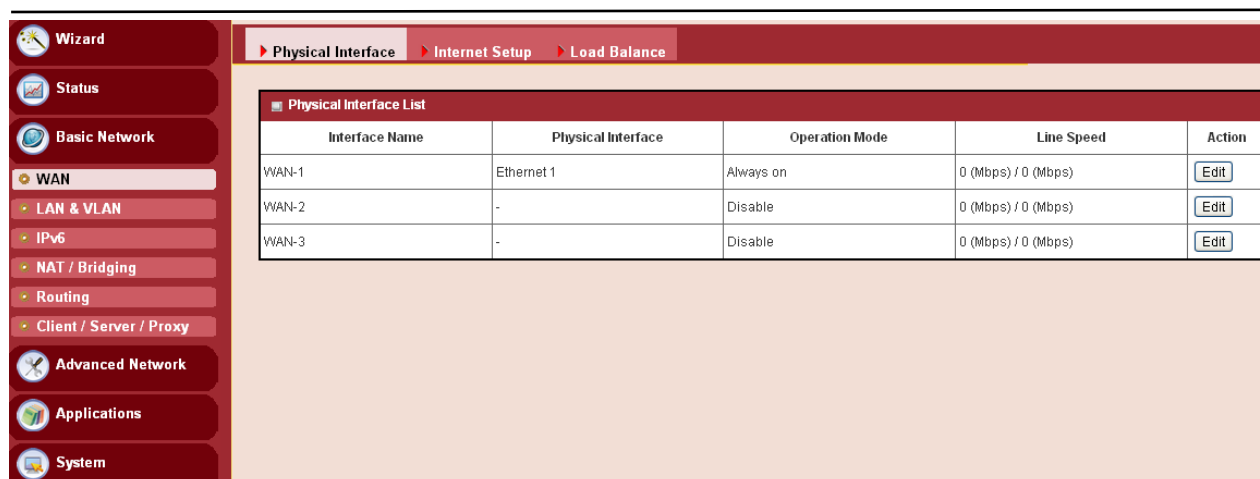


### 3.1.1 WAN Setup

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

**Ethernet WAN:** The product has two RJ45 Ethernet WAN ports. Please plug in RJ45 cable from your external DSL modem and follow UI setting to setup.

**USB 3G/4G WAN:** The product has one USB port for 3G/4G access, please plug in your USB 3G/4G modem dongle 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 operate as the primary internet connection; the interface WAN-2 / WAN-3 are disabled.

▶ 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)	<div>Edit</div>
WAN-2	-	Disable	0 (Mbps) / 0 (Mbps)	<div>Edit</div>
WAN-3	-	Disable	0 (Mbps) / 0 (Mbps)	<div>Edit</div>

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 options for this item.

**Always on:** Set this WAN interface to be active all the time. It means two or more Internet connections will be established simultaneously, and outgoing data will be transferred through these WAN connections based on load balance policies. This mode is especially suitable for high bandwidth requirement, such as video stream transmission.

**Failover:** Set this WAN interface to be a backup WAN connection. This WAN interface won’t be active until primary WAN connection is failed. If you specified a certain WAN interface as a “**Failover**” WAN, you have to further identify which WAN interface is to

be failover and fallback.

▶ Operation Mode	Failover ▼	WAN-1 ▼	Seamless <input type="checkbox"/> Enable
------------------	------------	---------	--

For the example above, if WAN-1 connection is broken, this gateway will try to failover the Internet connection to this WAN interface automatically. When WAN-1 connection becomes available again, the Internet connection will switch back to WAN-1 automatically.

Besides, for some mission-critical applications, this gateway supports “**Seamless failover**”<sup>3</sup> to shorten the switch time between WAN interface failover and fallback. That is, if an interface serves as a “**Seamless Failover**” WAN, the WAN connection will be activated after the system has been booted up normally, even without data flow in it. When the primary connection is broken, fast switching data flow to the WAN interface is the major concern for “**Seamless Failover**”.

**Disable:** Deactivate this WAN interface.

3. **Line Speed:** You can specify the downstream / upstream speed (Mbps) 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 requires a VLAN tag which has 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 three physical WAN interfaces that you can configure one by one to get proper internet connection setup. They include the Ethernet WANs - 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).

▶ Physical Interface▶ Internet Setup▶ Load Balance

Internet Connection List

Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet 1	Always on	L2TP	<a href="#">Edit</a>
WAN-2	-	Disable	-	<a href="#">Edit</a>
WAN-3	-	Disable	-	<a href="#">Edit</a>

3 Please note your ISP will charge the connection fee even if it's set to seamless failover.



### 3.1.1.2.1 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. There are 5 Internet connection types for Ethernet physical interface. They are “Static IP”, “Dynamic IP”, “PPP over Ethernet”, “PPTP” and “L2TP” as below.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet 1	Always on	L2TP	<a href="#">Edit</a>
WAN-2	-	Disable	-	<a href="#">Edit</a>
WAN-3	-	Disable	-	<a href="#">Edit</a>

#### ■ Dynamic IP Address

Internet Connection Configuration ( WAN - 1 )	
Item	Setting
▶ WAN Type	Dynamic IP <input type="button" value="v"/>
<b>Dynamic IP WAN Type Configuration</b>	
Item	Setting
▶ Host Name	<input type="text"/> (Optional)
▶ ISP Registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
▶ Connection Control	Auto-reconnect (Always on) <input type="button" value="v"/>
▶ 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 <input type="button" value="v"/>
▶ WAN IP Alias	<input type="checkbox"/> Enable <input type="text"/>

- WAN Type:** Choose “Dynamic IP Address” from the drop down list.
- 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 down list: “Auto-reconnect (Always on)”, “Dial-on-demand”, or “Manually”. If you select “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 you choose "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. Please be noted, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will disappear since it is "Auto-reconnect (Always on)".

5. **Maximum Idle Time:** The default value is 600 seconds, you can change it if required. The setting is required when the Connection Control is not "Auto-reconnect (Always on)".
6. **MTU:** Most ISP's offer MTU value to users. The default value is 0 (auto).
7. **NAT:** If you disable this option, it will act with a non-NAT function.
8. **Network Monitoring:** It is a checking mechanism design to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checks, the timeout of one check, response latency threshold, fail times threshold, touched target 1 and touched target 2.
9. **IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.
10. **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 user 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	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
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

- WAN Type:** Choose “Static IP Address” from the drop list
- WAN IP address / Subnet Mask / Gateway:** Enter the IP address, subnet mask, and gateway address, provided to you by your ISP.
- Primary DNS / Secondary DNS:** Input the Primary/Secondary DNS if necessary.
- MTU:** Most ISP offers MTU value to users. The default value is 0 (auto)
- NAT:** If you disable this option, it will act with a non-NAT function.
- Network Monitoring:** It is a checking mechanism designed to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checks, the timeout of one check, response latency threshold, fail times threshold, touched target 1 and touched target 2.
- IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.
- 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.

## ■ 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"/>

- 1. WAN Type:** Choose “PPP Over Ethernet” from the drop list
- 2. IPv6 Dual Stack:** You can enable this option if your ISP provides not only one IPv4 but also one IPv6 address. Please be noted, the setting is for WAN-1 only.
- 3. 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.
- 4. 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.
- 5. Connection Control:** Select your connection control scheme from the drop down list: “Auto-reconnect (Always on)”, “Dial-on-demand”, or “Manually”. If you select “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 you

choose “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 you choose “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. Please be noted, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will disappear since it is “Auto-reconnect (Always on)”.

6. **Maximum Idle Time:** The default value is 600 seconds, you can change if required. The setting is required when the Connection Control is not “Auto-reconnect (Always on)”.
7. **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.
8. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
9. **NAT:** If you disable this option, it will act with a non-NAT function.
10. **Network Monitoring:** It is a checking mechanism design to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checks, the timeout of one check, response latency threshold, fail times threshold, touched target 1 and touched target 2.
11. **IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.
12. **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 used 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 <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"/>

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

PPTP WAN Type Configuration	
Item	Setting
IP Mode	Static IP Address
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	

- Server IP Address / Name:** The IP address of the PPTP server and designated Gateway provided by your ISP.
- 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 down list: "Auto-reconnect (Always on)", "Dial-on-demand", or "Manually". If you select "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 you choose "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. Please be noted, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will disappear since it is "Auto-reconnect (Always on)".
7. **Maximum Idle Time:** The default value is 600 seconds, you can change if required. The setting is required when the Connection Control is not "Auto-reconnect (Always on)".
8. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
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. **NAT:** If you disable this option, it will act with a non-NAT function.
11. **Network Monitoring:** It is a checking mechanism designed to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checking, the timeout of one checking, response latency threshold, fail times threshold, touched target 1 and touched target 2.
12. **IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.
13. **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 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
ICMP	Disable
WAN IP Alias	<input type="checkbox"/> Enable 10.0.0.1

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

L2TP WAN Type Configuration	
Item	Setting
IP Mode	Static IP Address
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	

- Server IP Address / Name:** The IP address of the PPTP server and designated Gateway provided by your ISP.
- L2TP Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security reasons, the password you input won't be displayed on web UI.
- Connection Control:** Select your connection control scheme from the drop down list: “Auto-reconnect (Always on)”, “Dial-on-demand”, or “Manually”. If you select



“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 you choose “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 you choose “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. Please note that, if the WAN interface serves as the primary one for another WAN interface in Failover role, the Connection Control parameter will disappear since it is “Auto-reconnect (Always on)”.

6. **Maximum Idle Time:** The default value is 600 seconds, you can change it if required. The setting is required when the Connection Control is not “Auto-reconnect (Always on)”.
7. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto)
8. **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.
9. **NAT:** If you disable this option, it will act with a non-NAT function.
10. **Network Monitoring:** It is a checking mechanism designed to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checking, the timeout of one checking, response latency threshold, fail times threshold, touched target 1 and touched target 2.
11. **IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.
12. **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 user to manage this device.

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

### 3.1.1.2.2 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 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	Albania
▶ Service Provider	Vodafone
▶ APN	(Optional)
▶ PIN Code	(Optional)
▶ Dial Number	
▶ 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

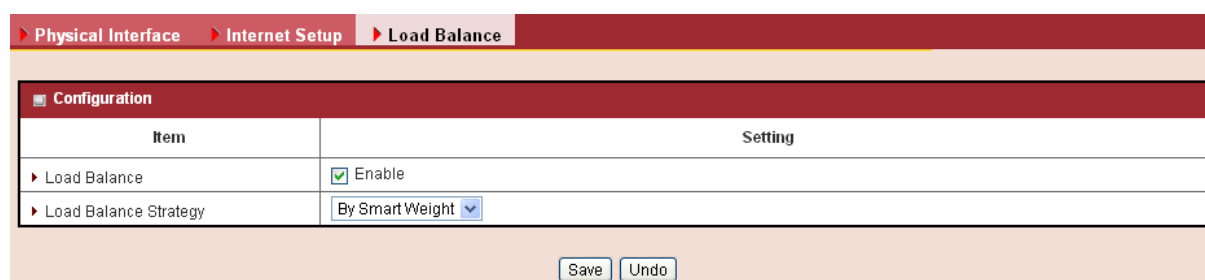
- 1. WAN Type:** Choose “3G” from the drop list.
- 2. Dial-up Profile:** After you subscribe 3G/4G data service, your operator will provide some information for you to setup connection, such as APN, dialed number, account, or password. If you know this information exactly, you can choose “Manual-configuration” 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-configuration” setting, this gateway will show responding information for your reference after you select country and service provider.
- 3. APN / PIN Code:** Enter the PIN Code for your SIM card (Optional).

4. **Dialed Number:** Enter the dialed number that is provided by your ISP.
5. **Account, Password:** Enter the account / Password that is provided by your ISP (Optional).
6. **Authentication:** Choose “Auto”, “PAP”, or “CHAP” according to your ISP’s authentication approach.
7. **Primary / Secondary DNS:** Enter IP address of Domain Name Server (Optional). You can keep them in blank, because most ISP will assign them automatically.
8. **Maximum Idle Time:** The default value is 600 seconds, you can change if required. The setting is required when the Connection Control is not “**Auto-reconnect (Always on)**”.
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:** If you disable this option, it will act with a non-NAT function.
12. **Network Monitoring:** It is a checking mechanism design to check if the WAN connection is alive or not. Configurable parameters include Enable/Disable, alive-connection checking approach, Loading Checking, the interval between two checking, the timeout of one checking, response latency threshold, fail times threshold, touched target 1 and touched target 2.
13. **IGMP:** Enable or disable multicast traffics from the internet. You may enable as auto mode or select by Auto, IGMP v1, IGMP v2, IGMP v3.

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

### 3.1.1.3 Load Balance

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

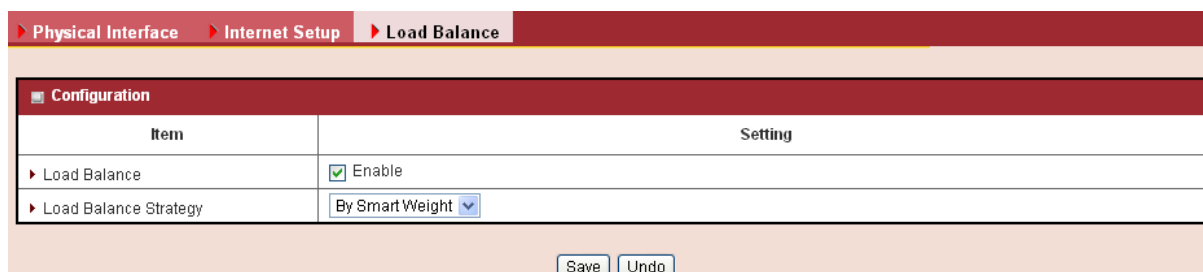


Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By SmartWeight

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 strategy: “**By Smart Weight**”, “**By Priority**” and “**By User Policy**”.

### **By Smart Weight:**

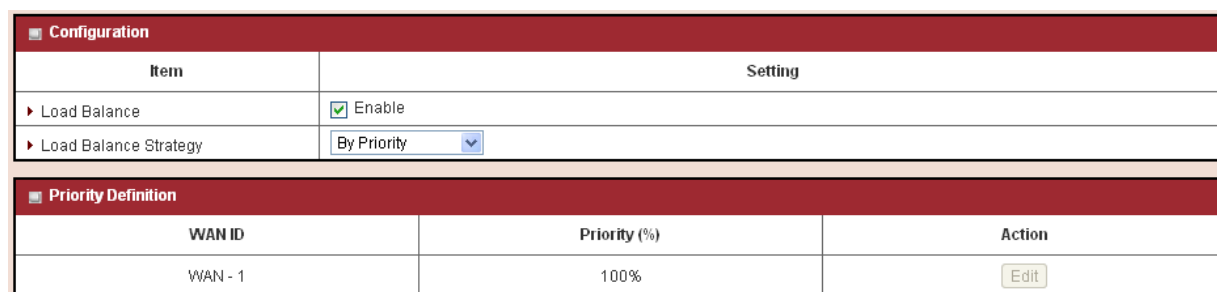


The screenshot shows the 'Load Balance' configuration page. The 'Configuration' section has two rows: 'Load Balance' with a checked 'Enable' checkbox, and 'Load Balance Strategy' with a dropdown menu set to 'By Smart Weight'. At the bottom, there are 'Save' and 'Undo' buttons.

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

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:**



The screenshot shows the 'Load Balance' configuration page with 'By Priority' selected in the 'Load Balance Strategy' dropdown. Below the configuration table is a 'Priority Definition' table.

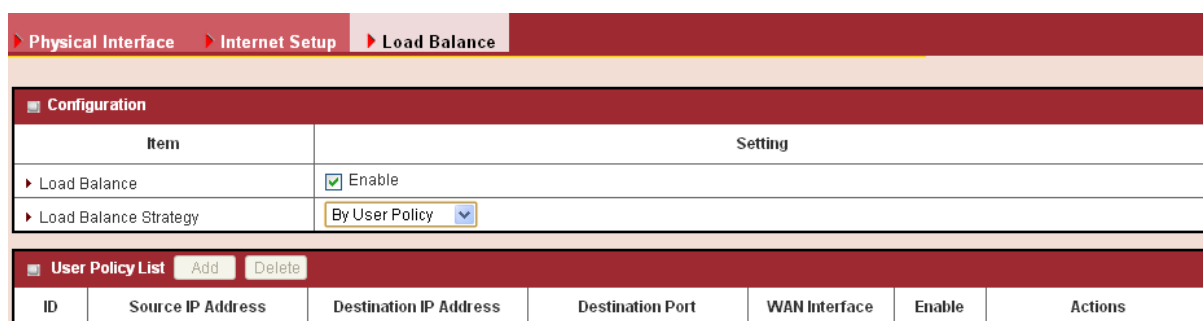
Item	Setting
Load Balance	<input checked="" type="checkbox"/> Enable
Load Balance Strategy	By Priority

WAN ID	Priority (%)	Action
WAN - 1	100%	<a href="#">Edit</a>

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 traffics for each WAN to access the internet.

### **By User Policy:**



The screenshot shows the 'Load Balance' configuration page with 'By User Policy' selected in the 'Load Balance Strategy' dropdown. Below the configuration table is a 'User Policy List' table.

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

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

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.

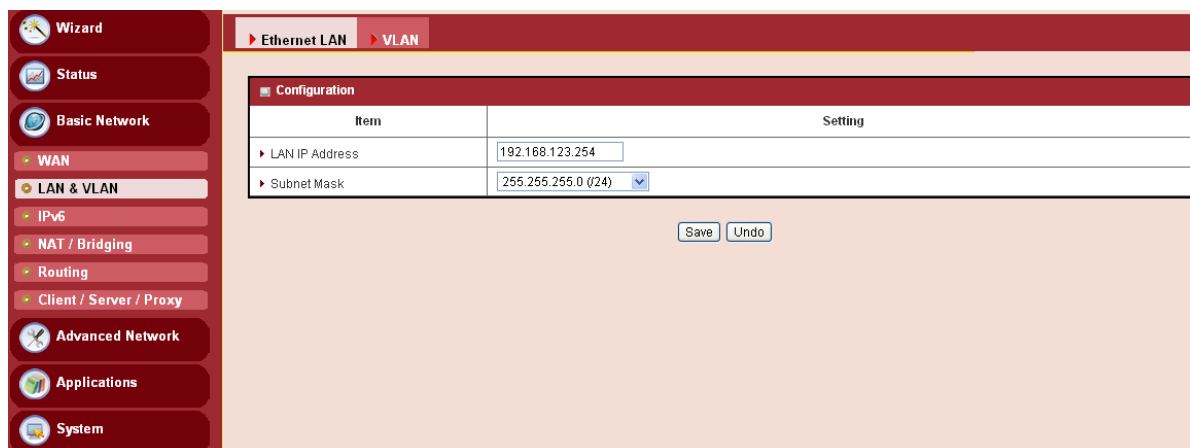
You can manage the outbound traffics flow and the force specific traffics to access Internet through designated WAN interface. For those traffics not covered in the user policy rules, the device will allocate the WAN interface by applying “Smart Weight” mechanism simultaneously.

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

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, Destination Port:** 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

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

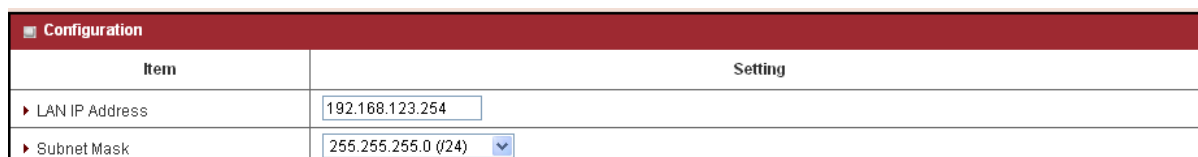


Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

Save Undo

### 3.1.2.1 Ethernet LAN

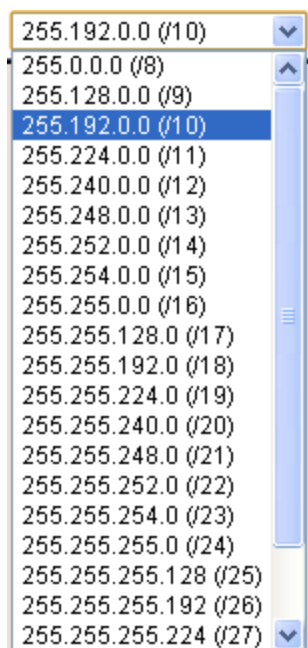
Please follow the below mentioned instructions for an IPv4 Network Setup.



Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

Save Undo

- 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.
- Subnet Mask:** Select 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.



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 logical network under a certain switch or router device to group lots of client hosts with a specific VLAN ID. This device supports both Port-based VLAN and Tag-based VLAN. In Port-based VLAN, all client hosts belong to the same group by transferring data via some physical ports that are tagged with same VLAN ID in the device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remain within the VLAN. However, in Tag-based VLAN, all packets with the same VLAN ID will be treated as the same group of and own same access property and QoS property. It is especially useful when individuals of a VLAN group are present at different locations.

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. In some cases, SMB departments are separated and located at any floor of building. All client hosts in same department should own common access property and QoS property. You can select either one operation mode, port-based VLAN or tag-based VLAN, and then configure according to your network configuration.

Configuration							
Item				Setting			
VLAN Types				Port-based			
DMZ Port-based VLAN Definition							
DMZ Port		DHCP Server			Action		
PORT6		DHCP 1/Enable 192.168.123.0/24			<a href="#">Edit</a>		
Port-based VLAN List <span style="float: right;">[ Help ]</span>							
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	0	<a href="#">Edit</a>
Port2	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port3	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port4	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port5	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port-based VLAN Summary							
VLAN IDs	Members		NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag	
1	Port1, Port2, Port3, Port4, Port5		NAT	DHCP 1	X	No	
<a href="#">Save</a> <a href="#">VLAN Routing Group</a>							

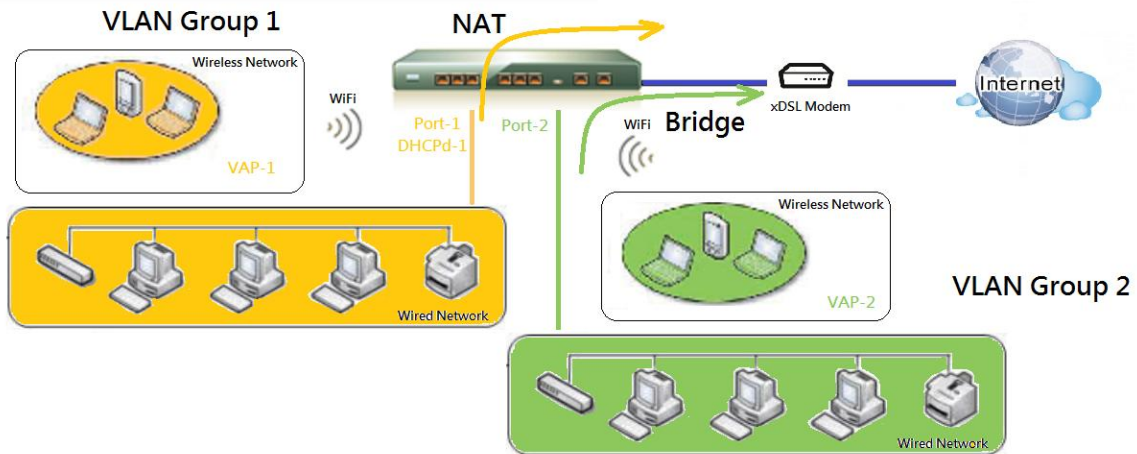
### 3.1.2.2.1 VLAN Scenarios

There are some common VLAN scenarios as follows:

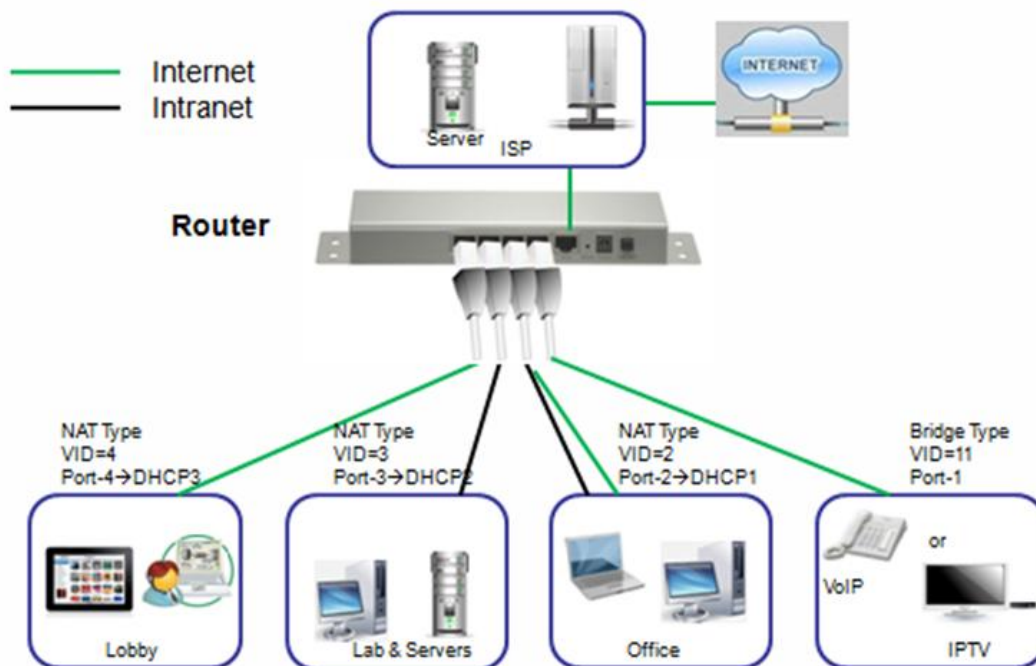
- **Port-Based VLAN Tagging for Differentiated Services**

Port-based VLAN function can group Ethernet ports, Port-1 ~ Port-5, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server is allocated for a NAT VLAN group to let group host member get its IP address. Thus, such a host can surf Internet via the NAT mechanism of business access gateway. But at bridge mode, Intranet packet flow was delivered out WAN trunk port with VLAN tag to upper link for different services.



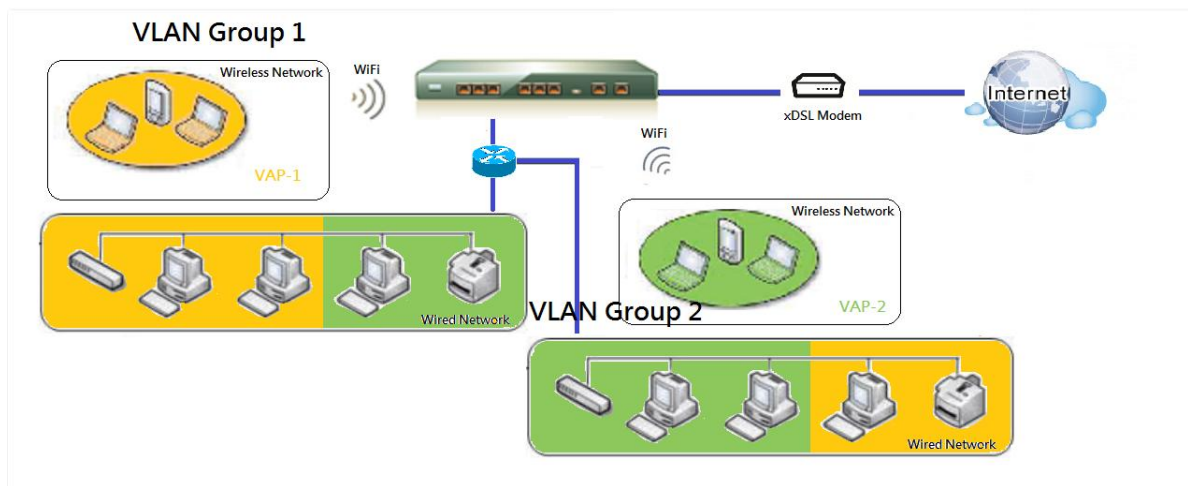


A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical group segment. Following is a descriptive example, and there is difference at interfaces for different models. In SMB or a company, administrator schemes out 4 segments, Lobby, Lab & Servers, Office and VoIP & IPTV. In a Wireless Gateway (there is no Wi-Fi interface for some models), administrator can configure Lobby segment with VLAN ID 4. The VLAN group includes Port-4 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. He also configures Lab & Servers segment with VLAN ID 3. The VLAN group includes Port-3 with NAT mode and DHCP-2 server equipped. However, he configures Office segment with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode and DHCP-1 server equipped. At last, administrator also configures VoIP & IPTV segment with VLAN ID 11. The VLAN group includes Port-1 with bridge mode to WAN interface as shown at following diagram.

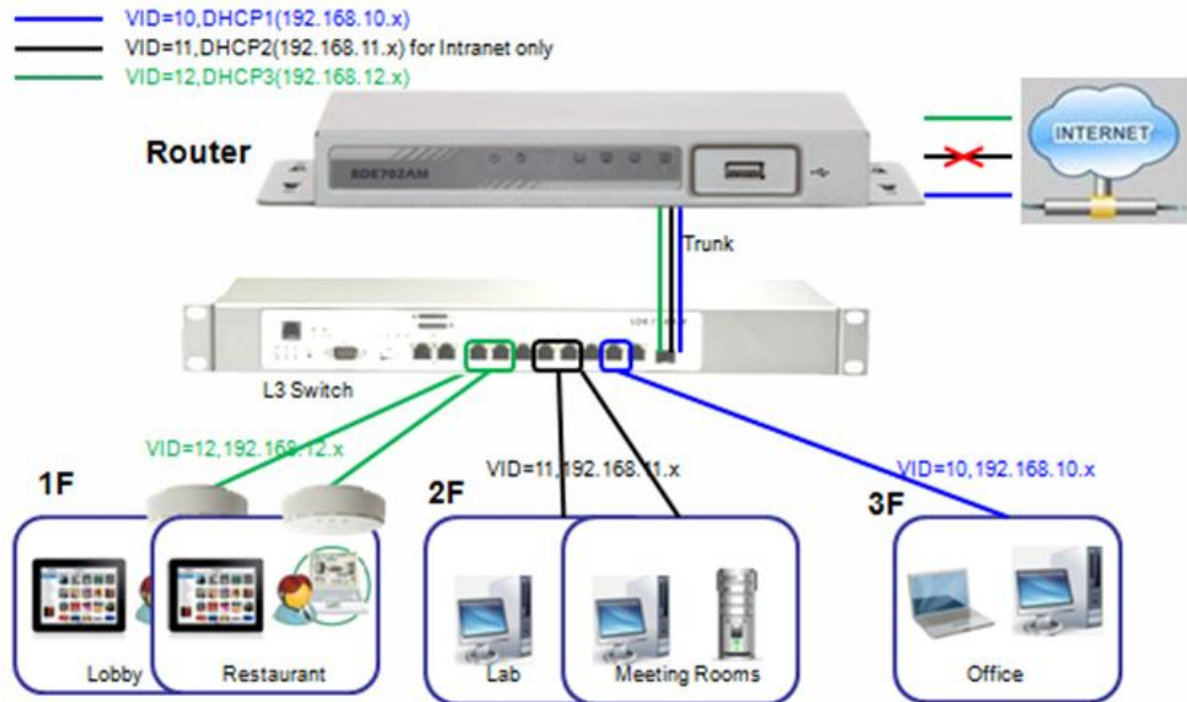


- Tag-based VLAN Tagging for Location-free Departments

Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-5 , together with different VLAN tags for deploying department subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical port for Intranet. These flows can be directed to different destination because they have differentiated tags. The approach is very useful to group some hosts in different geographic location to be the same department.



Tag-based VLAN is also called a VLAN Trunk. The VLAN Trunk collects all packet flows with different VLAN IDs from Router device and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. Administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. Following is an example. In SMB or a company, administrator schemes out 3 segments, Lobby & Restaurant, Lab & Meeting Rooms and Office. In a Security VPN Gateway, administrator can configure Lobby & Restaurant segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configures Lab & Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. However, he configures Office segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet. In this example, VLAN 10 and 12 groups can access the Internet as shown in the following diagram.

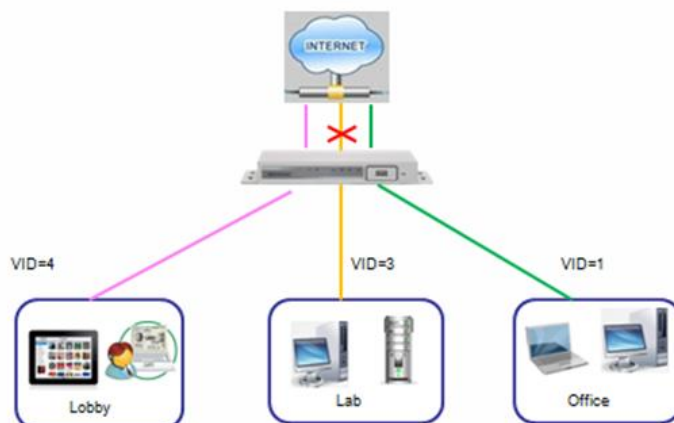


### ● VLAN Group Access Control

Administrator can specify the Internet access right for all VLAN groups. He also can configure which VLAN groups can communicate with each other.

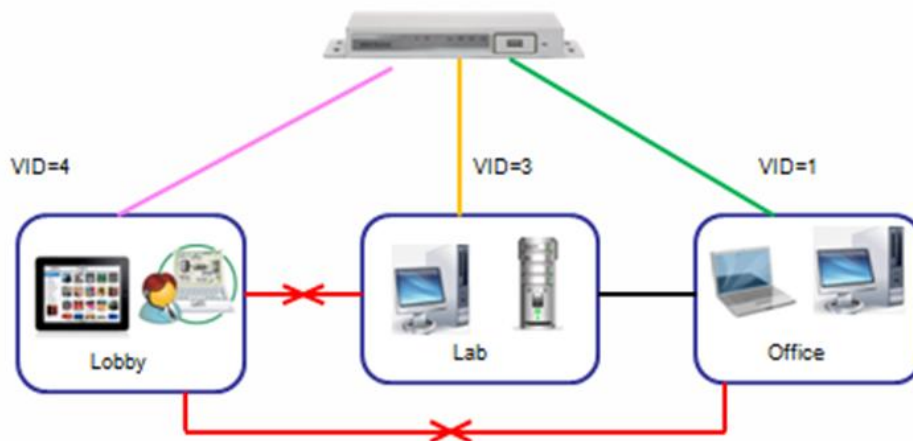
### VLAN Group Internet Access

Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 1 and 4 can access Internet but the one with VID is 3 can't. That is, visitors in Lobby and staff in office can access Internet. But ones in Lab can't because of security issue. Servers in Lab serve only for trusted staffs or are accessed in secure tunnels.



### **Inter VLAN Group Routing**

In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair has not the transitive property. That is, A can communicate with B, and B can communicate with C, that does not mean A can communicate with C. An example is shown in the following diagram. VLAN groups of VID is 1 and 3 can access each other but the ones between VID 3 and VID 4 and between VID 1 and VID 4 cannot.



### 3.1.2.2.2 Port-Based VLAN

A port-based VLAN is a group of ports on an Ethernet switch or router that forms a logical group segment. There are five LAN ports in this device, so you can have various VLAN configurations to organize the available LAN ports if required.

Configuration							
Item				Setting			
VLAN Types				Port-based			

DMZ Port-based VLAN Definition		
DMZ Port	DHCP Server	Action
PORT6	DHCP 1/Enable 192.168.123.0/24	<a href="#">Edit</a>

Port-based VLAN List								[ Help ]
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	0	<a href="#">Edit</a>	
Port2	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>	
Port3	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>	
Port4	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>	
Port5	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>	

Port-based VLAN Summary					
VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag
1	Port1, Port2, Port3, Port4, Port5	NAT	DHCP 1	X	No

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

At first, you must select the “**Port-based**” for your VLAN configuration type if you want to. Based on your selection of VLAN Type, you can do corresponding configuration.

Configuration	
Item	Setting
VLAN Types	Port-based

Besides, the device provides a DMZ port for various servers deployment in the Intranet. For its VLAN configuration, you must specify which DHCP server needs to be used for the DMZ port by clicking on the “**Edit**” button. Please be noted that the virtual server, virtual computer and DMZ host configuration in **Basic Network >> NAT/Bridging** needs to be same subnet with the specific DHCP server for DMZ Port.

Port-based VLAN List								[ Help ]
Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action	
Port1	NAT	1	X	DHCP 1	X	0	<a href="#">Edit</a>	

Now, you can setup the VLAN configuration for all Ethernet LAN ports in the device. By default, all the 5 LAN ports belong to one VLAN. This VLAN is a NAT type network, and the IP address of all local devices is allocated by DHCP-1 server. If you want to divide them

into different VLANs, click on the “**Edit**” button related to each port.

Port-based VLAN List							[ Help ]
Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
Port1	NAT	1	X	DHCP 1	X	0	<a href="#">Edit</a>
Port2	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port3	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port4	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>
Port5	NAT	1	X	DHCP 1/Enable 192.168.123.0/24	X	0	<a href="#">Edit</a>

Port-based VLAN Summary					
VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag
1	Port1, Port2, Port3, Port4, Port5	NAT	DHCP 1	X	No

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

- NAT/Bridge:** Select “**NAT**” or “**Bridge**” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
- VLAN ID:** Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN group. When NAT/Bridge is “**Bridge**” and the “**Tx Tag**” is checked, the VLAN ID will be equal to the WAN ID and will carry that VID into the VLAN group of subnet.
- Tx TAG:** If NAT/Bridge is “**Bridge**”, the specific Ethernet LAN port will bridge to some WAN interface and carry the VLAN ID into the VLAN group of subnet by checking the Tx TAG box.
- DHCP Server:** Specify a DHCP server for configuring VLAN. This device provides up to 6 DHCP servers to serve the DHCP requests from different VLANs and DMZ port. You must define the DHCP Server objects beforehand in **Basic Network >> Client&Server&Proxy** to assign one DHCP Server object to one VLAN group that is NAT type.
- Available WAN:** If “**NAT/Bridge**” is “**Bridge**”, you must specify which WAN interface will be the target interface to bridge from the Ethernet LAN port.
- 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.



## 7. VLAN Routing Group:

Summary			
LAN VALN Settings			
Ethernet	NAT/Bridge	VLAN ID	Tx TAG
Port1	NAT	1	<input type="checkbox"/>
Port2	NAT	1	<input type="checkbox"/>
Port3	NAT	1	<input type="checkbox"/>
Port4	NAT	1	<input type="checkbox"/>
Port5	NAT	1	<input type="checkbox"/>

VLAN Group Internet Access Definition		
VLAN IDs	Members	Internet Access(WAN)
1	PORT1, PORT2, PORT3, PORT4, PORT5	Allow <a href="#">Edit</a>

Inter VLAN Group Routing		
VLAN IDs	Members	Action
		<a href="#">Edit</a>
		<a href="#">Edit</a>
		<a href="#">Edit</a>
		<a href="#">Edit</a>

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

Above configuration example supports 3 access policies. The first one is Internet Access Policy that includes Port-1, Port-2 and Port-3. All client hosts via these ports can access the Internet. The second policy is Intranet access Policy that includes only Port-4. All client hosts via the port can't access the Internet. But the Ethernet client hosts of VLAN 1 and 3 groups can communicate with each other. The last one policy is the Bridge to WAN Policy that includes only Port-5.

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

### 3.1.2.2.3 Tag-Based VLAN

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

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

Configuration [ Help ]			
Item	Setting		
VLAN Type	Tag-based		

DMZ Port Tag-based VLAN Definition			
VLAN ID	DMZ Port	DHCP Server	Action
11	PORT6	DHCP 1	<a href="#">Edit</a>
<a href="#">Save</a>			

Tag-based VLAN List <a href="#">Add</a> <a href="#">Delete</a>				
VLAN ID	Internet	Port	DHCP Server	Actions
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5	DHCP 1	<a href="#">Edit</a>

Tag-based VLAN Summary	
Port	VLAN IDs
Port1	1
Port2	1
Port3	1
Port4	1
Port5	1

Besides DMZ Port, all the LAN ports belong to one VLAN group, and this VLAN ID is forced to “1”. It is a special tag based VLAN for devices to operate, there is no tag required for this default VLAN ID.

If you want to configure your own tag-based VLANs, select “**Tag-based**” for VLAN Type first.

Configuration [ Help ]	
Item	Setting
VLAN Type	Tag-based

Besides, the device provides a DMZ port for various servers deployment in the Intranet. For its VLAN configuration, you must specify which DHCP server to be used for the DMZ port by clicking on the “**Edit**” button. You also can define the VLAN ID there. Please be noted that the virtual server, virtual computer and DMZ host configuration in **Basic Network >> NAT/Bridging** need to be same subnet with the specific DHCP server for DMZ Port.

DMZ Port Tag-based VLAN Definition			
VLAN ID	DMZ Port	DHCP Server	Action
11	PORT6	DHCP 1	<a href="#">Edit</a>
<a href="#">Save</a>			

Now, you can setup the VLAN configuration for some different VLAN groups that you need. From the Tag-based VLAN List, you can add one new VLAN group by clicking on the



“**Add**” command button. But also you can modify some existing VLAN groups by clicking corresponding “**Edit**” command buttons at the end of each VLAN group in the Tag-based VLAN List. Besides, unnecessary VLAN groups can be removed by checking the “**Select**” box for those groups and then clicking on the “**Delete**” command button at the Tag-based VLAN List caption

Tag-based VLAN List				
VLAN ID	Internet	Port	DHCP Server	Actions
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5	DHCP 1	<input type="button" value="Edit"/>

Tag-based VLAN Summary	
Port	VLAN IDs
Port1	1
Port2	1
Port3	1
Port4	1
Port5	1

- VLAN ID:** Specify a VLAN tag for this VLAN group. The packets with the same VID are in the same VLAN group.
- 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 to the destination belonging to this configured VLAN group.
- Port 1 ~ Port 5:** Specifies whether it belongs to the VLAN group or not. You just have to select the check box of the selected ports.
- DHCP Server1~6 and “---”:** Specify a DHCP server for configuring the VLAN. This device provides up to 6 DHCP servers to serve the DHCP requests from different VLANs. If you choose “---”, it means Gateway will not make any response for those DHCP requests with that VLAN ID.

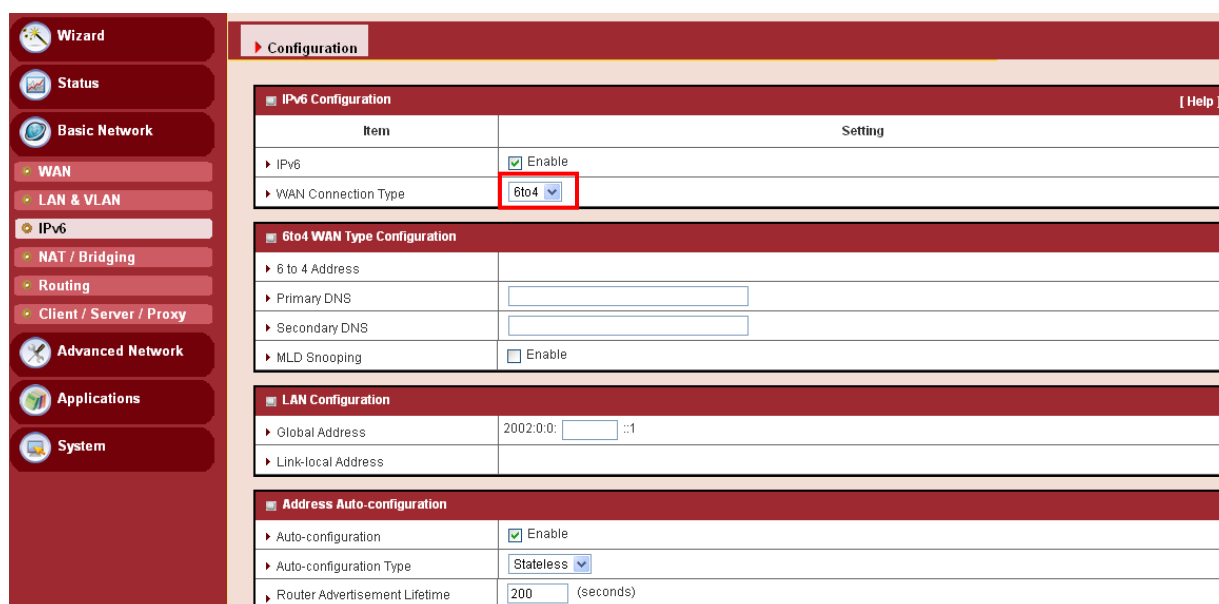
Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

### 3.1.3 IPv6 Setup

The growth of the Internet has created a need for more addresses than those that 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 (IPv6 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 6 to 4



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

6to4 WAN Type Configuration	
6 to 4 Address	
Primary DNS	
Secondary DNS	
MLD Snooping	<input type="checkbox"/> Enable

LAN Configuration	
Global Address	2002::1
Link-local Address	

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

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

#### **6 to 4 WAN IPv6 address settings:**

- 6 to 4 Settings:** You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
- DNS:** Please enter the IPv6 address Primary DNS address and secondary DNS address.
- MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This

list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

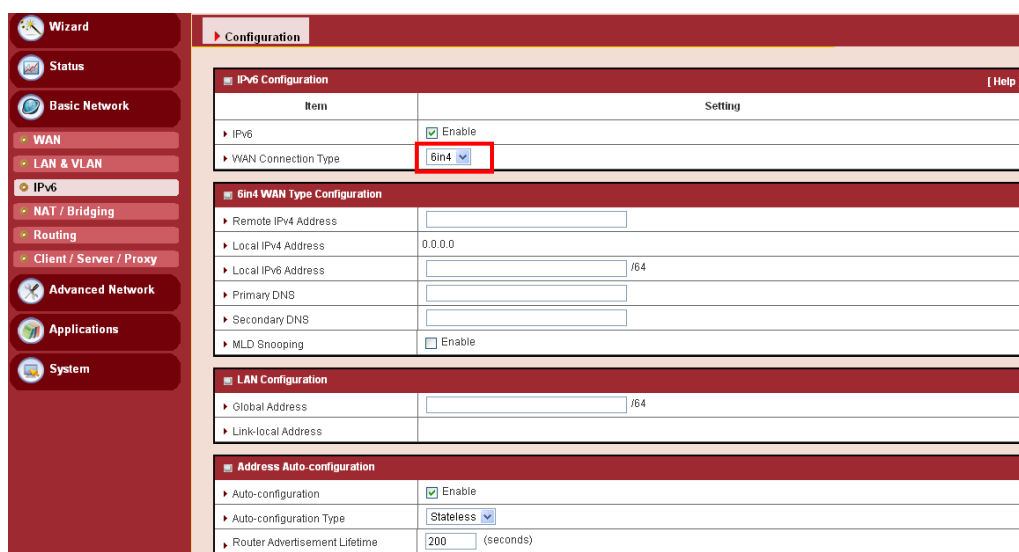
### LAN Configuration:

4. **Global Address:** Please enter global Address.
5. **LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

### Address auto configuration settings:

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

### 3.1.3.2 6 in 4



The screenshot shows the 'Configuration' tab in the DIGISOL web interface. The left sidebar contains navigation options: Wizard, Status, Basic Network, WAN, LAN & VLAN, IPv6, NAT / Bridging, Routing, Client / Server / Proxy, Advanced Network, Applications, and System. The main content area is titled 'IPv6 Configuration' and includes a 'Help' link. It contains several sections:

- IPv6 Configuration:** A table with two rows: 'IPv6' (checked 'Enable') and 'WAN Connection Type' (set to '6in4').
- 6in4 WAN Type Configuration:** Fields for 'Remote IPv4 Address', 'Local IPv4 Address' (0.0.0.0), 'Local IPv6 Address' (with a '/64' suffix), 'Primary DNS', 'Secondary DNS', and 'MLD Snooping' (checked 'Enable').
- LAN Configuration:** Fields for 'Global Address' (with a '/64' suffix) and 'Link-local Address'.
- Address Auto-configuration:** Fields for 'Auto-configuration' (checked 'Enable'), 'Auto-configuration Type' (set to 'Stateless'), and 'Router Advertisement Lifetime' (200 seconds).

---

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

### **6 in 4 WAN IPv6 address settings:**

1. **Remote / Local IPv4 and IPv6 Address:** You may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **DNS:** Please enter IPv6 address Primary DNS address and secondary DNS address.
3. **MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

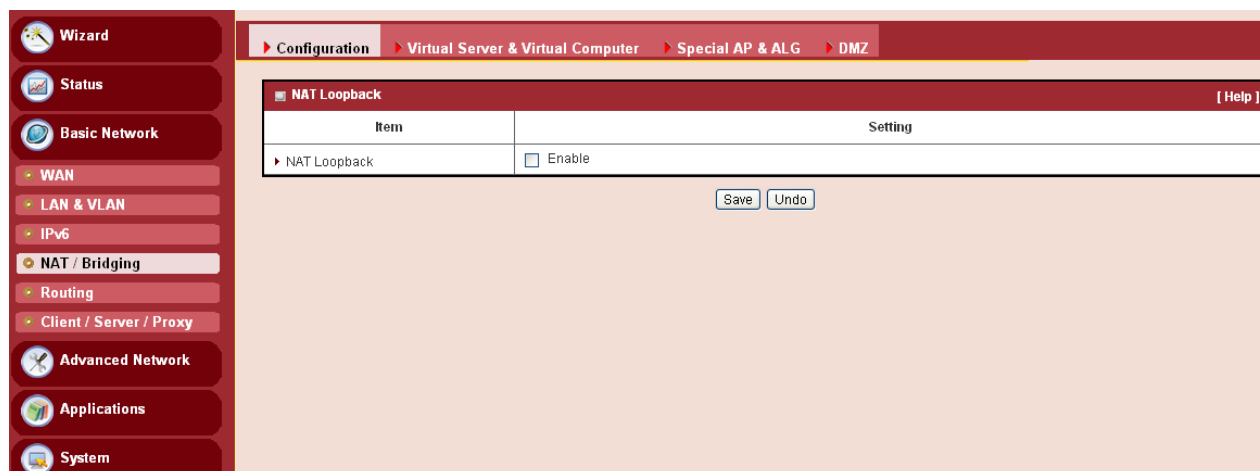
### **LAN Configuration:**

4. **Global Address:** Please enter global Address.
5. **LAN IPv6 address settings:** Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

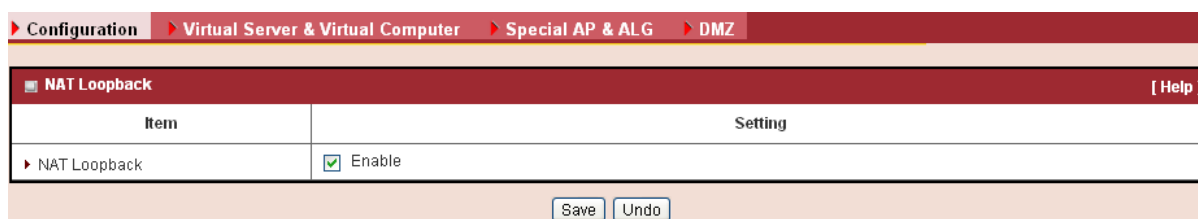
### **Address auto configuration settings:**

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

## 3.1.4 NAT / Bridging



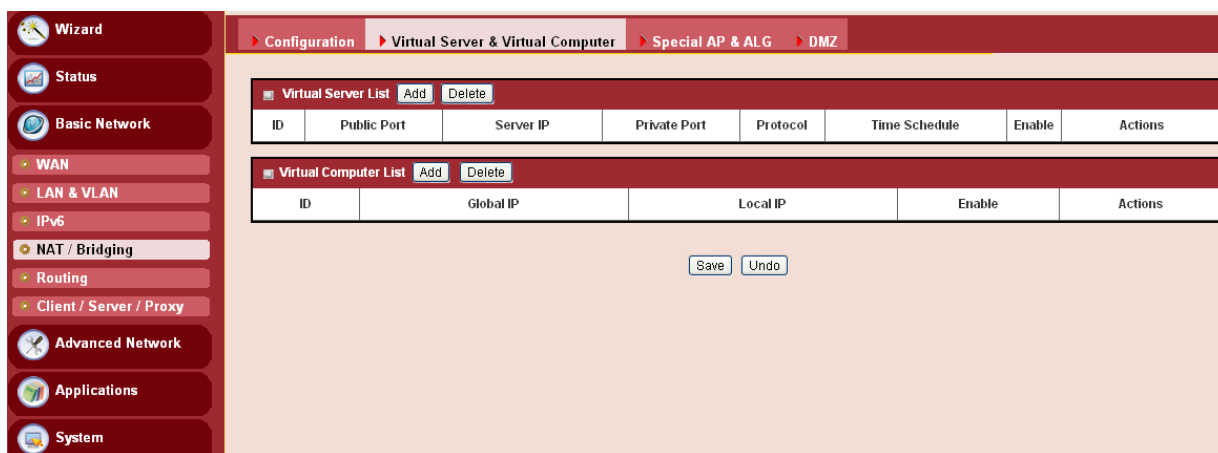
### 3.1.4.1 Configuration



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 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 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.

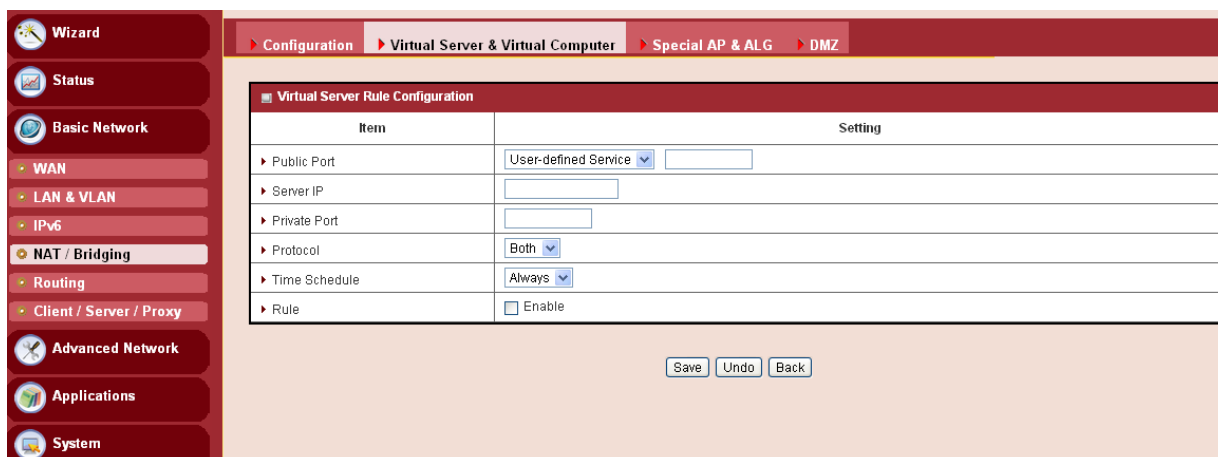
## 3.1.4.2 Virtual Server & Virtual Computer

### 3.1.4.2.1 Virtual Server



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

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



For example, if you have an **FTP server (Service port 21) at 10.0.75.1**, a **Web server1 (Service port 80) at 10.0.75.2**, a **Web server2 (Service Port 8080 and Private port 80) at 10.0.75.3**, and a **VPN server at 10.0.75.6**, then you need to specify the following virtual server mapping table

Service Port	Private Port	Server IP	Enable
21		10.0.75.1	V
80		10.0.75.2	V
8080	80	10.0.75.3	V
1723		10.0.75.6	V

### 3.1.4.2.2 Virtual Computer

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

Virtual Server List
Add
Delete

ID	Public Port	Server IP	Private Port	Protocol	Time Schedule	Enable	Actions
----	-------------	-----------	--------------	----------	---------------	--------	---------

Virtual Computer List
Add
Delete

ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

Virtual Computer Rule Configuration
[ Help ]

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

Save

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

### 3.1.4.3 Special AP & ALG

#### 3.1.4.3.1 ALG

Application-level gateway allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "**control/data**" protocols such as SIP, RTSP, file transfer in IM applications, etc.

Configuration
Virtual Server & Virtual Computer
Special AP & ALG
DMZ

Configuration

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

Special AP List
Add
Delete

ID	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions
----	--------------	----------------	---------------	--------	---------

Save
Undo

## 1. SIP ALG: Support some SIP ALG, like STUN.

### 3.1.4.3.2 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.

Special AP List		Add	Delete												
ID	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions										
<div>Special AP Rule Configuration [ Help ]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Trigger Port</td> <td>Port : <input type="text"/> Popular Applications : -- select one --</td> </tr> <tr> <td>▶ Incoming Ports</td> <td><input type="text"/></td> </tr> <tr> <td>▶ Time Schedule</td> <td>(0) Always</td> </tr> <tr> <td>▶ Rule</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <div>Save</div>						Item	Setting	▶ Trigger Port	Port : <input type="text"/> Popular Applications : -- select one --	▶ Incoming Ports	<input type="text"/>	▶ Time Schedule	(0) Always	▶ Rule	<input type="checkbox"/>
Item	Setting														
▶ Trigger Port	Port : <input type="text"/> Popular Applications : -- select one --														
▶ Incoming Ports	<input type="text"/>														
▶ Time Schedule	(0) Always														
▶ Rule	<input type="checkbox"/>														

- 1. Trigger Port:** The outbound port number issued by the application. There are some popular applications to be selected for the trigger port.
- 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 on according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.
- 4. Rule:** Check the box to enable the Special AP feature.

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

### 3.1.4.4 DMZ

Configuration		Virtual Server & Virtual Computer	Special AP & ALG	DMZ						
<div>Configuration [ Help ]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ DMZ</td> <td>IP Address of DMZ Host: <input type="text"/> <input type="checkbox"/> Enable</td> </tr> <tr> <td>▶ Relay</td> <td>DHCP Relay: <input type="text"/> <input type="checkbox"/> Enable</td> </tr> </tbody> </table> <div>Save Undo</div>					Item	Setting	▶ DMZ	IP Address of DMZ Host: <input type="text"/> <input type="checkbox"/> Enable	▶ Relay	DHCP Relay: <input type="text"/> <input type="checkbox"/> Enable
Item	Setting									
▶ DMZ	IP Address of DMZ Host: <input type="text"/> <input type="checkbox"/> Enable									
▶ Relay	DHCP Relay: <input type="text"/> <input type="checkbox"/> Enable									

DMZ (Demilitarized Zone) Host is a host that is exposed to the Internet cyberspace but still with the protection of firewall by gateway device. So, the function allows a computer to execute 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. Otherwise, if specific application is blocked by NAT

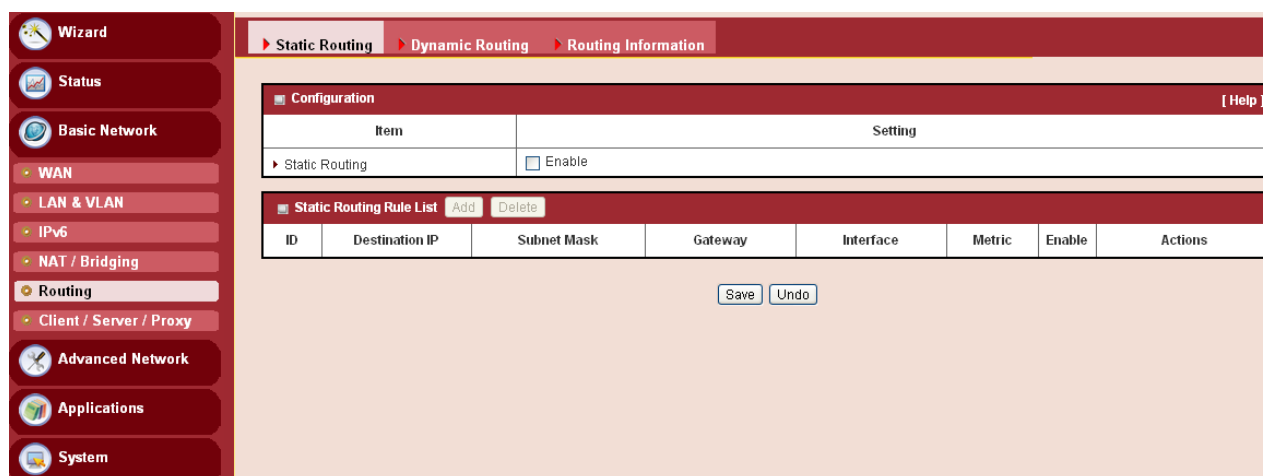


mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

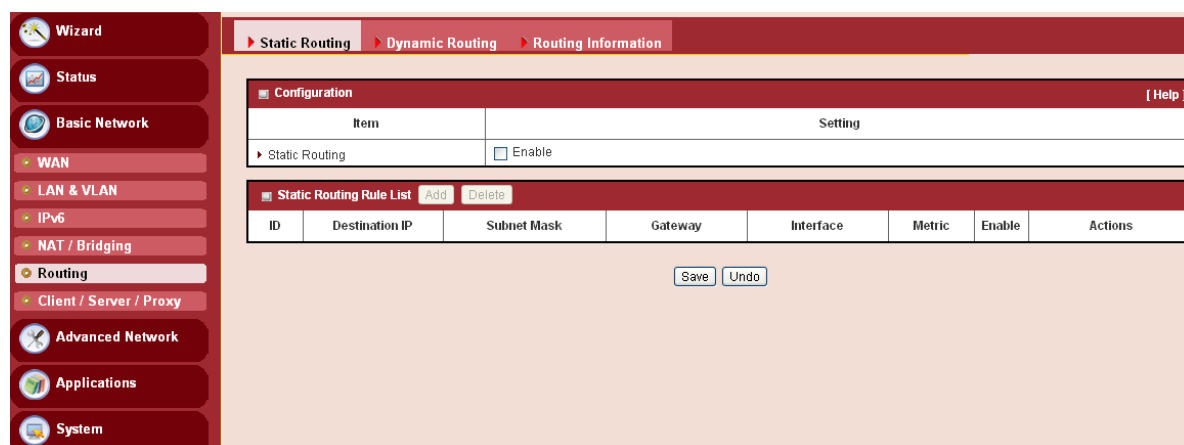
1. **IP Address of DMZ Host:** Enter IP Address of DMZ Host.
2. **DHCP Relay:** DHCP Relay Agent component relays DHCP messages between DHCP clients and DHCP servers on different IP networks. Because DHCP is a broadcast-based protocol, by default its packets do not pass through routers. If you need this feature in the environment, please enable it.

## 3.1.5 Routing

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



### 3.1.5.1 Static Routing



For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the destination IP address, Subnet Mask, Gateway, and Metric for each routing rule, and

then enable or disable the rule by checking or un-checking the Enable check box.

Please click Add or Edit button to configure a static routing rule:

▶ Static Routing
▶ Dynamic Routing
▶ Routing Information

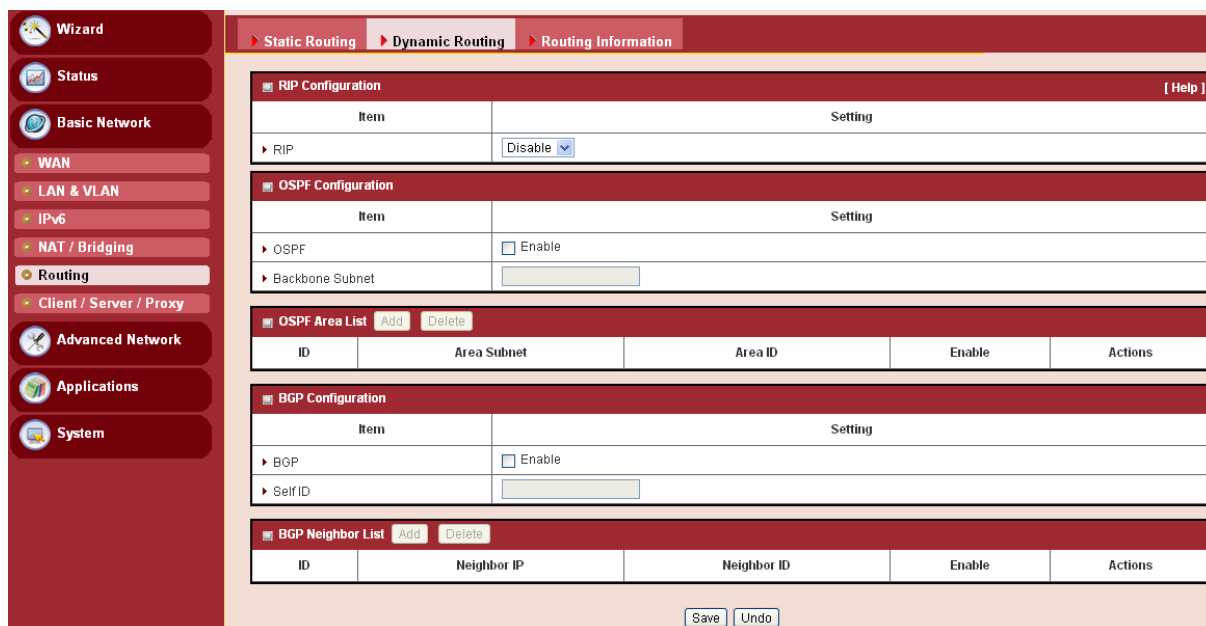
Static Routing Rule Configuration

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

- Destination IP:** Enter the subnet network of routed destination.
- Subnet Mask:** Input your subnet mask. Subnet mask defines the range of IP address in destination network.
- Gateway:** The IP address of gateway that you want to route for this destination subnet network. The assigned gateway is required to be in the same subnet of LAN side or WAN side.
- Metric:** The router uses the value to determine the best possible route. It will go in the direction of the gateway with the lowest metric.
- Rule:** Check the Enable box to enable this static routing rule.

### 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.



The screenshot displays the 'Dynamic Routing' configuration page. It includes a sidebar with navigation options like Wizard, Status, Basic Network, WAN, LAN & VLAN, IPv6, NAT / Bridging, Routing (selected), Client / Server / Proxy, Advanced Network, Applications, and System. The main content area has tabs for Static Routing, Dynamic Routing, and Routing Information. The 'Dynamic Routing' tab is active, showing configuration for RIP, OSPF, and BGP. The RIP Configuration section has a table with 'RIP' set to 'Disable'. The OSPF Configuration section has a table with 'OSPF' set to 'Enable' and a 'Backbone Subnet' field. The OSPF Area List section has a table with columns for ID, Area Subnet, Area ID, Enable, and Actions. The BGP Configuration section has a table with 'BGP' set to 'Enable' and a 'Self ID' field. The BGP Neighbor List section has a table with columns for ID, Neighbor IP, Neighbor ID, Enable, and Actions. At the bottom, there are 'Save' and 'Undo' buttons.

- 1. 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.
- 2. OSPF:** OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

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

OSPF Area List <span>Add</span> <span>Delete</span>				
ID	Area Subnet	Area ID	Enable	Actions

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

Save

You can enable the OSPF routing function by checking on the “**Enable**” box for the OSPF item and filling the “**Backbone Subnet**”. You can add up to 8 area subnets for the OSPF network and enable them individually by clicking on the “**Add**” command button. But also you can modify some existing OSPF areas by clicking corresponding “**Edit**” command buttons at the end of each OSPF area definition in the OSPF Area List. Besides, unnecessary OSPF areas can be removed by checking the “**Select**” box for those areas and then clicking on the “**Delete**” command button at the OSPF Area List caption. When you finish with the setting, click on “**Save**” to store your settings.

- 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 as 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 <span>Add</span> <span>Delete</span>				
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

Save

You can enable the BGP routing function by checking on the “**Enable**” box for the BGP item and filling the “**Self ID**”. You can add up to 8 BGP neighbors for the BGP network and enable them individually by clicking on the “**Add**” command button. But also you can modify some existing BGP neighbors by clicking corresponding “**Edit**” command buttons at the end of each BGP neighbor definition in the BGP Neighbor List. Besides, unnecessary BGP neighbors can be removed by checking the “**Select**” box for those neighbors and then clicking on the “**Delete**” command button at the BGP Neighbor List caption. When you finish the setting, click on “**Save**” to store your settings.

### 3.1.5.3 Routing Information

Static Routing

Dynamic Routing

Routing Information

Routing Table

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

Policy Routing Information

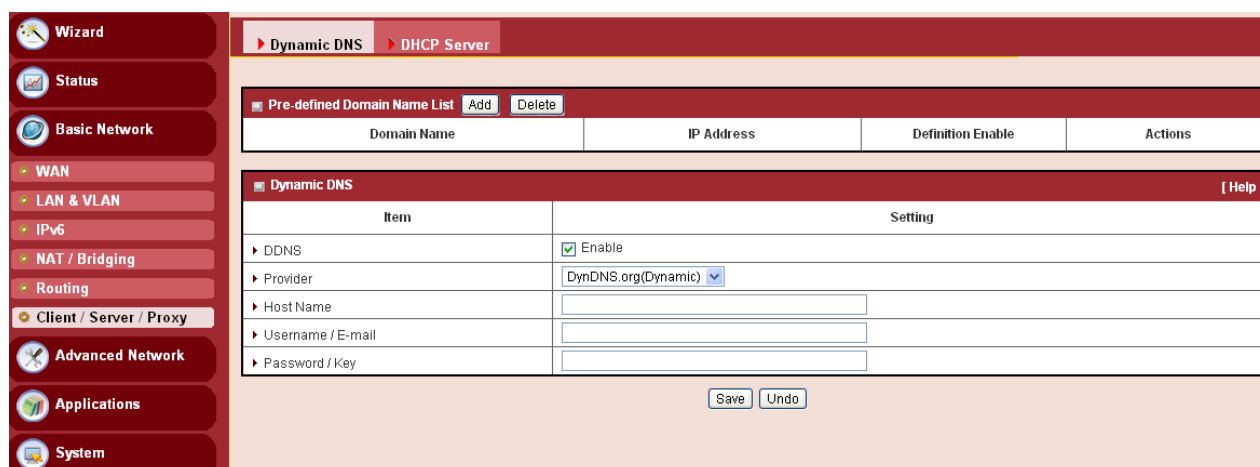
Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Refresh

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.

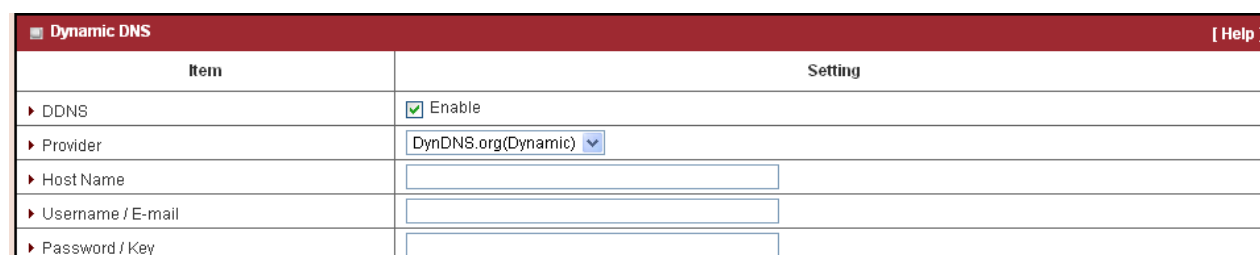
## 3.1.6 Client/Server/Proxy



### 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 domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider. This device supports most popular 3-party DDNS service provider, including TZO.com, No-IP.com, DynDNS.org (Dynamic), DynDNS.org (Custom), and DHS.org. Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in Provider field.



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

1. **DDNS:** Check the Enable box if you would like to activate this function.
2. **Provider:** The DDNS provider supports service for you to bind your IP (even private IP) with a certain Domain name. You could choose your favorite provider. There are following options:

DynDNS.org(Dynamic)   
 DynDNS.org(Dynamic)  
 DynDNS.org(Custom)  
 No-IP.com  
 TZO.com  
 dhs.org

3. **Host Name:** Register a domain name to the DDNS provider. The full domain name is concatenated with host name (you specify) and a suffix (DDNS provider specifies).
4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you registered.
5. **Password/Key:** Input password or key based on the DDNS provider you select.

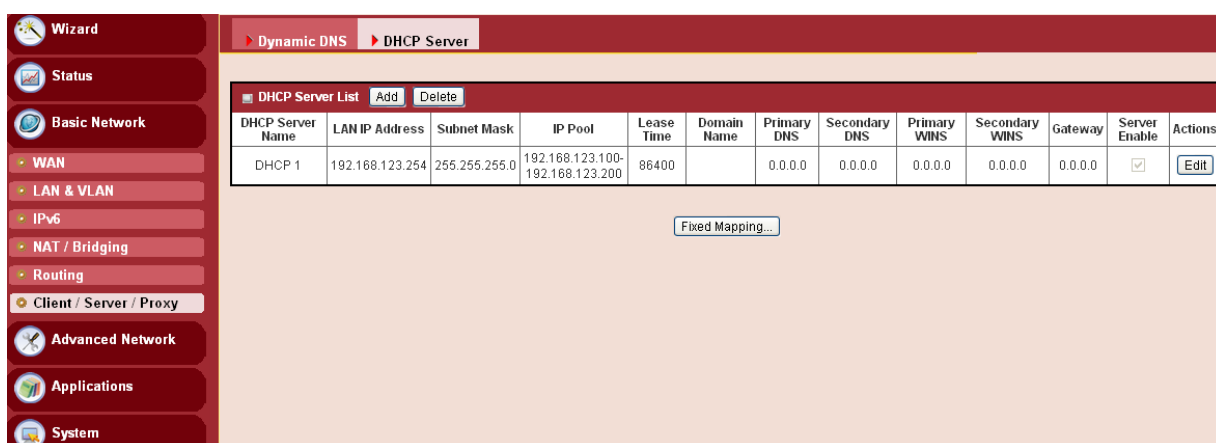
Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

### 3.1.6.2 DHCP Server

#### 3.1.6.2.1 DHCP Server List

The gateway supports up to 6 DHCP servers to serve the DHCP requests from different VLAN groups and DMZ port. And there is one default one whose LAN IP Address and Subnet Mask are the same ones of gateway LAN interface, and IP Pool ranges from .100 to .200 as shown at following DHCP Server List. You can add or edit one DHCP server configured by clicking on the “**Add**” button behind “**DHCP Server List**” or the “**Edit**” button at the end of DHCP server information.

There are two additional buttons that can be used to show the DHCP client list and the fixed mapping between MAC address and IP address of local client hosts as shown in the following diagram.



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"/>	<a href="#">Edit</a>

Fixed Mapping...

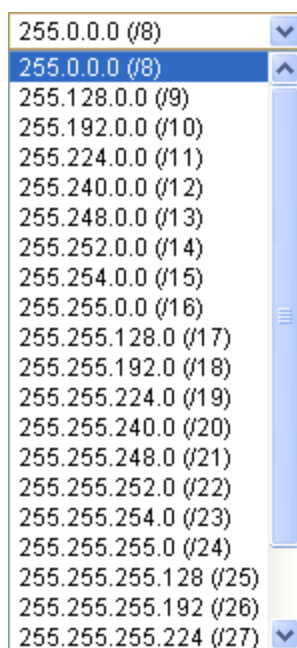
### 3.1.6.2.2 DHCP Server Configuration

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

- DHCP Server Name:** The server name of DHCP server. By default, they are “DHCP-1” ~ “DHCP-6”.
- LAN IP Address:** Specify the local IP address of the enabled DHCP Server. It's the LAN IP address of this gateway for DHCP-1 server. For other DHCP servers, their LAN IP addresses also have default values and can be modified by user.
- Subnet Mask:** Select the subnet mask for the specific DHCP-n server. Subnet Mask defines how many clients are allowed in one network or subnet. It is the same to one of the LAN interface for DHCP-1 server. For other DHCP servers, the default subnet mask is 255.255.255.0/24, 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.





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 networks according to 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 DNS Servers.
8. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign WINS Servers.
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 example, this gateway will assign IP address to local computers, but local computers will go to Internet through another gateway.
10. **Server:** Check the “Enable” box to activate the DHCP server.

### 3.1.6.2.4 Fixed Mapping

Press “**Fixed Mapping ...**” button at the bottom of the DHCP server list page and you can specify a certain IP address for designated local device (MAC address) manually, so that the DHCP Server will reserve the special IPs for designated devices. For internal servers, you can use this feature to ensure each of them receives same IP address all the time.

Fixed Mapping

[ Help ]

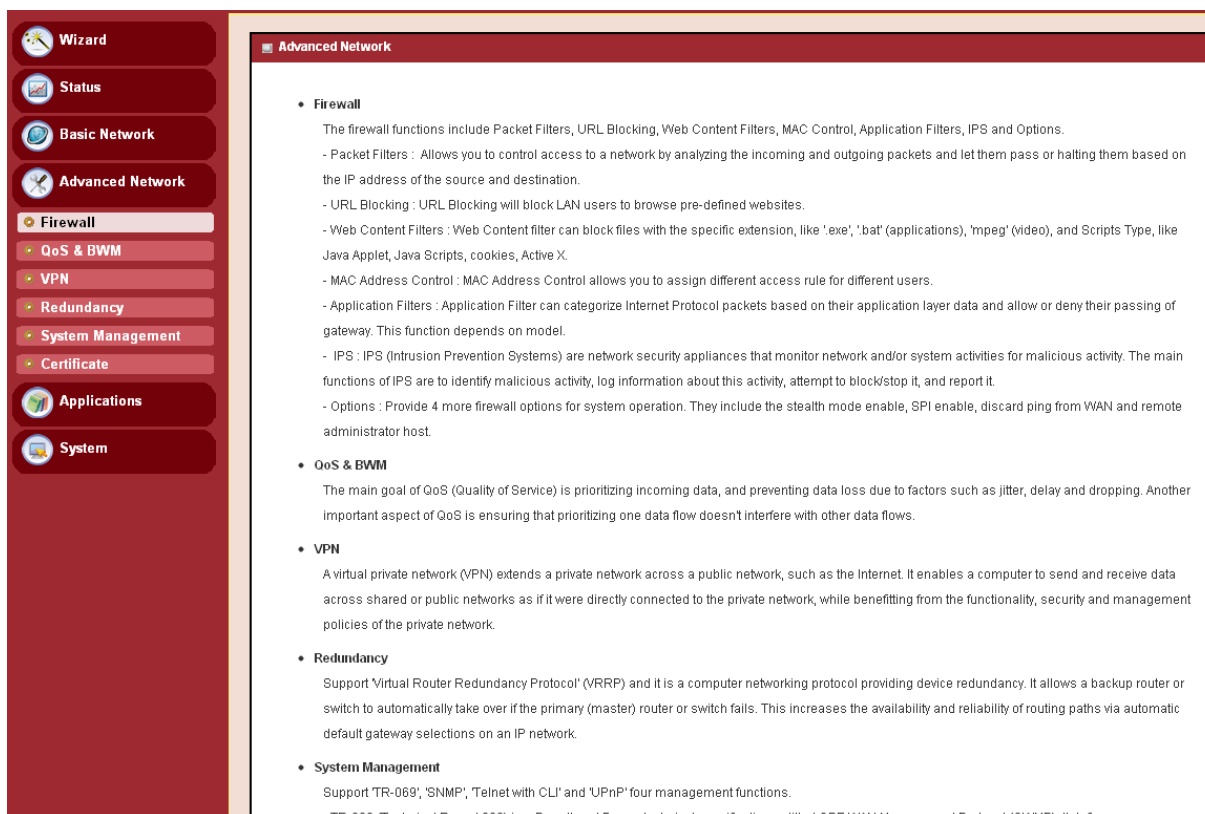
DHCP clients
-- select one --
Copy to ID --

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

<<Previous
Next>>
Save
Undo
Back

## 3.2 Advanced Network

This device also supports many advanced network features, such as Firewall, QoS & Bandwidth Management, VPN Security, Redundancy, System Management and Certificate. You can finish these configurations in this section.



**Advanced Network**

- Firewall**

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and Options.

  - Packet Filters : Allows you to control access to a network by analyzing the incoming and outgoing packets and let them pass or halting them based on the IP address of the source and destination.
  - URL Blocking : URL Blocking will block LAN users to browse pre-defined websites.
  - Web Content Filters : 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.
  - MAC Address Control : MAC Address Control allows you to assign different access rule for different users.
  - Application Filters : Application Filter can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway. This function depends on model.
  - 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.
  - Options : Provide 4 more firewall options for system operation. They include the stealth mode enable, SPI enable, discard ping from WAN and remote administrator host.
- QoS & BWM**

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.
- VPN**

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.
- Redundancy**

Support 'Virtual Router Redundancy Protocol' (VRRP) and it 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.
- System Management**

Support 'TR-069', 'SNMP', 'Telnet with CLI' and 'UPnP' four management functions.

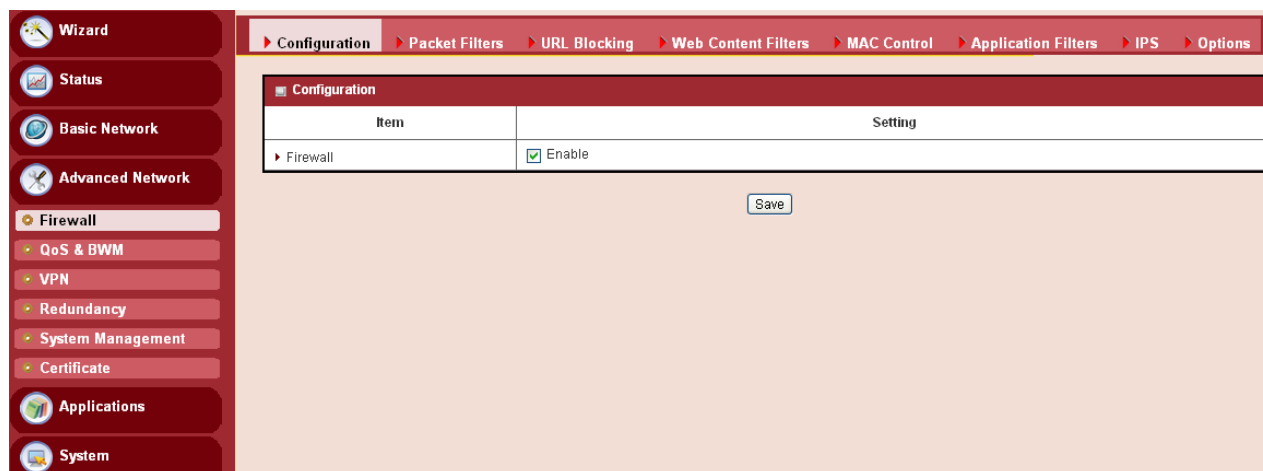
  - TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled 'CPE WAN Management Protocol' (CWMP). It defines an

## 3.2.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and some firewall options.

### 3.2.1.1 Configuration

One Firewall Enable check box lets you activate all firewall functions that you want.

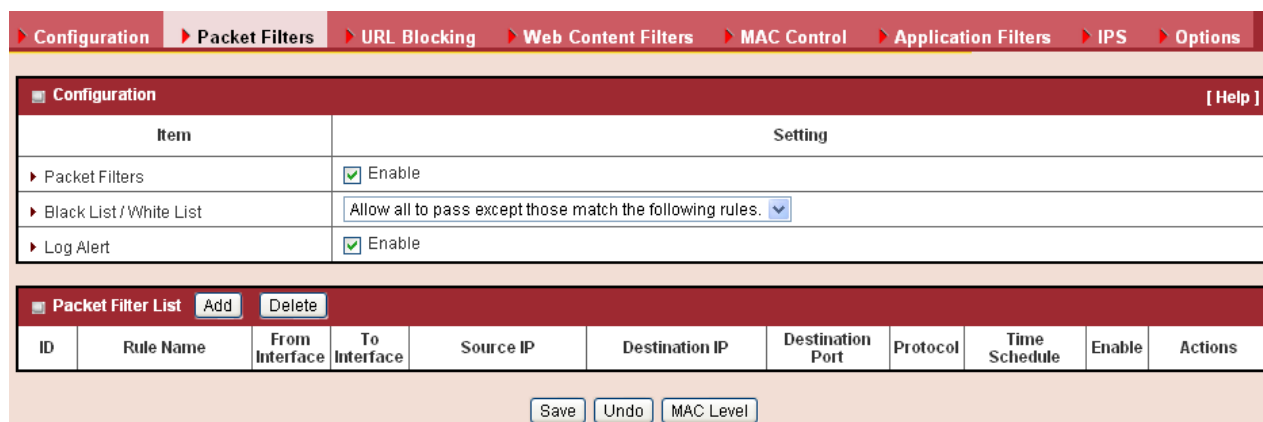


Item	Setting
Firewall	<input checked="" type="checkbox"/> Enable

Save

### 3.2.1.2 Packet Filters

**Packet Filters** function can let you define both outbound filter and inbound filter rules by specifying the source IP and destination IP in a rule. It enables you to control what packets are allowed or blocked to pass the router. Outbound filters are applied to all outbound packets. However, inbound filters are applied to packets that are destined to virtual servers or DMZ host / port only.



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

Packet Filter List

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

Save Undo MAC Level

### 3.2.1.2.1 Configuration

You can enable packet filter function here. And select one of the two filtering policies as follows. The first one is to define the black list. System will block the packets that match the active filter rules. However, the second one is the white list. System will allow the packets to pass the gateway, which match the active filter rules.

1. Allow all to pass except those which match the specified rules. (Black List)
2. Deny all to pass except those which match the specified rules. (White List)

Configuration <span>[ Help ]</span>	
Item	Setting
▶ Packet Filters	<input checked="" type="checkbox"/> Enable
▶ Black List / White List	Allow all to pass except those match the following rules. <span>▼</span>
▶ Log Alert	<input checked="" type="checkbox"/> Enable

Besides, you also can enable the log alerting so that system will record packet blocking events when filter rules are fired. At the right upper corner of screen, one “[Help]” command let you see the on-line help message about Packet Filter function.

### 3.2.1.2.2 Packet Filter List

It is a list of all packet filter rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existing packet filter rules by clicking corresponding “Edit” command buttons at the end of each filter rule in the Packet Filter List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the Packet Filter List caption.

Packet Filter List <span>Add</span> <span>Delete</span>										
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions
<span>Save</span> <span>Undo</span> <span>MAC Level</span>										

### 3.2.1.2.3 Packet Filter Rule Configuration

It supports the adding of one new rule or the editing of one existing rule. There are some parameters that need to be specified in one packet filter rule. They are Rule Name, From Interface, To Interface, Source IP, Destination IP, Destination Port, Protocol, Time Schedule and finally, the rule enable.

Packet Filter Rule Configuration	
Item	Setting
▶ Rule Name	Rule1
▶ From Interface	Any
▶ To Interface	Any
▶ Source IP	Specific IP Address
▶ Destination IP	Specific IP Address
▶ Destination Port	User-defined Service
▶ Protocol	TCP
▶ Time Schedule	(0) Always
▶ Rule	<input type="checkbox"/> Enable

- 1. Rule Name:** The name of packet filter rule.
- 2. From Interface:** Any interface or some LAN interface or some WAN interface.
- 3. To Interface:** Any interface or some LAN interface or some WAN interface.
- 4. Source IP:** Specify the Source IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A “0.0.0.0” implies all IP addresses.
- 5. Destination IP:** Specify the Destination IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A “0.0.0.0” implies all IP addresses.
- 6. Destination Port:** Choose “User-defined Service” to let you specify manually the destination service port of packets that want to be filtered out in the packet filter rule. You can define a single port (80) or a range of ports (1000-1999). A “0” implies all ports are used. You also can choose one well-known service instead so that the chosen service will provide its destination port and protocol number for the rule. The supported well-known services include:

-- select one --

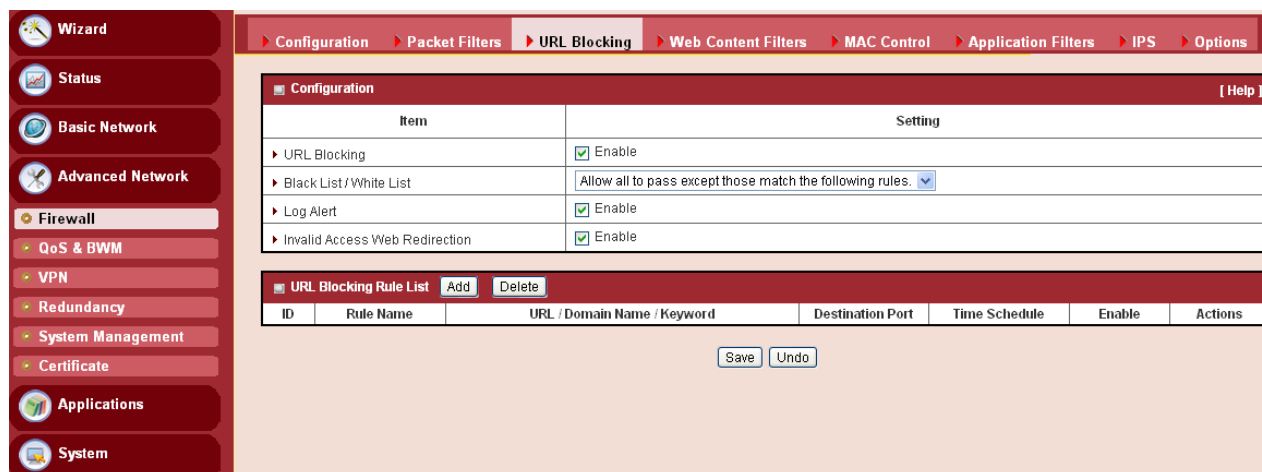
-- select one --
Any (Both:1-65535)
FTP (TCP:21)
SSH (TCP:22)
TELNET (TCP:23)
SMTP (TCP:25)
TFTP (UDP:69)
HTTP (TCP:80)
POP3 (TCP:110)
SFTP (TCP:115)
SNMP & traps (UDP:161-162)
HTTPS (TCP:443)
SMTPs (TCP:465)
ISAKMP (UDP:500)
RTSP (TCP:554)
POP3s (TCP:995)
L2TP (UDP:1701)
PPTP (TCP:1723)

7. **Protocol:** Specify which packet protocol is to be filtered. It can be TCP, UDP, or Both.
8. **Time Schedule:** The rule can be turned on 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**.
9. **Rule Enable:** Check the enable box if you want to activate 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.

### 3.2.1.3 URL Blocking

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

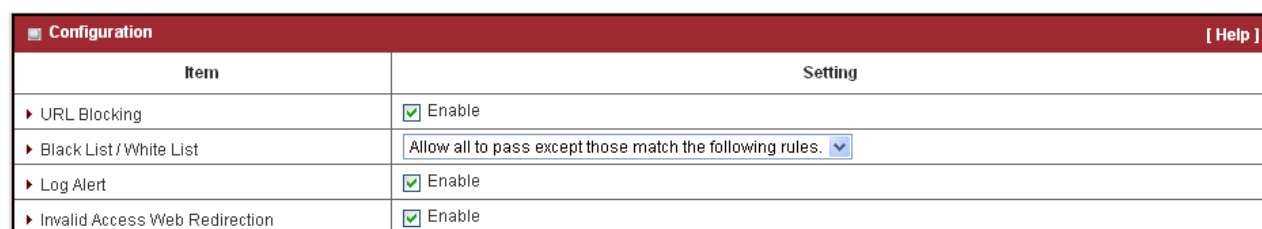


The screenshot shows the DIGISOL Firewall Configuration interface. On the left is a sidebar with navigation options: Wizard, Status, Basic Network, Advanced Network, Firewall (selected), QoS & BWM, VPN, Redundancy, System Management, Certificate, Applications, and System. The main area has a top navigation bar with tabs: Configuration, Packet Filters, URL Blocking (selected), Web Content Filters, MAC Control, Application Filters, IPS, and Options. Below the tabs is a 'Configuration' section with a table of settings:

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 checked="" type="checkbox"/> Enable
Invalid Access Web Redirection	<input checked="" type="checkbox"/> Enable

Below the table is a 'URL Blocking Rule List' section with 'Add' and 'Delete' buttons. It contains a table with columns: ID, Rule Name, URL / Domain Name / Keyword, Destination Port, Time Schedule, Enable, and Actions. At the bottom are 'Save' and 'Undo' buttons.

#### 3.2.1.3.1 Configuration



The screenshot shows the 'Configuration' section of the DIGISOL Firewall Configuration interface. It contains a table with the following settings:

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 checked="" type="checkbox"/> Enable
Invalid Access Web Redirection	<input checked="" type="checkbox"/> Enable

1. **URL Blocking:** Check the enable box if you want to activate URL Blocking function.
2. **Black List / White List:** Select one of the two filtering policies for the defined rules in URL Blocking Rule List.
  - Allow all to pass except those which match the specified rules (Black List).
  - Deny all to pass except those which match the specified rules (White List).
3. **Log Alert:** Enable the log alerting so that system will record URL blocking events when blocking rules are fired.
4. **Invalid Access Web Redirection:** Users will see a specific web page to know their

access is blocked by rules.

5. **[Help]:** At the right upper corner of the screen, one “[Help]” command lets you see the on-line help message about URL Blocking function.

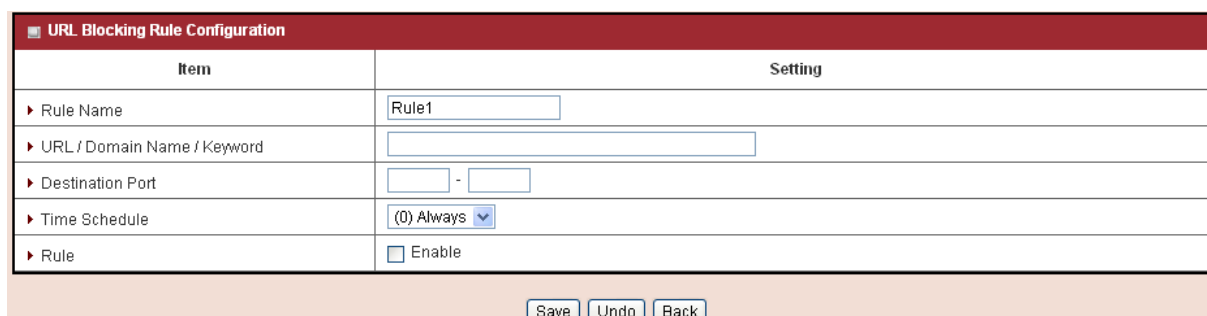
### 3.2.1.3.2 URL Blocking Rule List

It is a list of all URL Blocking rules. You can add one new rule by clicking on the “**Add**” command button. But also you can modify some existing URL blocking rules by clicking the corresponding “**Edit**” command buttons at the end of each blocking rule in the URL Blocking Rule List. Besides, unnecessary rules can be removed by checking the “**Select**” box for those rules and then clicking on the “**Delete**” command button at the URL Blocking Rule List caption



### 3.2.1.3.3 URL Blocking Rule Configuration

It supports the adding of one new rule or the editing of one existing rule. There are some parameters which need to be specified in one URL blocking rule. They are Rule Name, URL / Domain Name / Keyword, Destination Port, Time Schedule and finally, the Rule enable.



1. **Rule Name:** The name of URL blocking rule.
2. **URL/Domain Name/Keyword:** If any part of the Website's URL matches the pre-defined words, 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., “**google, yahoo, org**”; In addition to URL keywords, it can also block the designated domain name, like “**www.xxx.com**”, “**www.123aaa.org, mma.com**”.
3. **Destination Port:** Specify the destination port in URL requests that want to be blocked in the URL blocking rule. You can define a single port (80) or range of ports (1000-1999). An empty or “0” implies all ports are used.
4. **Time Schedule:** The rule can be turned on according to the schedule rule you specified,



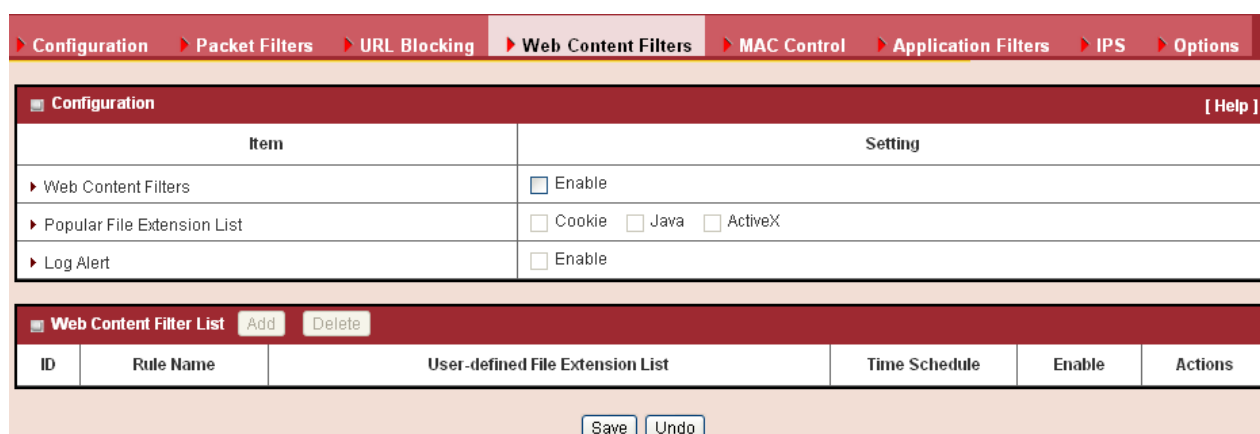
and gives users more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System >> Scheduling menu**.

5. **Rule Enable:** Check the enable box if you want to activate 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 Web Content Filters

**Web Content Filters** can block HTML requests with the specific extension file name, like ".exe", ".bat" (applications), "mpeg" (video) and block HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.



Item	Setting
Web Content Filters	<input 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
----	-----------	----------------------------------	---------------	--------	---------

#### 3.2.1.4.1 Configuration

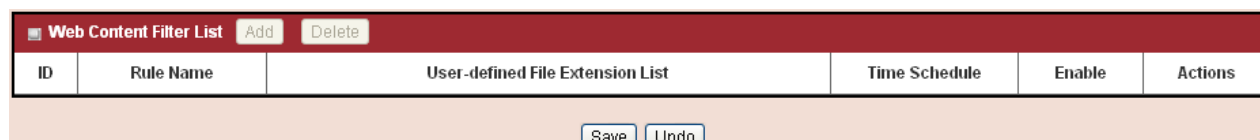


Item	Setting
Web Content Filters	<input type="checkbox"/> Enable
Popular File Extension List	<input type="checkbox"/> Cookie <input type="checkbox"/> Java <input type="checkbox"/> ActiveX
Log Alert	<input type="checkbox"/> Enable

1. **Web Content Filters:** Check the Enable box if you want to enable Web Content Filters function.
2. **Popular File Extension List:** Check which extension types, Cookie, Java, ActiveX, are to be blocked.
3. **Log Alert:** Enable the log alert so that system will record Web content filtering events when filtering rules are fired.

### 3.2.1.4.2 Web Content Filter Rule List

It is a list of all Web Content Filter rules. You can add one new rule by clicking on the “**Add**” command button. But also you can modify some existing Web Content Filter rules by clicking corresponding “**Edit**” command buttons at the end of each filtering rule in the Web Content Filter List. Besides, unnecessary rules can be removed by checking the “**Select**” box for those rules and then clicking on the “**Delete**” command button at the Web Content Filter List caption.



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

### 3.2.1.4.3 Web Content Filter Configuration

It supports the adding of one new rule or the editing of one existing rule. There are some parameters that need to be specified in one Web Content Filter rule. They are Rule Name, User-defined File Extension List, Time Schedule and finally, the rule enable.



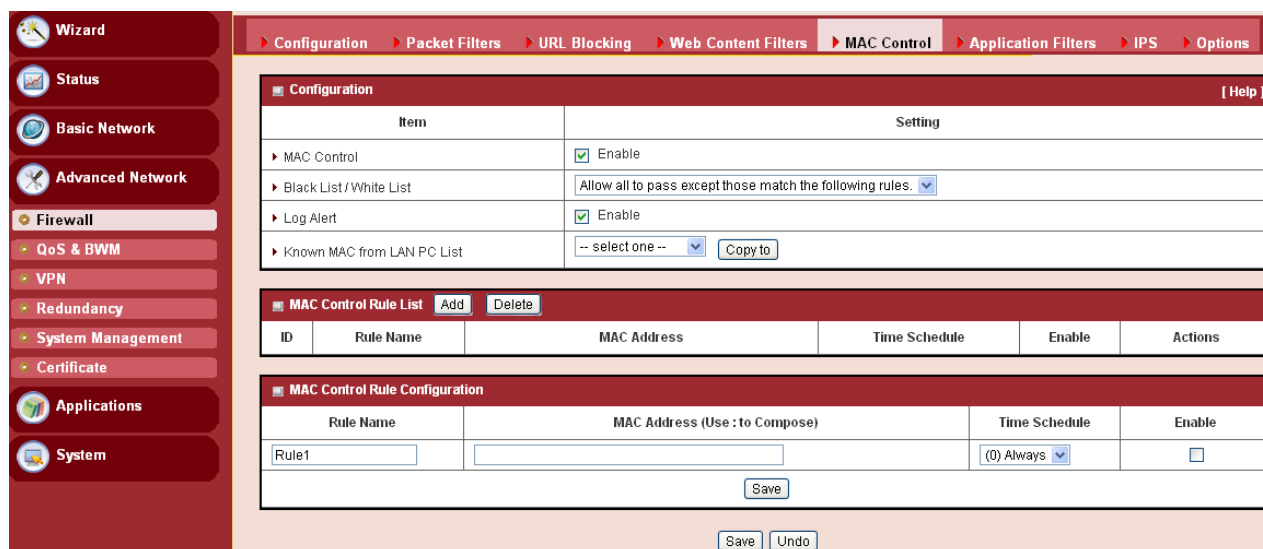
Rule Name	User-defined File Extension List (Use ; to Concatenate)	Time Schedule	Enable
Rule1		(0) Always	<input type="checkbox"/>

- 1. Rule Name:** The name of Web Content Filter rule.
- 2. User-defined File Extension List:** You can enter up to 10 file extensions to be blocked in a rule by using ‘;’ to concatenate these file extensions.
- 3. Time Schedule:** The rule can be turned on 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.
- 4. Enable:** Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

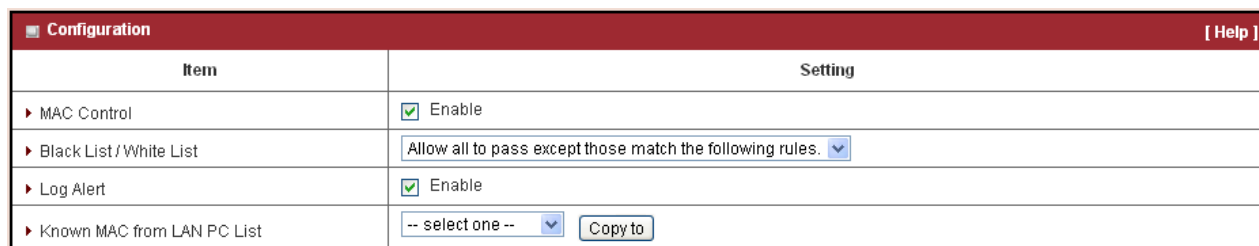
Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

### 3.2.1.5 MAC Control

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



#### 3.2.1.5.1 Configuration



- MAC Control:** Check the “**Enable**” box to activate the MAC Control function. All of the settings in this page will take effect only when “**Enable**” is checked.
- Black List / White List:** Select one of the two filtering policies for the defined rules.  
Black List - Allow all to pass except those which match the specified rules.  
White List - Deny all to pass except those which match the specified rules.
- Log Alert:** Enable the log alert so that system will record MAC control events when control rules are fired.
- Known MAC from LAN PC List:** You can see all the connected clients from this list, and copy their MAC address to the MAC Control Rule Configuration window below.

### 3.2.1.5.2 MAC Control Rule List

It is a list of all MAC Control rules. You can add one new rule by clicking on the “**Add**” command button. But also you can modify some existing MAC control rules by clicking corresponding “**Edit**” command buttons at the end of each control rule in the MAC Control Rule List. Besides, unnecessary rules can be removed by checking the “**Select**” box for those rules and then clicking on the “**Delete**” command button at the MAC Control Rule List caption.

MAC Control Rule List <span>Add</span> <span>Delete</span>					
ID	Rule Name	MAC Address	Time Schedule	Enable	Actions

### 3.2.1.5.3 MAC Control Rule Configuration

It supports the adding of one new rule or the editing of one existing rule. There are some parameters that need to be specified in one MAC Control rule. They are Rule Name, MAC Address, Time Schedule and finally, the rule enable.

MAC Control Rule Configuration			
Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
<input type="text" value="Rule1"/>	<input type="text"/>	(0) Always <span>▼</span>	<input type="checkbox"/>
<span>Save</span>			

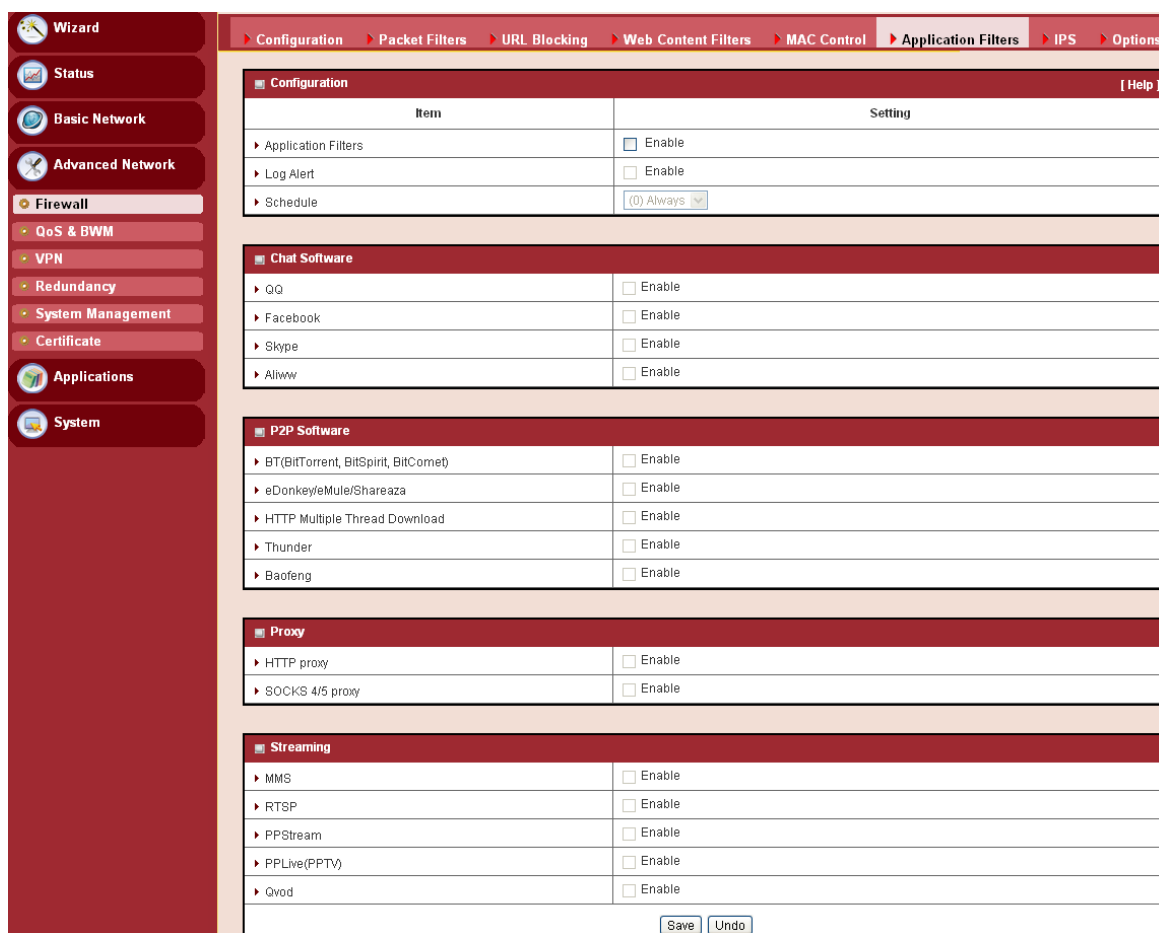
- 1. Rule Name:** The name of MAC Control rule.
- 2. MAC Address:** Input the MAC address of local device. You can input manually or copy it from **Known MAC from LAN PC List**. Please note the format of MAC address is like “xx:xx:xx:xx:xx:xx”. “x” is a hexadecimal digit.
- 3. Schedule:** The rule can be turn on 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.
- 4. Enable:** Check the box 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.

### 3.2.1.6 Application Filters

**Application Filters** can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway.

This device supports the application filters for various Internet chat software, P2P download, Proxy and A/V streaming. You can select the applications to be blocked after the function is enabled, and specify the schedule rule for such Application Filters function.



The screenshot shows the DIGISOL firewall configuration interface. The left sidebar contains navigation options: Wizard, Status, Basic Network, Advanced Network, Firewall (selected), QoS & BWM, VPN, Redundancy, System Management, Certificate, Applications, and System. The main panel displays the 'Application Filters' configuration tab. It includes a 'Configuration' section with a table of settings, followed by sections for 'Chat Software', 'P2P Software', 'Proxy', and 'Streaming', each with a table of settings. At the bottom, there are 'Save' and 'Undo' buttons.

Item	Setting
Application Filters	<input type="checkbox"/> Enable
Log Alert	<input type="checkbox"/> Enable
Schedule	(0) Always

Item	Setting
QQ	<input type="checkbox"/> Enable
Facebook	<input type="checkbox"/> Enable
Skype	<input type="checkbox"/> Enable
Aliww	<input type="checkbox"/> Enable

Item	Setting
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

Item	Setting
HTTP proxy	<input type="checkbox"/> Enable
SOCKS 4/5 proxy	<input type="checkbox"/> Enable

Item	Setting
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

### 3.2.1.6.1 Configuration

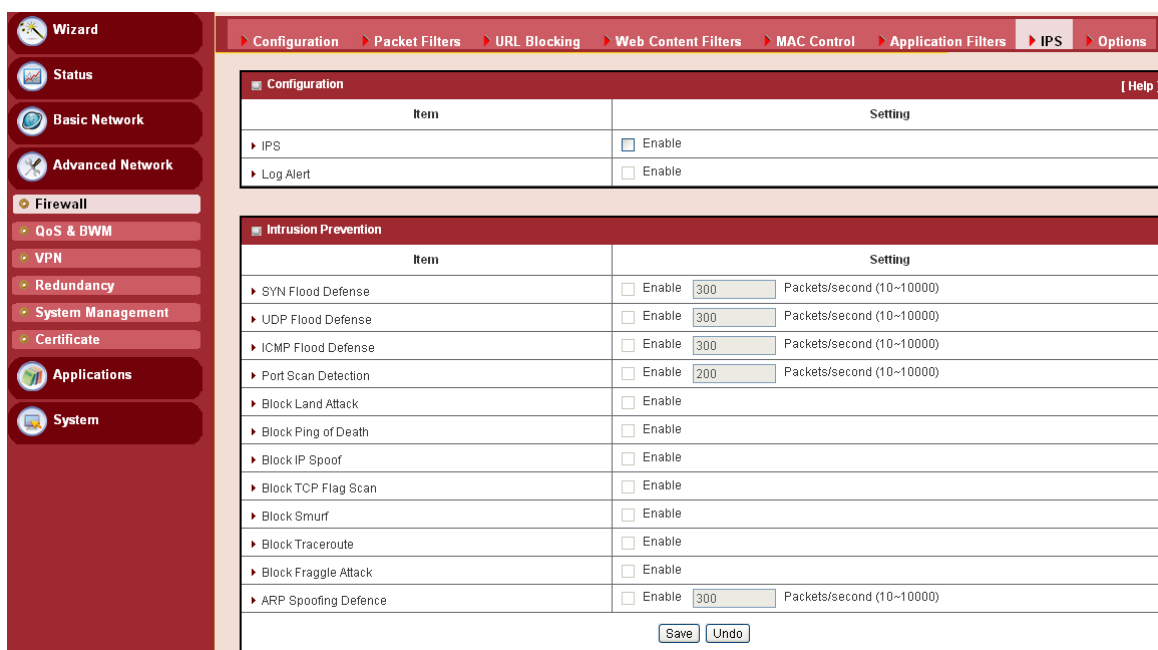
Configuration [ Help ]	
Item	Setting
Application Filters	<input type="checkbox"/> Enable
Log Alert	<input type="checkbox"/> Enable
Schedule	(0) Always

- Application Filters:** Check the “**Enable**” box to activate the Application Filters function. All of the settings in this page will take effect only when “**Enable**” is checked.
- Log Alert:** Enable the log alerting so that system will record Application Filter events when filtering rules are fired.
- Schedule:** All Application Filter rules can be turned on according to the schedule rule you specified, and give user more flexibility on access control. By default, they are always turned on when Application Filters function is enabled. For more details, please refer to the **System >> Scheduling menu**.

### 3.2.1.7 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.

You can enable the IPS function and check the listed intrusion activities if necessary. There are some intrusion prevention items that need further Threshold parameter to work properly for intrusion detection. Besides, you can enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.



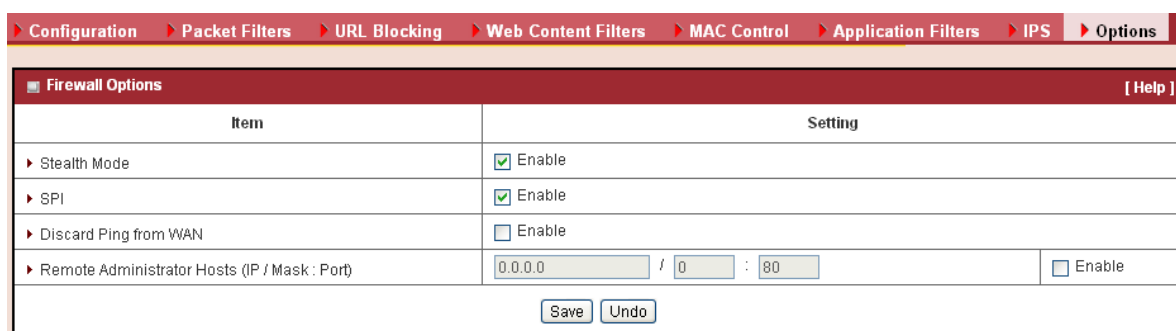
Item	Setting
IPS	<input checked="" type="checkbox"/> Enable
Log Alert	<input checked="" type="checkbox"/> Enable

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

Save Undo

### 3.2.1.8 Options



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

3. **Discard PING from WAN:** If this feature is enabled, this gateway won't reply any ICMP request packet from WAN side. It means any remote host can't get response when pinged to this gateway. "Ping" is a useful command that we use to detect if a certain host is alive or not. But it also lets hackers know about this. Therefore, many Internet servers will be set to ignore IGMP request.
4. **Remote Administrator Hosts (IP / Mask: Port):** In general, only local clients (LAN users) can browse the device's built-in web pages for device administration setting. This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specify a group of trusted IP addresses. For example, "10.1.2.0/24".

**NOTE: When Remote Administration is enabled, the web server port will be configured to 80 as default. You also can change web server port to other port**

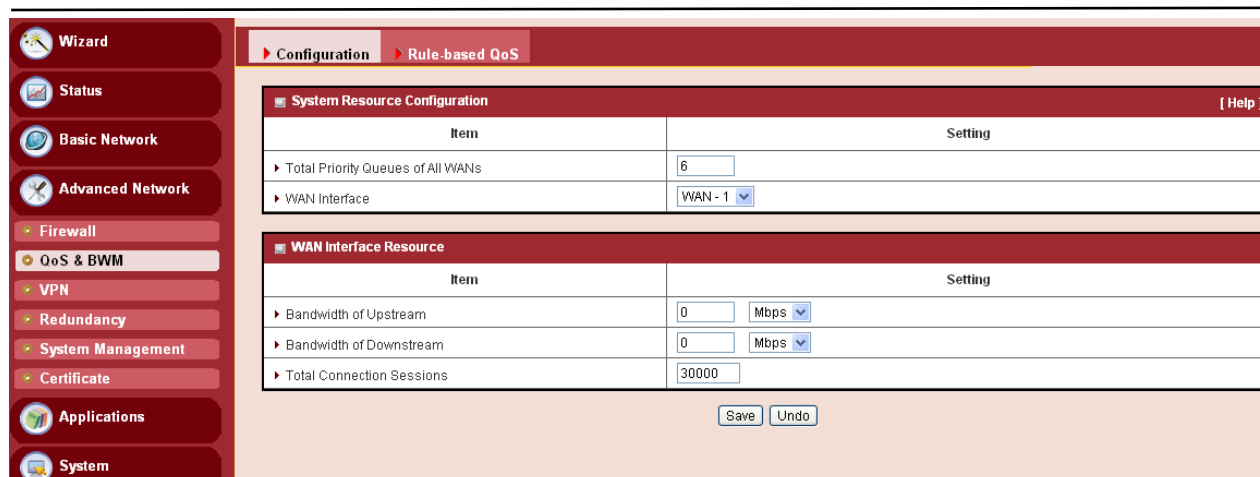
Afterwards, click on "**Save**" to store your settings or click "**Undo**" to give up the changes.

### 3.2.2 QoS & BWM

The total amount of data traffic increases nowadays as the higher demand of mobile devices, like Game / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

The main goal of QoS & BWM (Quality of Service and Bandwidth Management) 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 does not interfere with other data flows. So, 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.

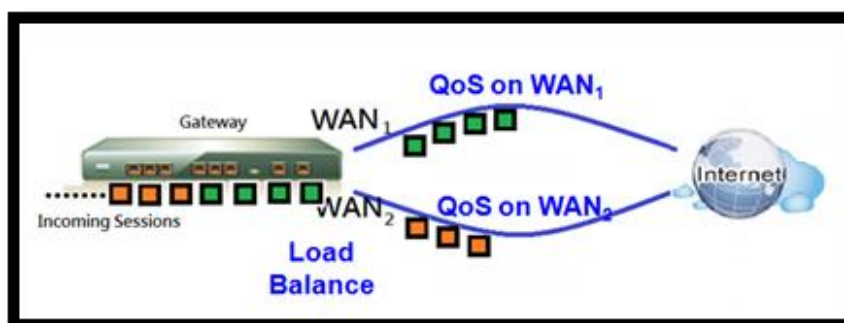
To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management. It provides a Rule-based QoS to carry out the requirements.



### 3.2.2.1 Configuration

#### ■ QoS on Multiple WAN Interfaces

- QoS on all WAN interfaces satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management in a more flexible approach.
- Integrated with Multi-WAN load balance function to maximize the total network throughput.



#### ■ Flexible Bandwidth Management (FBM)

- Adjust the bandwidth distribution dynamically based on current bandwidth usage situation to get the maximum system network performance, and it is transparent to all users.

Before QoS & BWM function can work correctly, this gateway needs to define the resource for each WAN interface. First one is the available bandwidth of WAN connection. It was set in the **Basic Network >> WAN >> Physical Interface menu** and shown here. Second one is the maximum number of connection sessions that the WAN interface supports. The last is the maximum number of priority queues that the WAN interface supports.



Configuration
Rule-based QoS

System Resource Configuration [ Help ]

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

- Total Priority Queues of All WANs:** Input the maximum number of priority queues for all WAN interfaces.
- WAN Interface:** Select the WAN interface to configure following parameters.
- Bandwidth of Upstream:** The maximum bandwidth of uplink in Mbps.
- Bandwidth of Downstream:** The maximum bandwidth of downlink in Mbps.
- Total Connection Sessions:** Input the maximum number of connection sessions for the WAN interface.

### 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.

#### Flexible QoS Rule Definition

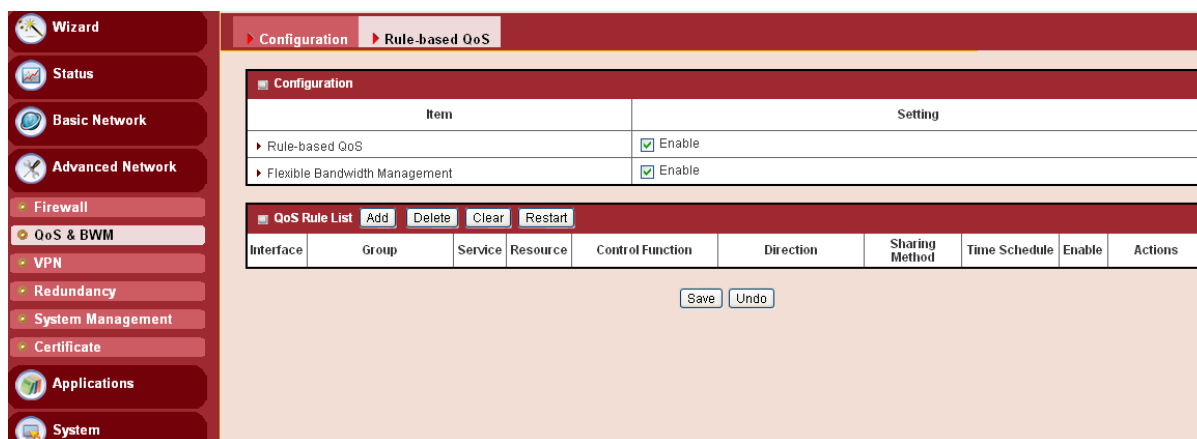
- Multiple Group Categories
  - Specify the group category in a QoS rule for the target objects that rule to be applied on.
  - Group Category is based on VLAN ID, MAC Address, IP Address, Host Name or Packet Length. Category depends on model.
- Differentiated Services
  - Specify the service type in a QoS rule for the target packets that rule to be applied on.
  - Differentiated services can be based on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services.
  - Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110),

Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), Net Meeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723).

- Available Control Functions
  - There are 4 resources that can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources.
  - For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth. For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.
- Individual / Group Control
  - One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model.
- Outbound / Inbound Control
  - One QoS rule can be applied to the outbound or inbound direction of packet flow, even for both. This feature depends on model.

### 3.2.2.2.1 Configuration

It supports the activation of Rule-based QoS.



1. **Rule-based QoS Enable:** Check the box if you want to enable the QoS & BWM function.

Besides, at the right upper corner of the screen, one “[Help]” command lets you see the on-line help message about Rule-based QoS function.

### 3.2.2.2.2 QoS Rule List

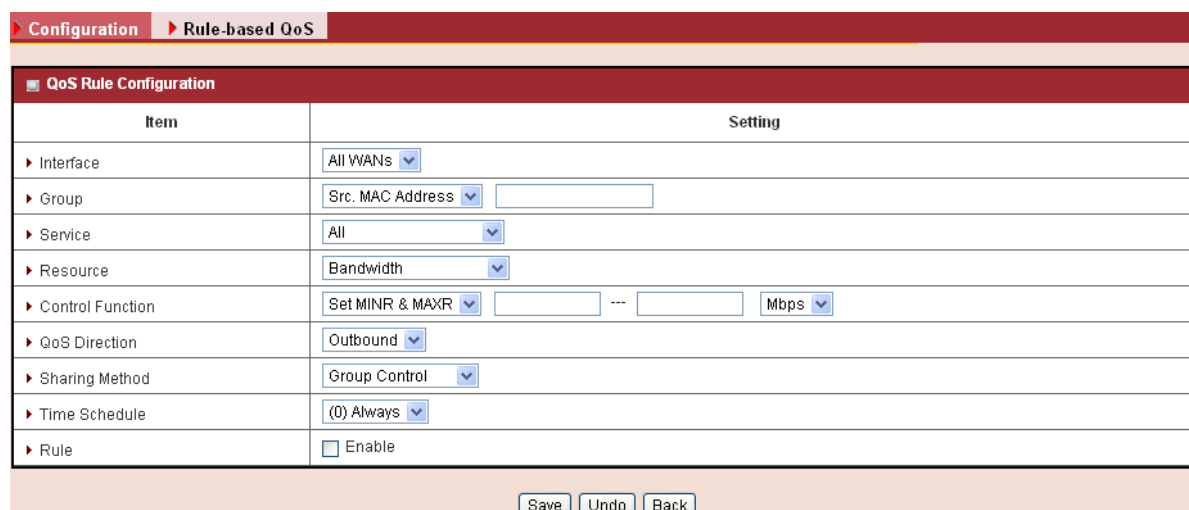
It is a list of all QoS rules. You can add one new rule by clicking on the “**Add**” command button. But also you can modify some existing QoS rules by clicking corresponding “**Edit**” command buttons at the end of each rule in the QoS Rule List. Besides, unnecessary rules can be removed by checking the “**Select**” box for those rules and then clicking on the “**Delete**” command button at the QoS Rule List caption. One “**Clear**” command button can let you clear all rules and “**Restart**” command button can let you restart the operation of all QoS rules.

QoS Rule List									
<div> Add Delete Clear Restart </div>									
Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
<div> Save Undo </div>									

- Add:** After you enable the rule-based QoS function, you can click on the “Add” button to create a new QoS rule.
- Delete:** After you select some QoS rules by checking the “Select” box for each rule, you can click on the “Delete” button to remove those rules from the list.
- Clear:** Delete all existing QoS rules.
- Restart:** Press “Restart” button to re-initiate all QoS rules again.
- Edit:** Configure the specific QoS rule again.

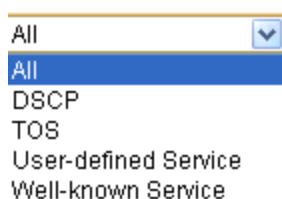
### 3.2.2.2.3 QoS Rule Configuration

It supports the adding of one new rule or the editing of one existing rule. There are some parameters that need to be specified in one QoS rule. They are Interface, Group, Service, Resource, Control Function, QoS Direction, Sharing Method, Time Schedule and finally, the rule enable.

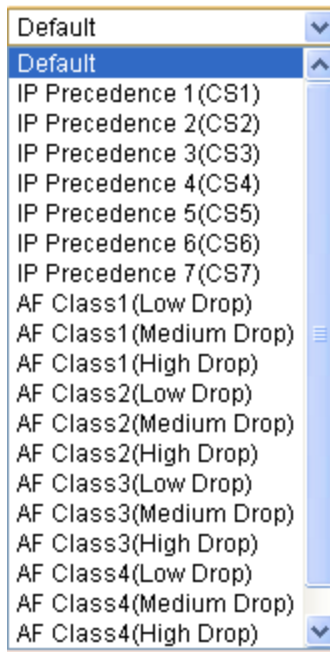


Item	Setting
Interface	All WANs
Group	Src. MAC Address
Service	All
Resource	Bandwidth
Control Function	Set MINR & MAXR
QoS Direction	Outbound
Sharing Method	Group Control
Time Schedule	((0) Always
Rule	<input type="checkbox"/> Enable

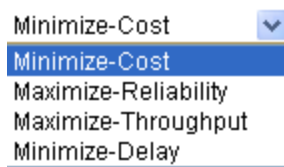
- Interface:** Select the WAN interface for the QoS rule.
- Group:** Specify the target client members for the rule by their VLAN ID, MAC Address, IP Address, Host Name or Group Object. These base categories depend on product models. Besides, “IP Address” group can be defined as an IP range with an IP address and its subnet mask and “Group Object” is defined in the **System -> Grouping** menu. But what kinds of groups to use depend on product models.
- Service:** There are 5 options for service, including All, DSCP, TOS, User-defined Services and Well-known Service as below.



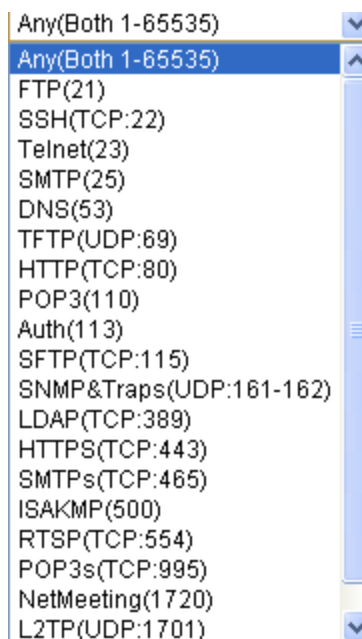
By default, it is “All”. It defines “what” kinds of service packets need to be managed. When “DSCP” is selected, another “DiffServ CodePoint” value must be specified. DSCP means DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags. The DSCP categories that this gateway can detect are as below.



You need to choose a correct one according to your device's specification. When “**TOS**” is selected for Service, TOS value must be chosen from a list of 4 options. For example:



When “**User-defined Services**” is selected, two more parameters, Protocol Number and Service Port Range, must be defined. Protocol Number is either TCP or UDP or Both. Finally, when “**Well-known Service**” is selected, you can choose the well-known from a list like:



4. **Resource:** There are 4 resources that can be chosen to control in the QoS rule. They are “Bandwidth”, “Connection Sessions”, “Priority Queues” and “DiffServ Code Points”.
5. **Control Function:** It depends on the chosen resource. For “Bandwidth” resource, the control function is “**Set MINR & MAXR**”. For “Connection Sessions”, the control function is “Set Session Limitation”. For “Priority Queues”, it is “Set Priority”. However, for “DiffServ Code Points”, it is “DSCP Marking” and you need to specify the DSCP value additionally.
6. **QoS Direction:** Select the traffic direction to be applied for this rule.

Direction	
IN	For Inbound data
OUT	For Outbound data
BOTH	Inbound and Outbound

7. **Sharing Method:** If you want to apply the value of control setting on each selected host in the “**Group**”, you need to select “**Individual Control**” for Sharing Method. On the other hand, if the value of control setting wants to be applied on all selected hosts in the “Group”, you need to select “Group Control”. For example, you define Control Function as “Set Session Limitation” and the limited sessions are 2000 sessions. You also define Sharing Method as “Individual Control”. Then, that means the maximum connection sessions of each selected host can’t exceed 2000 sessions. On the contrary, changing to “Group Control”, it means that group of client hosts totally can’t use over 2000 connection sessions.
8. **Time Schedule:** The rule can be turned on according to the schedule rule you specified, and gives users 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**.
9. **Enable:** Check the box 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.

### Example #1 for adding a “DSCP” type QoS rule

Configuration Rule-based QoS	
QoS Rule Configuration	
Item	Setting
Interface	All WANs
Group	IP 10.0.75.196 Subnet Mask: 255.255.255.255 (/32)
Service	DSCP DiffServ CodePoint IP Precedence 4(CS4)
Resource	DiffServ Code Points
Control Function	DSCP Marking AF Class2(High Drop)
QoS Direction	Inbound
Sharing Method	Group Control
Time Schedule	(0) Always
Rule	<input checked="" type="checkbox"/> Enable

- ◆ Interface: Select “All WANs”.
- ◆ Group: Select “IP” and enter IP range: 10.0.75.196/30.
- ◆ Service: Select “DSCP” with DiffServ CodePoint is CS4.
- ◆ Resource: Select “DiffServ Code Points”.
- ◆ Control Function: Select “DSCP Marking” with “AF Class 2 (High Drop)”.
- ◆ QoS Direction: Select “Inbound” for inbound traffic only.
- ◆ Sharing Method: Select “Group Control”.
- ◆ Time Schedule: Leave the default value of“(0) Always” as it is.

This rule means IP packets from all WAN interfaces to LAN IP address 10.0.75.196 ~ 10.0.75.199 which have DiffServ code points with “IP Precedence 4(CS4)” value will be modified by “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

### Example #2 for adding a “Connection Sessions” type QoS rule

QoS Rule Configuration	
Item	Setting
Interface	All WANs
Group	IP 10.0.75.196 Subnet Mask: 255.255.255.255 (/32)
Service	All
Resource	Connection Sessions
Control Function	Set Session Limitation 20000
QoS Direction	Inbound
Sharing Method	Group Control
Time Schedule	(0) Always
Rule	<input checked="" type="checkbox"/> Enable

- ◆ Interface: Select “WAN-1”.
- ◆ Group: Select “IP” and enter IP range: 10.0.75.16/28.
- ◆ Service: Select “ALL”.
- ◆ Resource: Select “Connection Sessions”.

- ◆ Control Function: Select “Set Session Limitation”, and set session number to 20000.
- ◆ QoS Direction: Select “Outbound” for outbound traffic only. It is for the client devices under the gateway to establish multiple sessions with servers in the Internet.
- ◆ Sharing Method: Select “Group Control”.
- ◆ Time Schedule: Leave the default value of“(0) Always” as it is.

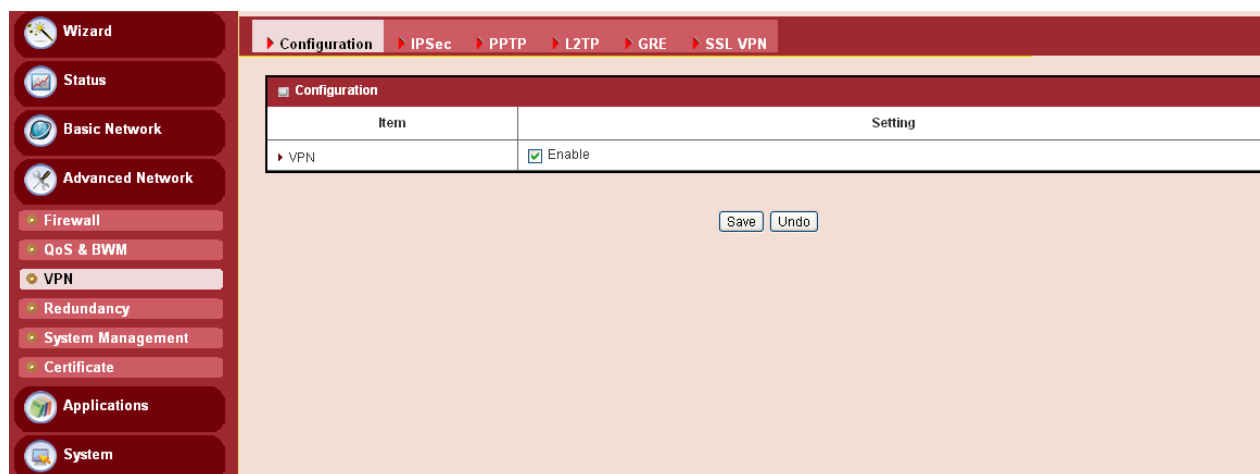
This rule defines that all client hosts, whose IP address is in the range of 10.0.75.16~31, can access the Internet and keep a maximum 20000 connection sessions totally at any time.

### 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 benefiting 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 product series supports following tunneling technologies to establish secure tunnels between multiple sites for data transferring, including IPSec, PPTP, L2TP (over IPSec) and GRE. Advanced functions include Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN.

In Configuration page, there is only one parameter, “VPN” with “Enable” Check box. Check that box to activate the VPN function whatever you use which tunneling technology beforehand.

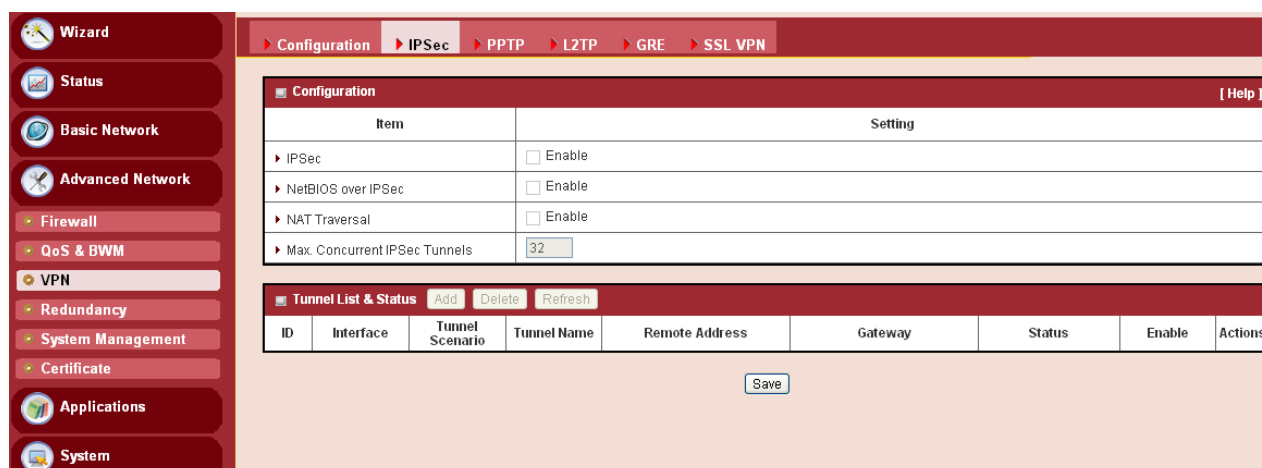




### 3.2.3.1 IPSec

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.

An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase. At IKE phase, IKE authenticates IPSec peers and negotiates IKE SAs (Security Association) during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2. At IPSec phase, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After these both phases, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

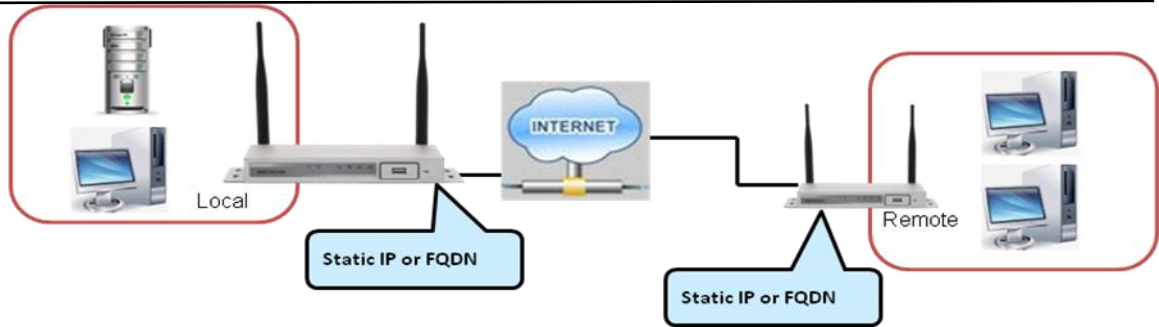


#### 3.2.3.1.1 IPSec VPN Tunnel Scenarios

There are some common IPSec VPN connection scenarios as follows:

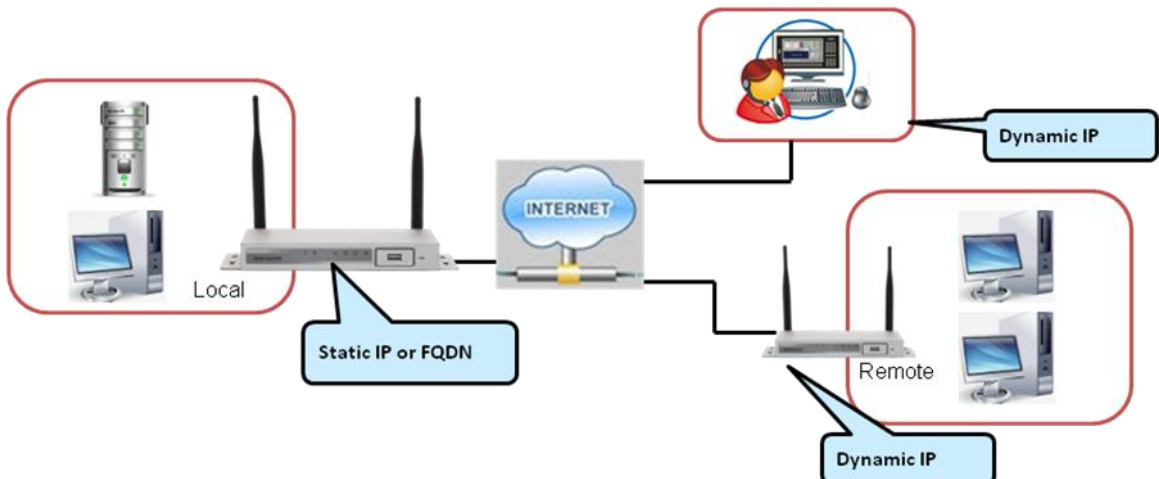
- Site to Site

DG-WU2005V establishes IPSec VPN tunnels with security gateway in headquarters or branch offices. Either local or remote device, 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 for data communication between these two subnets of hosts.



- **Dynamic VPN**

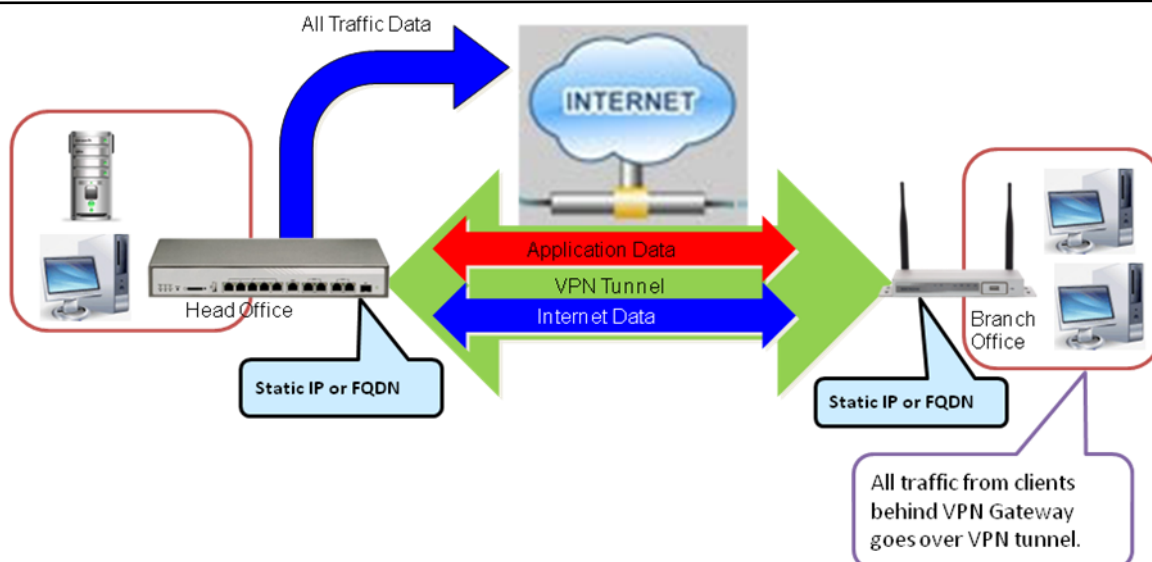
Business Security Gateway can ignore IP information of clients when using Dynamic VPN, so it is suitable for users to build VPN tunnels with Business Security Gateway from a remote mobile host or mobile site. Remote peer is a host or a site which will be indicated in the negotiation packets, including what remote subnet is. It must be noted that the remote peer has to initiate the tunnel establishing process first in this application scenario.



There is one more advanced IPSec VPN application:

- **Site to Site – Support Full Tunnel Application**

When Full Tunnel function of remote Business Security Gateway is enabled, all data traffic from remote clients behind remote Business Security Gateway will go over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote Business Security 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 Business Security Gateway, including surfing the Internet. 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 Business Security Gateway.



### 3.2.3.1.2 IPSec Configuration

Configuration <span style="float: right;">[ Help ]</span>	
Item	Setting
▶ IPSec	<input type="checkbox"/> Enable
▶ NetBIOS over IPSec	<input type="checkbox"/> Enable
▶ NAT Traversal	<input type="checkbox"/> Enable
▶ Max. Concurrent IPSec Tunnels	32

1. **IPSec:** You could trigger the function of IPSec VPN if you check “Enable” box.
2. **NetBIOS over IPSec:** If you would like two Intranets behind two Business Security Gateways to receive the NetBIOS packets from Network Neighborhood, you have to check “Enable” box.
3. **NAT Traversal:** Some NAT routers will block IPSec packets if they don’t support IPSec pass through. If your Business Security Gateway connects to this kind of NAT router which does not support IPSec pass through, you need to activate this option in your Business Security Gateway.
4. **Max. Concurrent IPSec Tunnels:** 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

Tunnel List & Status <span>Add</span> <span>Delete</span> <span>Refresh</span>								
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. **Refresh:** To refresh the Tunnel List & Status each 2 seconds by clicking on the “Refresh” button.
4. **Tunnel:** Check the “Enable” box to activate the IPSec tunnel.
5. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

### 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 <input type="text" value="30"/> (seconds)

1. **Tunnel Name:** Enter the name of tunnel.
2. **Interface:** Decide the WAN Interface to establish the tunnel.
3. **Operation Mode:** Default is “Always on” and other options depend on product models.
4. **Tunnel Scenario:** Support “Site to Site” and “Dynamic VPN”.
5. **Encapsulation Protocol:** Default is ESP and other options depend on product models.
6. **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 exists in the opposite side of the VPN tunnel (Eg. You can input the LAN IP address of remote Business Security 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 Local & Remote Configuration

Local & Remote Configuration	
Item	Setting
Local Subnet	192.168.123.0 <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Local Netmask	-- select one -- -- select one -- -- select one -- -- select one -- -- select one --
Full Tunnel	<input type="checkbox"/> Enable
Remote Subnet	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Remote Netmask	-- select one -- -- select one -- -- select one -- -- select one -- -- select one --
Remote Gateway	<input type="text"/> (IP Address/FQDN)

Authentication	
Item	Setting
Key Management	IKE+Pre-shared Key <input type="text"/> (Min. 8 characters)
Local ID	Type: User Name ID: <input type="text"/>
Remote ID	Type: User Name ID: <input type="text"/>

IKE Phase	
Item	Setting
Negotiation Mode	Main Mode
X-Auth	None X-Auth Account User Name : <input type="text"/> Password : <input type="text"/>
Dead Peer Detection (DPD)	<input type="checkbox"/> Enable Timeout: 180 (seconds) Delay: 30 (seconds)

- Local Subnet:** The subnet of LAN site of local Business Security Gateway. It can be a host, a partial subnet, the whole subnet or multiple subnets of LAN site of local gateway. The device supports VPN hub and spoke function. There are 5 local subnets to be defined here and the information will be transferred to remote VPN sites for routing remote packets to these 5 local subnets via this VPN tunnel.
- Local Netmask:** The local netmask and associated local subnet IP can define a subnet domain for the local devices connected via the VPN tunnel. There are 5 local subnet domains to be defined here for hub and spoke function.
- Full Tunnel:** All traffic from Intranet of Business Security Gateway goes over the IPSec VPN tunnel if these packets don't match the Remote Subnet of other IPSec tunnels. That is, both application data and Internet access packets land up at the VPN concentrator.

4. **Remote subnet:** The subnet of LAN site of remote Business Security Gateway. It can be a host, a partial subnet, the whole subnet or multiple subnets of LAN site of remote gateway. Since the device supports VPN hub and spoke function, there are 5 remote subnets to be defined here and any packets that want these 5 remote subnets will be transferred via this VPN tunnel.
5. **Remote Netmask:** The remote netmask and associated remote subnet IP can define a subnet domain for the remote devices connected via the VPN tunnel. There are 5 remote subnet domains to be defined here for hub and spoke function.
6. **Remote Gateway:** Enter the IP address or FQDN of remote Business Security Gateway.

### 3.2.3.1.6 Authentication

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key <input type="text"/> (Min. 8 characters)
▶ Local ID	Type: User Name ID: <input type="text"/>
▶ Remote ID	Type: User Name ID: <input type="text"/>

1. **Key Management:** Select “IKE+Pre-shared Key” or “Manually”. Other options depend on product models. By default, “IKE+Pre-shared Key” method is adopted for key management. It is the first key used in IKE phase for both VPN tunnel initiator and responder to negotiate further security keys to be used in IPsec phase. The pre-shared key must be the same for both VPN tunnel initiator and responder. When “Manually” key management is adopted, the Pre-shared is not necessary.
2. **Local ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the Remote ID of the remote VPN peer. There are 4 types for Local ID: User Name, FQDN, User@FQDN and Key ID.
3. **Remote ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the local ID of the remote VPN peer. There are also 4 types for Remote ID: User Name, FQDN, User@FQDN and Key ID.

### 3.2.3.1.7 IKE Phase

IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode
▶ X-Auth	None <input type="text"/> X-Auth Account User Name: <input type="text"/> Password: <input type="text"/>
▶ Dead Peer Detection (DPD)	<input type="checkbox"/> Enable Timeout: 180 (seconds) Delay: 30 (seconds)
▶ Phase1 Key Life Time	3600 (seconds) (Max. 86400)

### 1. **Negotiation Mode:** Choose **Main Mode** or **Aggressive Mode**.

Main Mode provides identity protection by authenticating peer identities when pre-shared keys are used. The IKE SA's are used to protect the security negotiations. Aggressive mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.

2. **X-Auth:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or Business Security Gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server. There are 3 roles to let DG-WU2005V behave as for X-Auth authentication, including None, Server and Client. For None role, no X-Auth authentication happens during VPN tunnel establishment. For Server role, click "X-Auth Account" button to modify 10 user accounts for user validation during tunnel establishment to VPN server. Finally, for Client role, there are two additional parameters to fill: "User Name" and "Password" for valid user to initiate that tunnel.
3. **Dead Peer Detection:** This feature will detect if remote VPN peer still exists. Delay indicates the interval between detections, and Timeout indicates the timeout of detected to be dead.
4. **Phase 1 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.

### 3.2.3.1.8 IKE Proposal Definition

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

There are 4 IKE proposals that can be defined by you and used in IKE phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192 and AES-256.
2. **Authentication:** There are five algorithms that can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.



3. **DH Group:** There are nine groups that can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18.
4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishment.

### 3.2.3.1.9 IPSec Phase

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	<input type="text" value="28800"/> (seconds) (Max. 86400)

1. **Phase 2 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 2 between two VPN peers.

### 3.2.3.1.10 IPSec Proposal Definition

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

There are 4 IPSec proposals that can be defined by you and used in IPSec phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms that can be selected: DES, 3DES, AES-auto, AES-128, AES-192 and AES-256.
2. **Authentication:** There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.
3. **PFS Group:** There are nine groups that 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 other 3 IPSec proposals uses the same choice.
4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishing.



### 3.2.3.2 PPTP

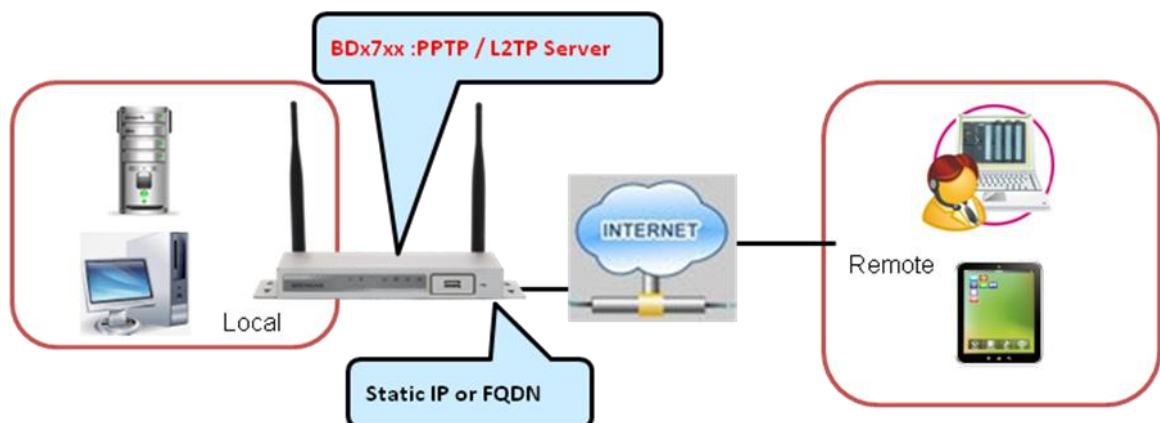
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families implement various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

#### 3.2.3.2.1 PPTP / L2TP VPN Tunnel Scenarios

There are some common PPTP/L2TP VPN connection scenarios as follows:

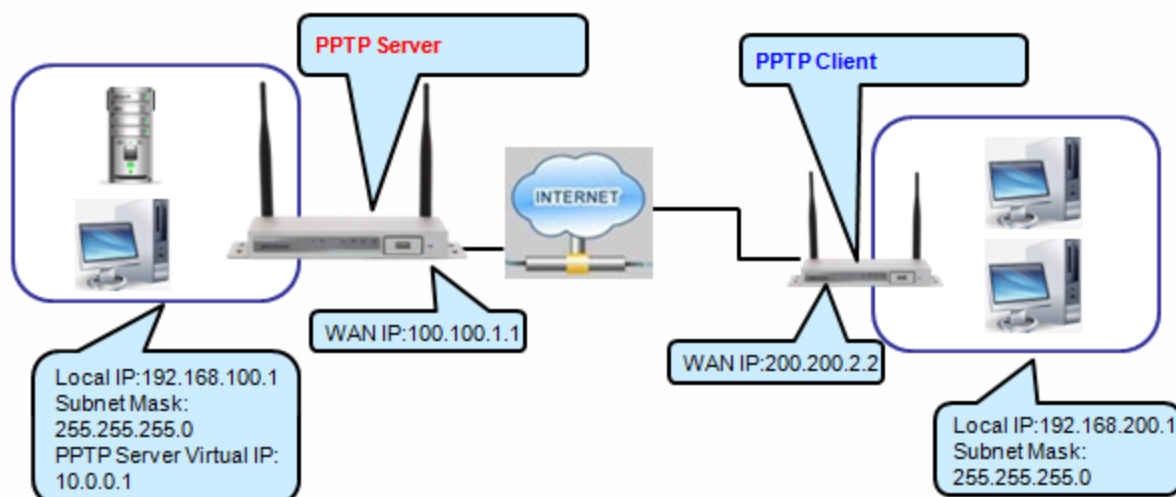
- **PPTP / L2TP Server for Remote Mobile Users**

DG-WU2005V acts as Server role for remote users to dial in and share some services in Intranet for them.



- **PPTP / L2TP Server / Client Application**

DG-WU2005V acts as Server or Client role in SMB Headquarters or Branch Office.



The Business Security Gateway can behave as a PPTP server and a PPTP client at the same time.

Configuration	
Configuration	IPSec
PPTP	L2TP
GRE	SSL VPN
Configuration	
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 PPTP VPN tunnels for the Business Security Gateway beneath the choosing screen. You can configure PPTP Client and PPTP Server one after the others.

### 3.2.3.2.1 PPTP Server Configuration

The Business Security Gateway can behave as a PPTP server, and it allows remote hosts to access LAN servers behind the PPTP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

PPTP Server Configuration	
Item	Setting
PPTP Server	<input checked="" 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 checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits

1. **PPTP Server:** Enable or disable PPTP server function.
2. **Server Virtual IP:** It is the virtual IP address of PPTP server used in PPTP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
3. **IP Pool Starting Address:** This device will assign an IP address for each remote PPTP client. This value indicates the beginning of IP pool.
4. **IP Pool Ending Address:** This device will assign an IP address for each remote PPTP client. This value indicates the end of IP pool.
5. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.
6. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

### 3.2.3.2 PPTP Server Status

The user name and connection information for each connected PPTP client to the PPTP server of the Business Security Gateway will be shown in this table.

PPTP Server Status <span>Refresh</span>				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

1. **Refresh:** To refresh the PPTP Server Status each 2 seconds by clicking on the “Refresh” button.
2. **Disconnect:** To terminate the connection between PPTP server and remote dialing in PPTP clients by clicking on the “Disconnect” button.

### 3.2.3.2.3 User Account List

You can input up to 10 different user accounts for dialing in PPTP server.

User Account List <span>Add</span> <span>Delete</span>				
ID	User Name	Password	Enable	Actions

1. **Add:** You can add one new user account by clicking on the “Add” button.
2. **Delete:** Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.
3. **Edit:** You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

### 3.2.3.2.4 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.

User Account Configuration		
User Name	Password	Account
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable
<input type="button" value="Save"/>		

1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Save:** To save the user account configuration.

### 3.2.3.2.5 PPTP Client

The Business Security Gateway also can behave as a PPTP client except PPTP server, and PPTP client tries to establish a PPTP tunnel to remote PPTP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the PPTP server.

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

1. **PPTP Client:** Enable or disable PPTP client function.

### 3.2.3.2.6 PPTP Client List & Status

You can add new up to 22 different PPTP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existing tunnel.

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

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

### 3.2.3.2.7 PPTP Client Configuration

PPTP Client Configuration	
Item	Setting
PPTP Client Name	PPTP #1
Interface	WAN 1
Operation Mode	Always on
Remote IP/FQDN	
User Name	
Password	
Default Gateway/Remote Subnet	Remote Subnet
Authentication Protocol	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable
NAT before Tunneling	<input checked="" type="checkbox"/> Enable
LCP Echo Type	Auto
	Interval 30 seconds Max. Failure Time 6 times
Tunnel	<input checked="" type="checkbox"/> Enable

- PPTP Client Name:** The name of this tunnel.
- Operation Mode:** Default is “Always on” and other options depend on product models.
- Peer IP/Domain:** The IP address or Domain name of remote PPTP server.
- User Name:** The user name which can be validated by remote PPTP server.
- Password:** The password which can be validated by remote PPTP server.
- Default Gateway/Remote Subnet:** You can choose “Default Gateway” option or “Remote Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this PPTP tunnel if these packets don’t match the Remote Subnet of other PPTP tunnels. There is only one PPTP tunnel to own the “Default Gateway” property. However, when “Remote Subnet” is chosen, peer subnet parameter need to be filled and it should be the LAN subnet of remote PPTP server. If an Intranet packet wants to go to this remote subnet, the PPTP tunnel will be established automatically.
- Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote PPTP server.
- MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
- NAT before Tunneling:** Check the “Enable” box to let hosts in the Intranet of Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option cannot be enabled.
- LCP Echo Type:** Choose the way to do connection keep alive. By default, it is “Auto” option that means system will automatically decide the time interval between two LCP

echo requests and the times that system can retry once system LCP echo fails. You also can choose “User-defined” option to define the time interval and the retry times by yourself. The last option is “Disable”.

11. **Tunnel:** Check the “Enable” box to activate the tunnel.

### 3.2.3.3 L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The Business Security Gateway can behave as a L2TP server and a L2TP client at the same time.

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

1. **L2TP:** Check the “Enable” box to activate L2TP client and server functions.
2. **Client/Server:** Choose Server or Client to configure corresponding role of L2TP VPN tunnels for the Business Security Gateway beneath the choosing screen. You can configure L2TP Client and L2TP Server one after the other.

#### 3.2.3.3.1 L2TP Server Configuration

The Business Security Gateway can behave as a L2TP server, and it allows remote hosts to access LAN servers behind the L2TP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

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	192.168.10.1
IP Pool Starting Address	10
IP Pool Ending Address	100
Authentication Protocol	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
MPPE Encryption	<input type="checkbox"/> Enable 40 bits
Service Port	1701

1. **L2TP Server:** Enable or disable L2TP server function.
2. **L2TP over IPSec:** L2TP over IPSec VPNs allow you to transport data over the Internet, while it is still maintaining a high level of security to protect data. Enter a Pre-shared key that system will use it in IPSec tunneling. When you use some devices, like Apple related mobile devices, you should also know that key to establish L2TP over IPSec tunnels.
3. **Server Virtual IP:** It is the virtual IP address of L2TP server used in L2TP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
4. **IP Pool Starting Address:** This device will assign an IP address for each remote L2TP client. This value indicates the beginning of IP pool.
5. **IP Pool Ending Address:** This device will assign an IP address for each remote L2TP client. This value indicates the end of IP pool.
6. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.
7. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

### 3.2.3.3.2 L2TP Server Status

The user name and connection information for each connected L2TP client to the L2TP server of the Business Security Gateway will be shown in this table.

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

1. **Refresh:** To refresh the L2TP Server Status each 2 seconds by clicking on the “Refresh” button.
2. **Disconnect:** To terminate the connection between L2TP server and remote dialing in L2TP clients by clicking on the “Disconnect” button.

### 3.2.3.3.3 User Account List

You can input up to 10 different user accounts for dialing in L2TP server.

User Account List <span>Add</span> <span>Delete</span>				
ID	User Name	Password	Enable	Actions

User Account Configuration		
User Name	Password	Account
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable
<span>Save</span>		

1. **Add:** You can add one new user account by clicking on the “Add” button.
2. **Delete:** Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.
3. **Edit:** You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

### 3.2.3.3.4 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.

User Account List													
ID	User Name	Password	Enable	Actions									
<div> <div>User Account Configuration</div> <table border="1"> <thead> <tr> <th>User Name</th> <th>Password</th> <th>Account</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td colspan="3"> <div>Save</div> </td> </tr> </tbody> </table> </div>					User Name	Password	Account	<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable	<div>Save</div>		
User Name	Password	Account											
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable											
<div>Save</div>													

1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Save:** To save the user account configuration.

### 3.2.3.3.5 L2TP Client

The Business Security Gateway also can behave as a L2TP client except L2TP server, and L2TP client tries to establish a L2TP tunnel to remote L2TP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the L2TP server.

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

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



### 3.2.3.3.6 L2TP Client List & Status

You can add new up to 22 different L2TP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existing tunnel.

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

L2TP Client List & Status								
<div> Add Delete Refresh </div>								
ID	L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status	Enable	Actions
<div>Save</div>								

- Add:** You can add one new L2TP client tunnel by clicking on the “Add” button.
- Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
- Tunnel:** Check the “Enable” box to activate the tunnel.
- Edit:** You can edit one L2TP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

### 3.2.3.3.7 L2TP Client Configuration

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

- L2TP Client Name:** The name of this tunnel.
- Interface:** Select the WAN interface.
- Operation Mode:** Default is “Always on” and other options depend on product models.

4. **User Name:** The user name which can be validated by remote L2TP server.
5. **Password:** The password which can be validated by remote L2TP server.
6. **Default Gateway/Remote Subnet:** You can choose “Default Gateway” option or “Remote Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this L2TP tunnel if these packets don’t match the remote Subnet of other L2TP tunnels. There is only one L2TP tunnel to own the “Default Gateway” property. However, when “Remote Subnet” is chosen, peer subnet parameter need to be filled and it should be the LAN subnet of remote L2TP server. If an Intranet packet wants to go to this peer subnet, the L2TP tunnel will be established automatically.
7. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote L2TP server.
8. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
9. **NAT before Tunneling:** Check the “Enable” box to let hosts in the Intranet of Business Security Gateway go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option cannot be enabled.
10. **LCP Echo Type:** Choose the way to do connection keep alive. By default, it is “Auto” option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose “User-defined” option to define the time interval and the retry times by yourself. The last option is “Disable”.
11. **Tunnel:** Check the “Enable” box to activate the tunnel.

### 3.2.3.4 GRE

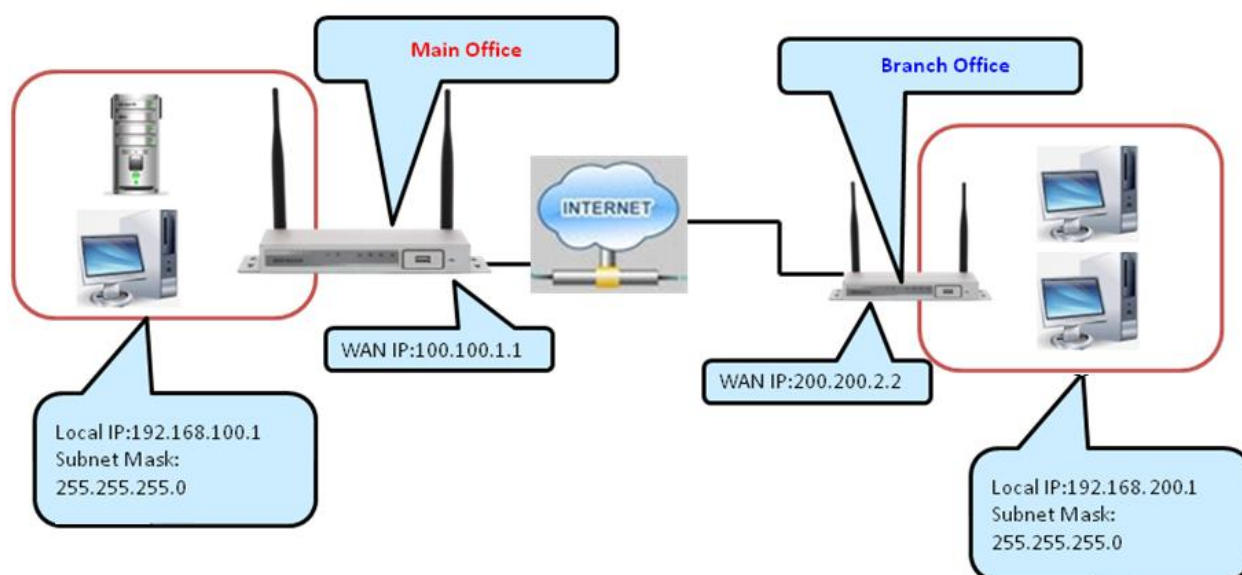
Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol inter network.

#### 3.2.3.4.1 GRE VPN Tunnel Scenario

There is one common GRE VPN connection scenario as follows:

- GRE Server / Client Application

The Business Security Gateway acts as GRE Server or Client role in SMB Headquarters or Branch Office.



#### 3.2.3.4.2 GRE Configuration

Configuration	
Configuration	[ Help ]
Item	Setting
GRE Tunnel	<input checked="" type="checkbox"/> Enable

1. **GRE Tunnel:** Check the “Enable” box to activate the GRE tunnel function

### 3.2.3.4.3 GRE Tunnel Definition

GRE Tunnel List <span>Add</span> <span>Delete</span>											
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Keep-alive	Default Gateway/Remote Subnet	Enable	Actions

1. **Add:** You can add one new GRE tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

### 3.2.3.4.4 GRE rule Configuration

GRE Rule Configuration <span>[ Help ]</span>	
Item	Setting
▶ Tunnel Name	GRE #1
▶ Interface	WAN 1
▶ Operation Mode	Always on
▶ Tunnel IP	
▶ Remote IP	
▶ Key	
▶ TTL	
▶ Keep-alive	<input checked="" 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 WAN interface.
3. **Operation Mode:** Select the operation modes Always ON, failover and load balance.
4. **Tunnel IP:** The gateway IP address of Business Security Gateway.
5. **Remote IP:** Enter the IP address of remote peer 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 router and still can't reach the destination, then this packet will be dropped.
8. **Default Gateway/Remote Subnet:** You can choose “Default Gateway” option or “remote Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this GRE tunnel if these packets don't match the remote Subnet of other GRE tunnels. There is only one GRE tunnel to own the “Default Gateway” property. However, when “Remote Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote GRE

server. If an Intranet packet wants to go to this peer subnet, the GRE tunnel will be established automatically.

### 3.2.3.4.5 SSL VPN

Wizard

Status

Basic Network

Advanced Network

Firewall

QoS & BWM

VPN

Redundancy

System Management

Certificate

Applications

System

Configuration

IPSec

PPTP

L2TP

GRE

SSL VPN

Configuration

Item	Setting
SSL VPN	<input checked="" type="checkbox"/> Enable
Server/Client for Cisco	Server

SSL VPN Server Network Extender List

ID	Service	Idle TO	Clean Cache	Full Tunnel	Server Virtual IP	Client IP Pool	DNS Servers	WINS Servers	Extended Subnets	Enable	Action
WAN-1	TCP 443	3600 Sec	<input type="checkbox"/>	<input type="checkbox"/>	10.8.0.1	10.8.0.10~10.8.0.20	/	/	Disable	<input type="checkbox"/>	<a href="#">Edit</a>
WAN-2	TCP 443	3600 Sec	<input type="checkbox"/>	<input type="checkbox"/>	10.8.0.1	10.8.0.10~10.8.0.20	/	/	Disable	<input type="checkbox"/>	<a href="#">Edit</a>
WAN-3	TCP 443	3600 Sec	<input type="checkbox"/>	<input type="checkbox"/>	10.8.0.1	10.8.0.10~10.8.0.20	/	/	Disable	<input type="checkbox"/>	<a href="#">Edit</a>

SSL VPN Server Extended Subnet List

[Add](#) [Delete](#)

ID	Extended Subnet Name	Subnet IP Address	Subnet Mask	Enable	Actions
1	123	192.168.123.0	255.255.255.0	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Select</a>

SSL VPN Server Web-based Application List

[Add](#) [Delete](#)

ID	Application Name	Service Type	Server IP Address	Server Port	Enable	Actions
----	------------------	--------------	-------------------	-------------	--------	---------

SSL VPN Server User Account List

[Add](#) [Delete](#)

ID	User Name/Group Name	User Type	Enable	Actions
----	----------------------	-----------	--------	---------

SSL VPN Server Portal Screen Configuration

Item	Setting
Portal Logo Upload	<a href="#">Choose File</a> No file chosen <a href="#">Upload</a> <a href="#">Cancel</a>
Welcome String	<input type="text"/>

SSL VPN Server Extended Subnet List

[Add](#) [Delete](#)

ID	Extended Subnet Name	Subnet IP Address	Subnet Mask	Enable	Actions
1	123	192.168.123.0	255.255.255.0	<input checked="" type="checkbox"/>	<a href="#">Edit</a> <a href="#">Select</a>

SSL VPN Server Extended Subnet Configuration

Extended Subnet Name	Subnet IP Address	Subnet Mask	Subnet
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Enable

[Save](#)

SSL VPN Server Web-based Application Configuration

[ Help ]

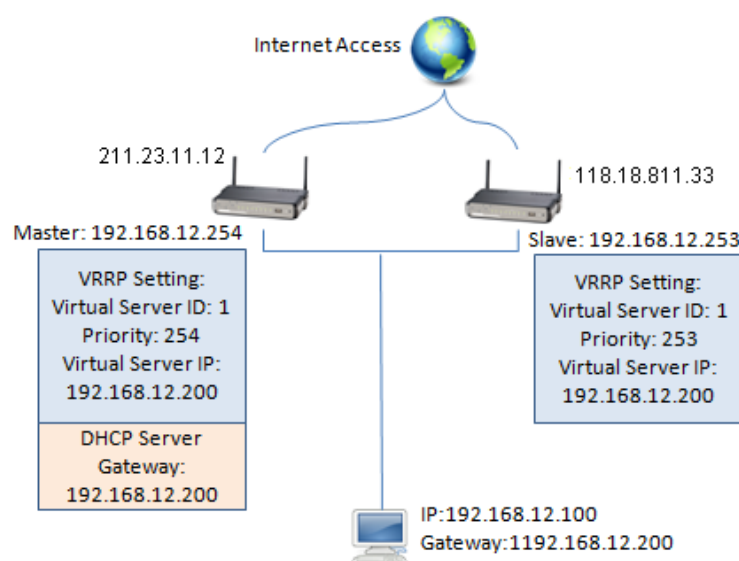
Item	Setting
Application Name	<input type="text"/>
Service Type	RDP <input type="checkbox"/> Screen Size: Full screen <input type="checkbox"/>
Server IP Address	<input type="text"/>
Server Port	3389
Application	<input type="checkbox"/> Enable

SSL VPN Server User Account List				
ID	User Name/Group Name	User Type	Enable	Actions
<div> <div>SSL VPN Server User Account Configuration</div> <div> <div>User Name/Group Name</div> <div>User Type</div> <div>User</div> </div> <div> <div> <div>▼</div> <div></div> </div> <div> <div>SSL Super User</div> <div>▼</div> </div> <div> <div><input type="checkbox"/></div> <div>Enable</div> </div> </div> <div>Save</div> </div>				

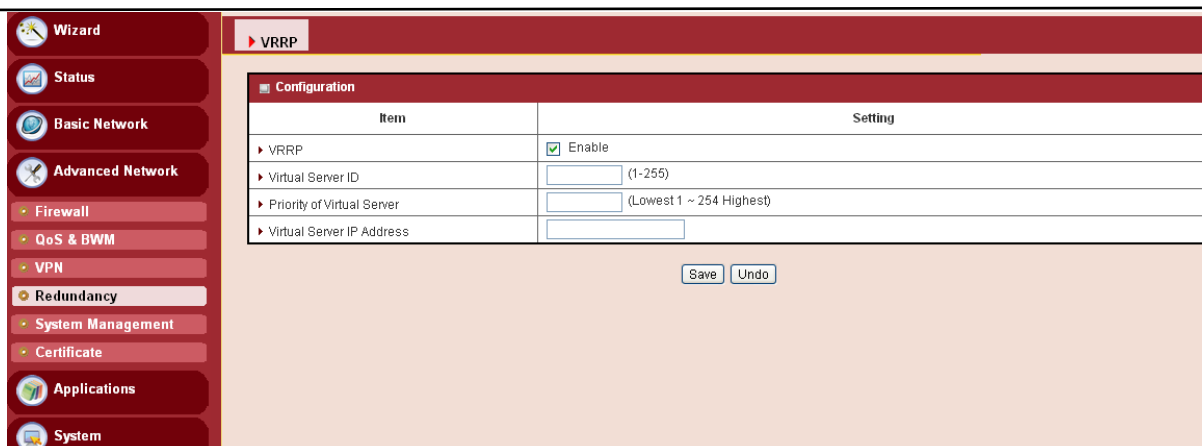
## 3.2.4 Redundancy

### 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.



Item	Setting
▶ VRRP	<input checked="" type="checkbox"/> Enable
▶ Virtual Server ID	<input type="text"/> (1-255)
▶ Priority of Virtual Server	<input type="text"/> (Lowest 1 ~ 254 Highest)
▶ Virtual Server IP Address	<input type="text"/>

1. **VRRP:** Enable or disable the VRRP function.
2. **Virtual Server ID:** Means Group ID. Specify the ID number of the virtual server. Its value ranges from 1 to 255.
3. **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are from 1 to 254, and a larger value has higher priority.
4. **Virtual Server IP Address:** Specify the IP address of the virtual server.

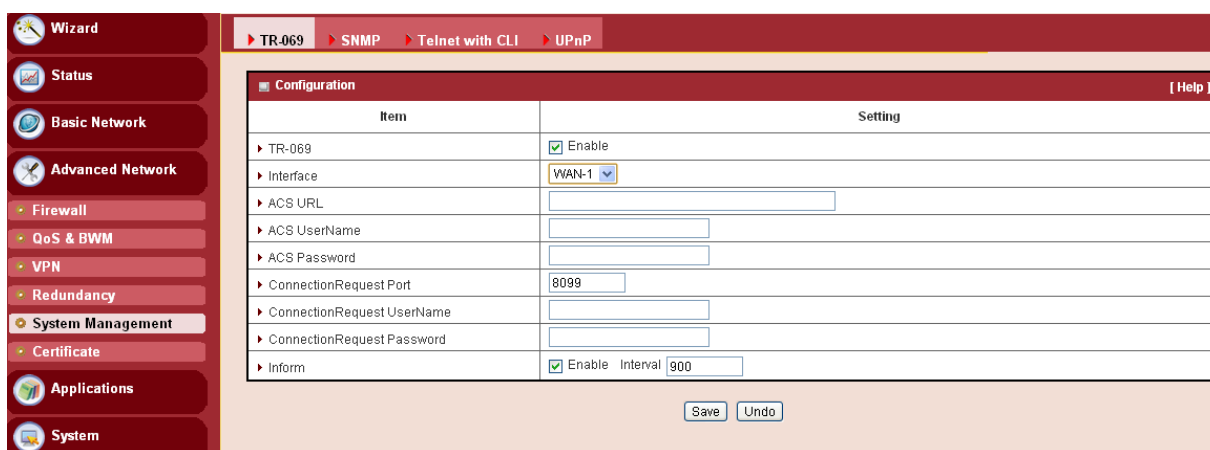
Click on “Save” to store what you just select or “Undo” to give up.

## 3.2.5 System Management

This device supports many system management protocols, such as TR-069, SNMP, Telnet with CLI and UPnP. You can finish those configurations in this sub-section.

### 3.2.5.1 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.



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

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. At the right upper corner of TR-069 Setting screen, one “[Help]” command you will see the same message about that.

### 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.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.



SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other meta data (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow:

- Supported MIBs
- MIB-II (RFC 1213, Include IPv6)
- IF-MIB, IP-MIB, TCP-MIB, UDP-MIB
- SMIV1 and SMIV2
- SNMPv2-TM and SNMPv2-MIB

TR-069
SNMP
Telnet with CLI
UPnP

Configuration
[ Help ]

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

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"/>	<a href="#">Edit</a>
2			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<a href="#">Edit</a>
3			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<a href="#">Edit</a>
4			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<a href="#">Edit</a>
5			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	<a href="#">Edit</a>

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 be request from WAN.
2. **Supported Version:** Supports SNMP V1 and V2c.
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

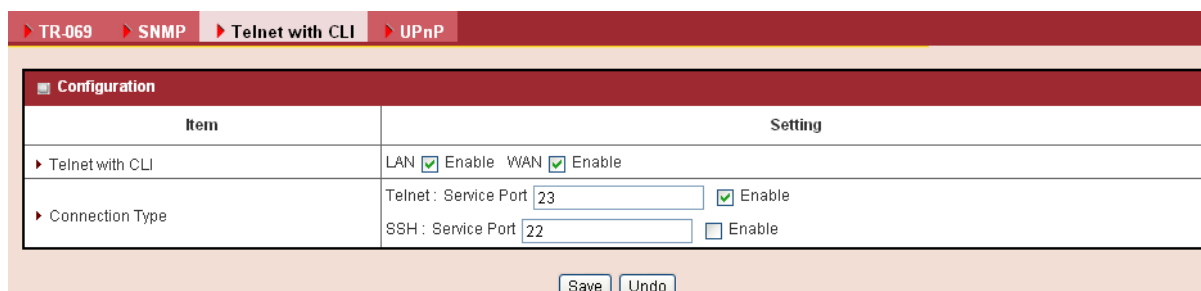
Management PCs. You have to specify it, so that the device can send SNMP Trap message to the management PCs consequently.

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.

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

### 3.2.5.3 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, console user interface, and character user interface (CUI), is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH CLI with default service port 2300 and 22, respectively. And it also accepts commands from both LAN and WAN sides.

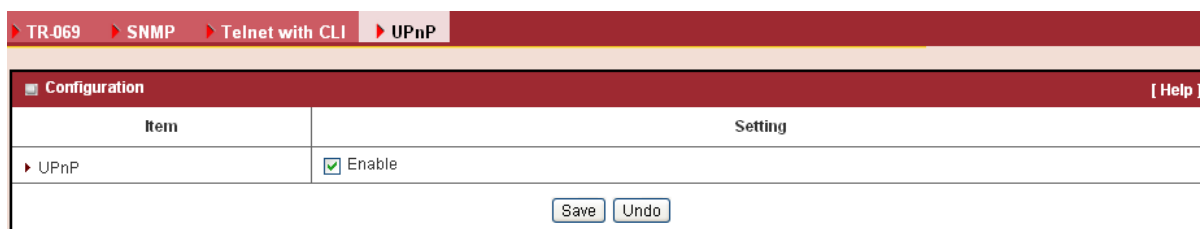


Item	Setting
Telnet with CLI	LAN <input checked="" type="checkbox"/> Enable WAN <input checked="" type="checkbox"/> Enable
Connection Type	Telnet: Service Port <input type="text" value="23"/> <input checked="" type="checkbox"/> Enable SSH: Service Port <input type="text" value="22"/> <input type="checkbox"/>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

Save 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.



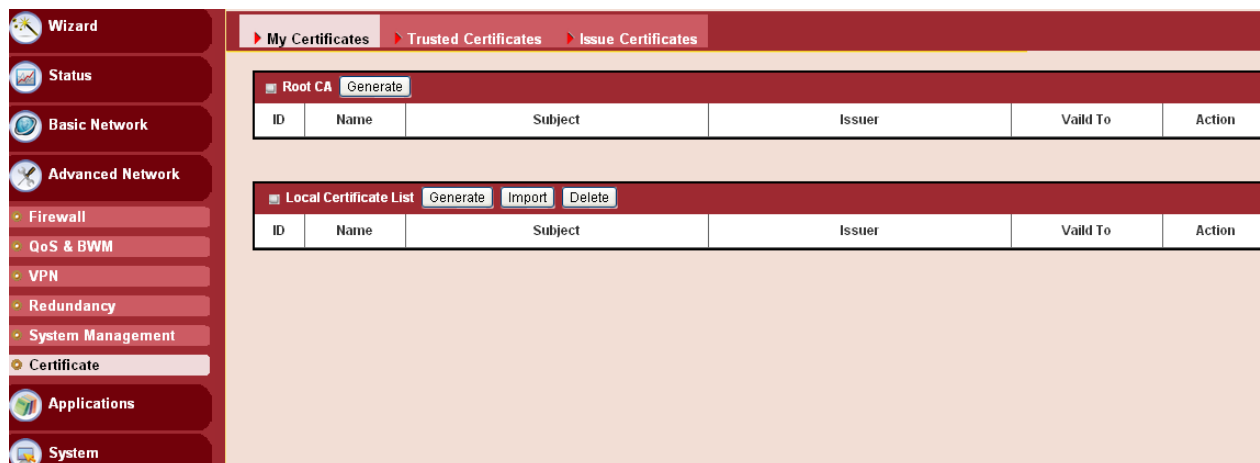
Item	Setting
UPnP	<input checked="" type="checkbox"/> Enable

Save Undo

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

### 3.2.6 Certificate

The screen shots below are My certificates, trusted certificate and the Issue certificates tabs.



ID	Name	Subject	Issuer	Valid To	Action
----	------	---------	--------	----------	--------

Generate Import Delete

My Certificates
Trusted Certificates
Issue Certificates

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"/>

Save
Back

My Certificates
Trusted Certificates
Issue Certificates

Trusted CA Certificate List

ID	Name	Subject	Issuer	Vaild To	Action

Trusted Client Certificate List

ID	Name	Subject	Issuer	Vaild To	Action

My Certificates
Trusted Certificates
Issue Certificates

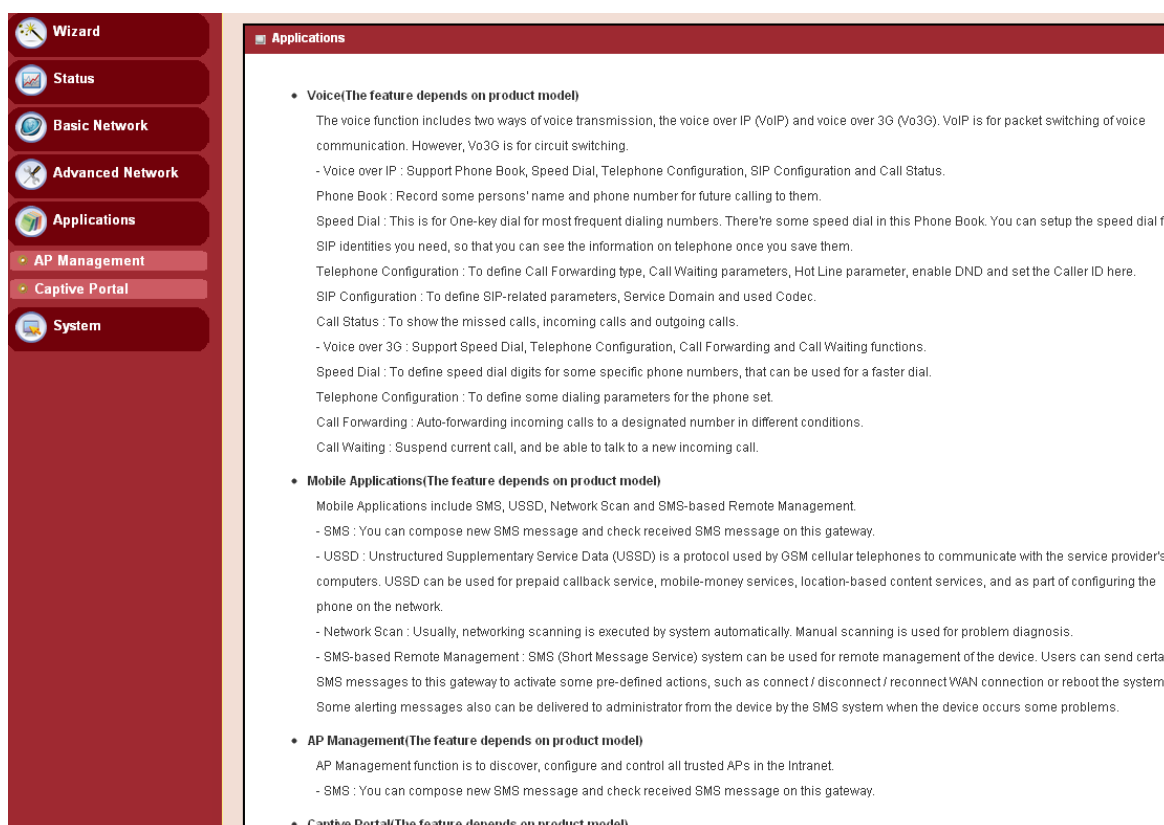
Certificate Signing Request (CSR) Import from a File

No file chosen

Certificate Signing Request (CSR) Import from a PEM

## 3.3 Applications

In this section you can finish the AP Management and Captive Portal settings. This device supports AP Management function to discover, configure and control all trusted APs in the Intranet. Besides, it also serves as an Internet access gateway. Any client host in the Intranet wants to surf the Internet, the device will redirect the Internet surfing request to an internal or external captive portal Web server for user authentication. If the authentication is successful, the requested client host will be allowed to access Internet by the device.



The screenshot shows the DIGISOL web interface. On the left is a sidebar menu with the following items: Wizard, Status, Basic Network, Advanced Network, Applications (highlighted), AP Management, Captive Portal, and System. The main content area is titled 'Applications' and contains the following information:

- Voice(The feature depends on product model)**  
 The voice function includes two ways of voice transmission, the voice over IP (VoIP) and voice over 3G (Vo3G). VoIP is for packet switching of voice communication. However, Vo3G is for circuit switching.  
 - Voice over IP : Support Phone Book, Speed Dial, Telephone Configuration, SIP Configuration and Call Status.  
 Phone Book : Record some persons' name and phone number for future calling to them.  
 Speed Dial : This is for One-key dial for most frequent dialing numbers. There're some speed dial in this Phone Book. You can setup the speed dial for SIP identities you need, so that you can see the information on telephone once you save them.  
 Telephone Configuration : To define Call Forwarding type, Call Waiting parameters, Hot Line parameter, enable DND and set the Caller ID here.  
 SIP Configuration : To define SIP-related parameters, Service Domain and used Codec.  
 Call Status : To show the missed calls, incoming calls and outgoing calls.  
 - Voice over 3G : Support Speed Dial, Telephone Configuration, Call Forwarding and Call Waiting functions.  
 Speed Dial : To define speed dial digits for some specific phone numbers, that can be used for a faster dial.  
 Telephone Configuration : To define some dialing parameters for the phone set.  
 Call Forwarding : Auto-forwarding incoming calls to a designated number in different conditions.  
 Call Waiting : Suspend current call, and be able to talk to a new incoming call.
- Mobile Applications(The feature depends on product model)**  
 Mobile Applications include SMS, USSD, Network Scan and SMS-based Remote Management.  
 - SMS : You can compose new SMS message and check received SMS message on this gateway.  
 - USSD : Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for prepaid callback service, mobile-money services, location-based content services, and as part of configuring the phone on the network.  
 - Network Scan : Usually, networking scanning is executed by system automatically. Manual scanning is used for problem diagnosis.  
 - SMS-based Remote Management : SMS (Short Message Service) system can be used for remote management of the device. Users can send certain SMS messages to this gateway to activate some pre-defined actions, such as connect / disconnect / reconnect WAN connection or reboot the system. Some alerting messages also can be delivered to administrator from the device by the SMS system when the device occurs some problems.
- AP Management(The feature depends on product model)**  
 AP Management function is to discover, configure and control all trusted APs in the Intranet.  
 - SMS : You can compose new SMS message and check received SMS message on this gateway.
- Captive Portal(The feature depends on product model)**

## 3.3.1 AP Management

### 3.3.1.1 Configuration

The following tabs will appear in the configuration tab.

Configuration
AP List
AP Configuration

AP Management Configuration

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

AP Configuration Proposal List
Add
Delete

ID	Ap Name	Actions
1	DIGISOL_DUAL_BAND_AP_Template	Edit <input type="checkbox"/> Select Apply to APs
2	DIGISOL_Single_BAND_AP_Template	Edit <input type="checkbox"/> Select Apply to APs

Save
Refresh

#### 3.3.1.1.1 AP Management Configuration

Configuration
AP List
AP Configuration

AP Management Configuration

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

- AP Management:** Check the Enable box if you want to enable this function.

#### 3.3.1.1.2 AP Configuration Proposal List

It is a list of AP Proposals, APC and APW proposal templates in default. You can add one new proposal by clicking on the “**Add**” command button. But also you can modify some existing proposals by clicking corresponding “**Edit**” command buttons at the end of proposal records in the list. Besides, unnecessary proposals can be removed by checking the “**Select**” box for those proposals and then clicking on the “**Delete**” command button at the list caption.

Configuration
AP List
AP Configuration

Proposal

Item	Setting
Proposal Name	<input type="text"/>
Proposal Template	-- select --

1. **Apply to APs:** Click on the button and you can select some trusted APs to apply the dedicated AP Configuration Proposal for their configuration settings.

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

### 3.3.1.2 AP List

#### 3.3.1.2.1 Trusted AP List & Status

The gateway will discover and show some information of trusted APs in the list. You can select one AP to click “Allow”, “Deny”, “Edit”, “Event” and “Apply” button to configure the selected AP. But also you can use “Batch FW Upgrade”, “Batch Reset” and “Batch Reboot” to set one or more existing trusted APs in the list. The AP list and their status is updated every 30 seconds.

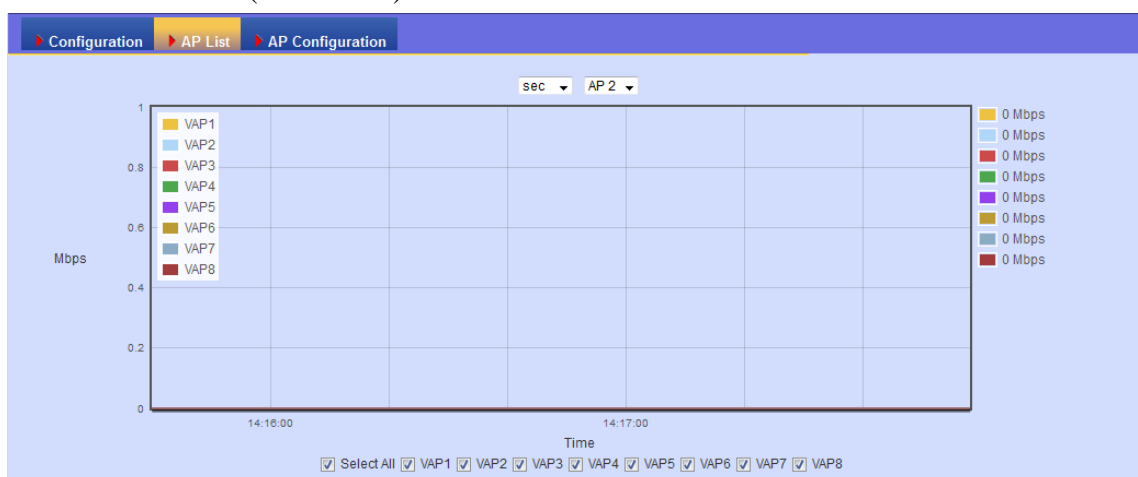
ConfigurationAP ListAP Configuration

Trusted AP List & Status

DiscoverBatch FW UpgradeBatch ResetBatch RebootUndo

ID	Name	IP	MAC	SSID	Status	Traffic	VID	Ch#	STAs	CPU ...	Actions
Refresh											

1. **Discover:** Click this button to find new deployed APs. In fact, the gateway will list new deployed APs automatically.
2. **Batch FW Upgrade:** Administrator can upgrade one or more Trusted APs.
3. **Batch Reset:** Administrator selects one or more Trusted APs and then click on the “Batch Reset” button to reset the selected APs to factory settings.
4. **Batch Reboot:** Administrator selects one or more Trusted APs and then click on the “Batch Reboot” button to reboot the selected AP devices.
5. **Statistics:** Please click “Statistics” button and you can see the network traffic graph by AP Device or VAP(Virtual AP)



6. **Allow:** It means stations which are connected to corresponded AP can access Intranet Network.
7. **Deny:** It means stations which are connected to corresponded AP can't access Intranet Network.
8. **Edit:** Click "Edit" to configure the trusted AP.
9. **Event:** You can view some important logs from the trusted AP by clicking on the "Event" Button.

Event Log		
Trap Level	Time	Trap Event
3	2014/6/24 14:17:18	2.4G Channel Change, now using Channel:2

### 3.3.1.3 AP Configuration

#### 3.3.1.3.1 AP Configuration

Administrator can configure related settings and execute some actions on the dedicated trusted AP, like WiFi configuration, System-related configuration and some executions by system tools.

Configuration
AP List
AP Configuration

Proposal

Item	Setting
Proposal Name	
Operation Function	System <div> -- select -- wifi 2.4G wifi 5G System </div>

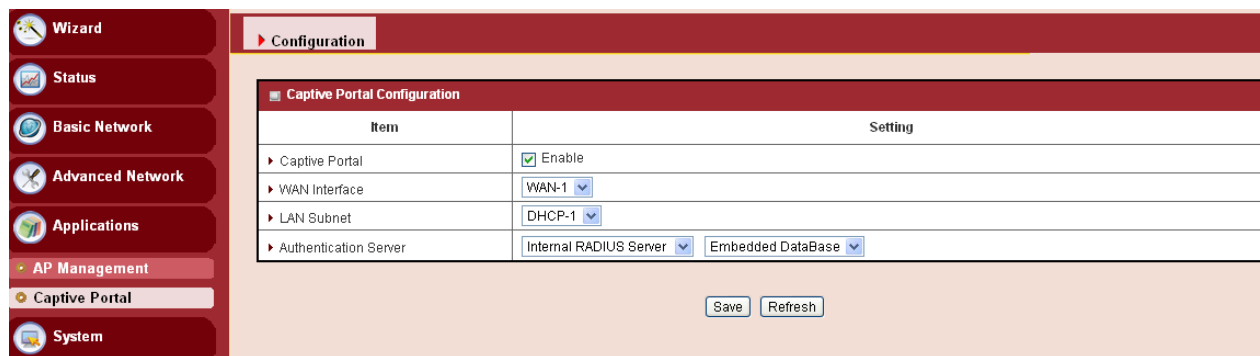
System

Item	Setting
AP Name	
Backup/Restore Settings	Dir Backup
FW Upgrade	Choose File No file chosen Upload Undo
Reboot	Now



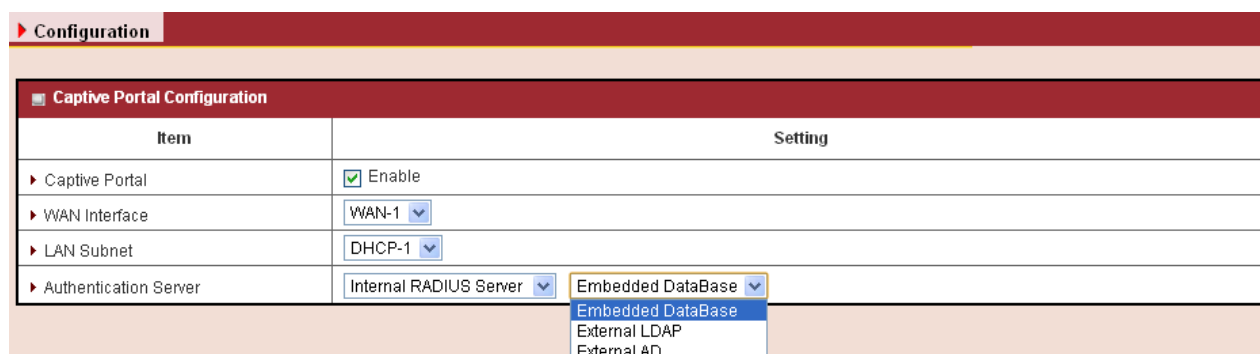
## 3.3.2 Captive Portal

### 3.3.2.1 Captive Portal Configuration



Item	Setting
▶ Captive Portal	<input checked="" type="checkbox"/> Enable
▶ WAN Interface	WAN-1
▶ LAN Subnet	DHCP-1
▶ Authentication Server	Internal RADIUS Server

Save Refresh



Item	Setting
▶ Captive Portal	<input checked="" type="checkbox"/> Enable
▶ WAN Interface	WAN-1
▶ LAN Subnet	DHCP-1
▶ Authentication Server	Internal RADIUS Server

Embedded DataBase  
Embedded DataBase  
External LDAP  
External AD

The gateway supports the Captive Portal function, including internal captive portal and external captive portal. For external captive portable, you must specify external RADIUS (Remote Authentication Dial In User Service) server and external UAM (Universal Access Method) server. In contrast, for internal captive portal, you will only select “**Internal RADIUS Server**” option for user authentication. The user account database can be an embedded database, an external AD database or an external LDAP database. Besides, the UAM server is not necessary for this case and the captive portal Web site is also embedded in the device.

### External Captive Portal

Before enabling external Captive Portal function, please go to **System >> External Servers** to define some external server objects, like RADIUS server and UAM server. Then configure Captive Portal function in this page to specific WAN Interface, select external Authentication Server and UAM Server from the pre-defined external server object list.

---

## ***Internal Captive Portal***

Before enabling internal Captive Portal function, please go to **System >> External Servers** to define some external server objects, like LDAP server or AD server if necessary. Then configure Captive Portal function in this page to specific WAN Interface, select “**Internal RADIUS Server**” option for user authentication and specify its user database to be the embedded one, an external LDAP server or an external AD server from the pre-defined external server object list.

**NOTE: All Internet Packets will forward to Captive Portal Web site of the gateway when enabled this feature. Please make sure that you had one account and password.**

## **3.4 System**

In the System section you can check system related information and execute some system operations, define some time schedule rules, execute user management, make object grouping, define external server objects and configure the operation parameters on Web UI surfing.

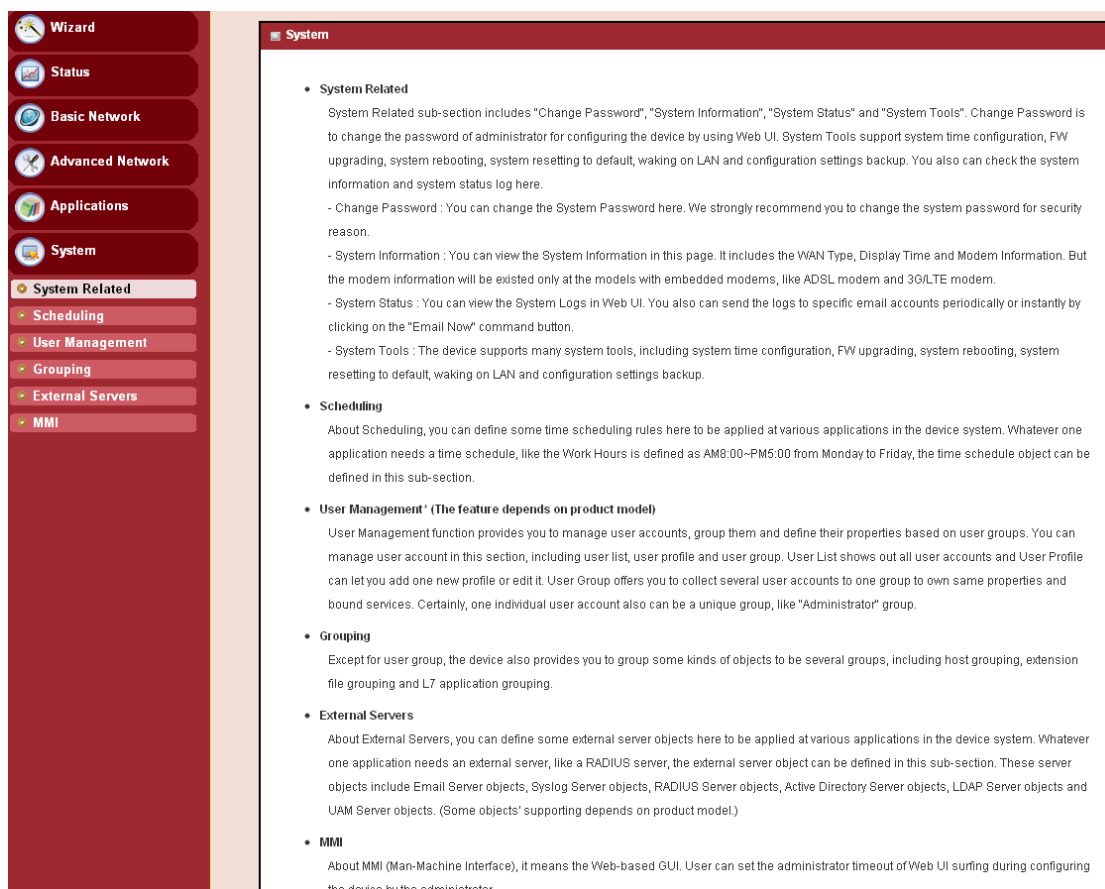
About system related, you can see system related information and system logs, use system tools for system update and do some network tests. Besides, you can also define some time scheduling rules here to be applied at various applications in the device system. Administrator Time-out in seconds defines the idle time-out for administrator to configure the device by using Web UI.

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 function provides you to manage user accounts, group them and define their properties based on user groups. 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.

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.

About MMI (Man-Machine Interface), it means the Web-based GUI. User can set the administrator timeout of Web UI surfing while configuring the device by the administrator.



**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**

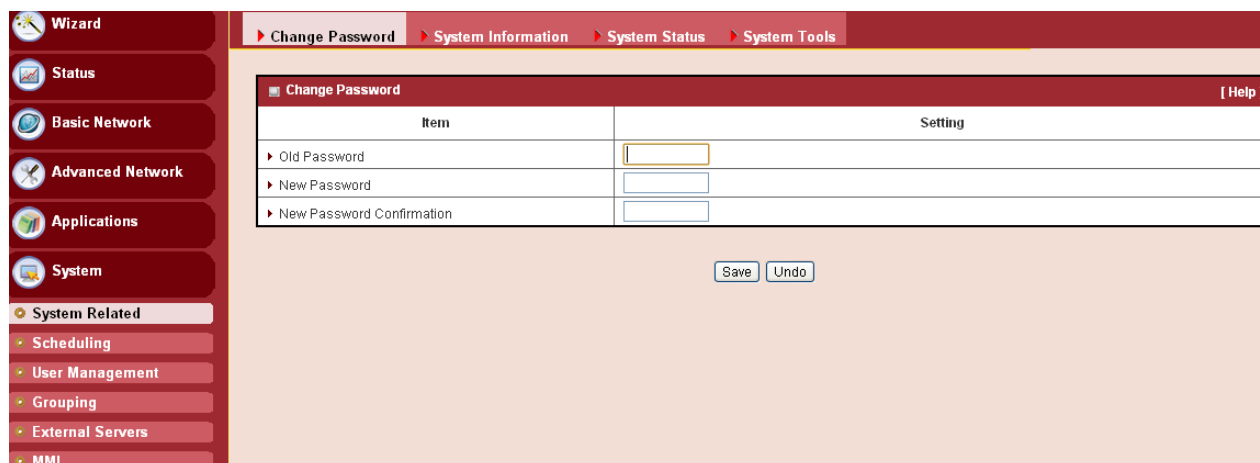
Except for user group, the device also provides you to group some kinds of objects to be several groups, including host grouping, extension file grouping and L7 application grouping.
- External Servers**

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 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.)
- MMI**

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.

### 3.4.1 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 configurations, FW upgrade, system rebooting, system resetting to default, wake on LAN and configuration settings backup. You also can check the system information and system status log here.

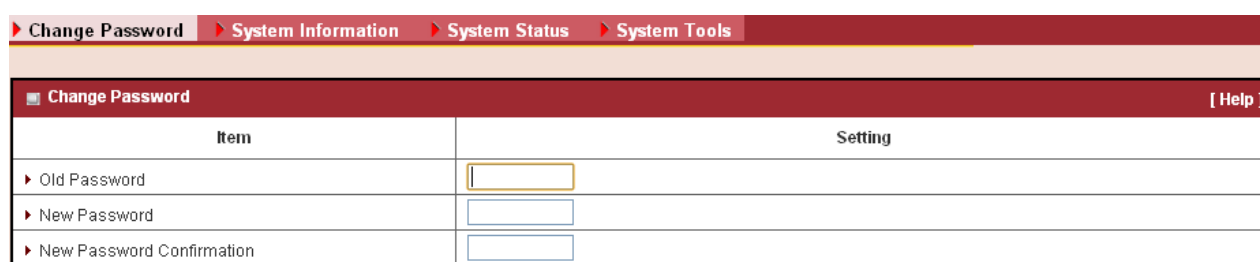


Item	Setting
Old Password	<input type="password"/>
New Password	<input type="password"/>
New Password Confirmation	<input type="password"/>

Save Undo

#### 3.4.1.1 Change Password

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



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

- Old Password:** Input the old password of administrator.
- New Password:** Input the new password of administrator for future logging in. Certainly, once the password is changed successfully, system will ask you to login again with new password.
- New Password Confirmation:** Re-type new password again here. It must be the same as the one in “New Password”; otherwise, an error message will be shown out.

### 3.4.1.2 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 existing only at the models with embedded modems, like ADSL modem and 3G/LTE modem.

Change Password System Information System Status System Tools	
System Information	
Item	Setting
WAN Type	L2TP
Display Time	Tue, 01 Jan 2013 07:01:37 +0530

### 3.4.1.3 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.

- Web Log:** You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop” and “Debug” types of logs for you to select.

Change Password System Information System Status System Tools	
System Web Log View Email Now	
Item	Setting
Web Log	<input checked="" type="checkbox"/> System <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Debug Categories
Email Alert	<input checked="" type="checkbox"/> Enable Server List: --- Option --- AddObject E-mail Addresses: <input type="text"/> E-mail Subject: System Log Contents
Syslogd	<input type="checkbox"/> Enable Server List: --- Option --- AddObject

- View:** You can browse, refresh, download and clear the log messages after clicking on the “View” command button.
- Email Alert:** This device can also export system logs via sending emails to specific recipients. The items you have to setup include:
  - \* **Enable:** Check it if you want to enable Email alert (send system logs via email).
  - \* **Server List:** Input the SMTP server IP and port, which are connected with '.'. If you do not specify port number, the default value is 25.
  - \* **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient by using ';' or ',' to separate these email addresses.
  - \* **E-mail Subject:** The subject of email alert is optional.
- Email Now:** A command button to let you email out current web logs right now instead of the email alert period.

### 3.4.1.4 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.

System Tools	
Item	Setting
System Time	<input type="button" value="Configure"/> <input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Friday July 31, 2015 11:14:03)"/>
Firmware Upgrade	<input type="button" value="Via Web UI"/> <input type="button" value="Firmware 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"/>

- System Time:** There are three approaches to setup the system time. Before the process, some basic information must be filled by clicking on the “**Configure**” command button. Basic information includes following items :

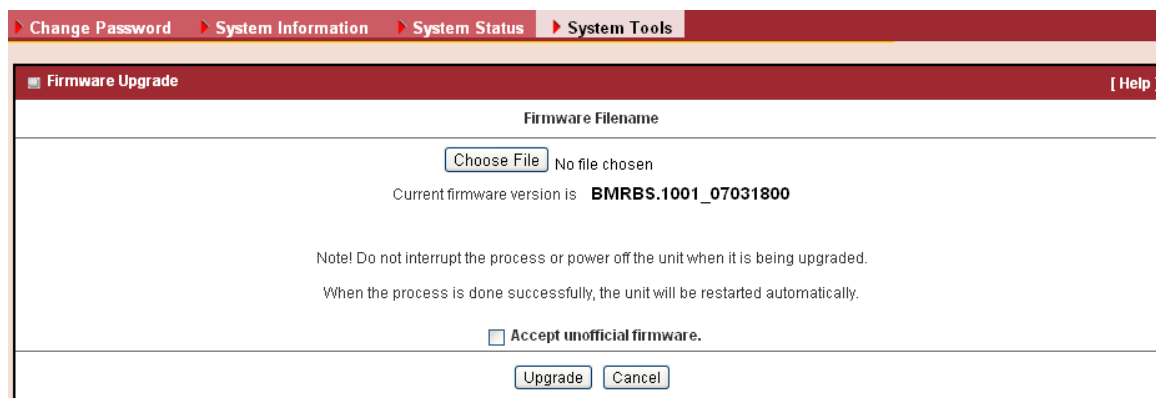
System Time Configuration	
Item	Setting
Time Zone	<input type="button" value="(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi"/>
Auto-synchronization	<input checked="" type="checkbox"/> Enable Time Server: <input type="text"/> Available Time Servers (RFC-868): <input type="button" value="Auto"/>
Daylight Saving Time	<input type="checkbox"/> Enable
Set Date & Time Manually	<input type="button" value="2015"/> / <input type="button" value="July"/> / <input type="button" value="31"/> (Year/Month/Day) <input type="button" value="11"/> : <input type="button" value="15"/> : <input type="button" value="35"/> (Hour:Minute:Second)

- Time Zone:** Select a time zone where this device is located.
- Auto-Synchronization:** Check the “**Enable**” Check box to enable this function. Besides, you can select a NTP time server to consult UTC time from the available list and by default, it is 132.163.4.102.
- Daylight Saving Time:** Check the “**Enable**” Check box to enable this function.
- Set Date & Time Manually:** Set the date and time for system manually. But Auto-Synchronization must be unchecked beforehand to do it.

Above is the first way to setup system date and time. That is, it is the manual way. The second way is “**Sync with Timer Server**”. Based on your selection of time server in basic information configuration, system will communicate with time server by NTP Protocol to get system date and time after you click on the button. The last way is “**Sync with my PC**”. Click on the button to let system synchronize its date and time with that of

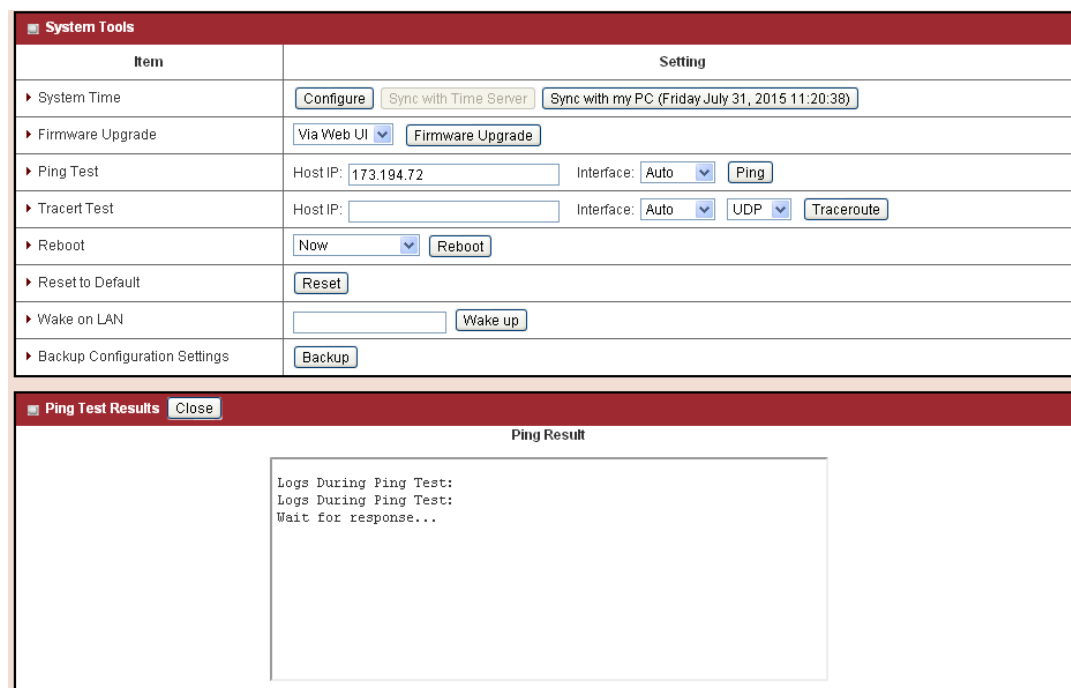
the configuration PC.

2. **FW Upgrade:** If new firmware is available, you can upgrade router firmware through the WEB GUI here. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrade process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.



**NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS IN PROGRESS.**

3. **Ping Test:** This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the “Ping” button. A test result window will appear beneath it. There is a “Close” command button that can let the test result window disappear.



#### 4. Tracert Test:

Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point. First, you need to specify an IP / FQDN, the test interface and used protocol number. Used protocol number is either “UDP” or “ICMP”, and by default, it is “UDP”. Then, system will try to trace the specified device to test whether it is alive after clicking on the “**Traceroute**” button. A test result window will appear beneath it. There is a “**Close**” command button that can let the test result windows disappear.

System Tools	
Item	Setting
System Time	<input type="button" value="Configure"/> <input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Friday July 31, 2015 11:22:07)"/>
Firmware Upgrade	<input type="button" value="Via Web UI"/> <input type="button" value="Firmware Upgrade"/>
Ping Test	Host IP: <input type="text" value="173.194.72"/> Interface: <input type="button" value="Auto"/> <input type="button" value="Ping"/>
Tracert Test	Host IP: <input type="text" value="173.194.72"/> 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"/>

Tracert Test Results <input type="button" value="Close"/>	
Traceroute Result	
<div> Logs During Tracert Test:  Interface error, traceroute fail... </div>	

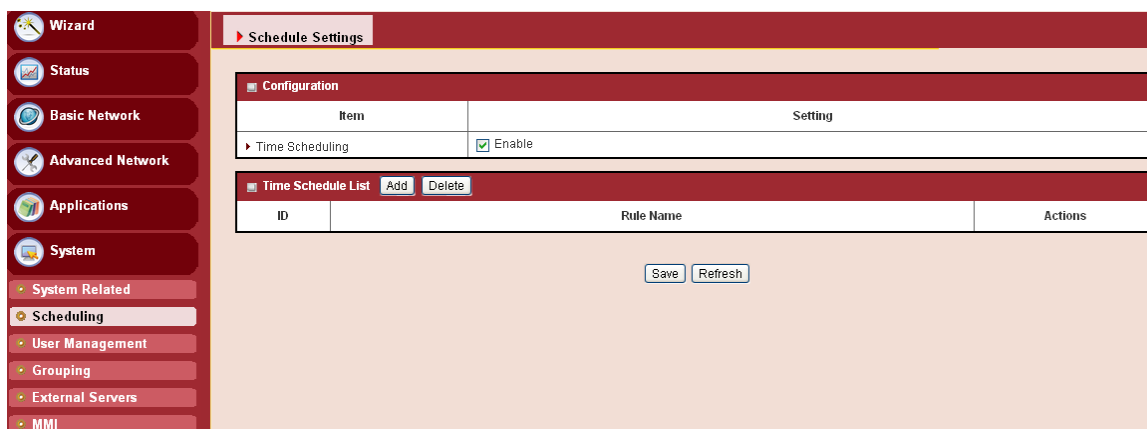
- Reboot:** You can also reboot this device by clicking the “Reboot” button.
- Reset to Default:** You can also reset this device to factory default settings by clicking the “Reset” button.
- Wake on LAN:** Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the “Wake up” command button.
- Backup Configuration Settings:** You can backup your settings by clicking the “Backup” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

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

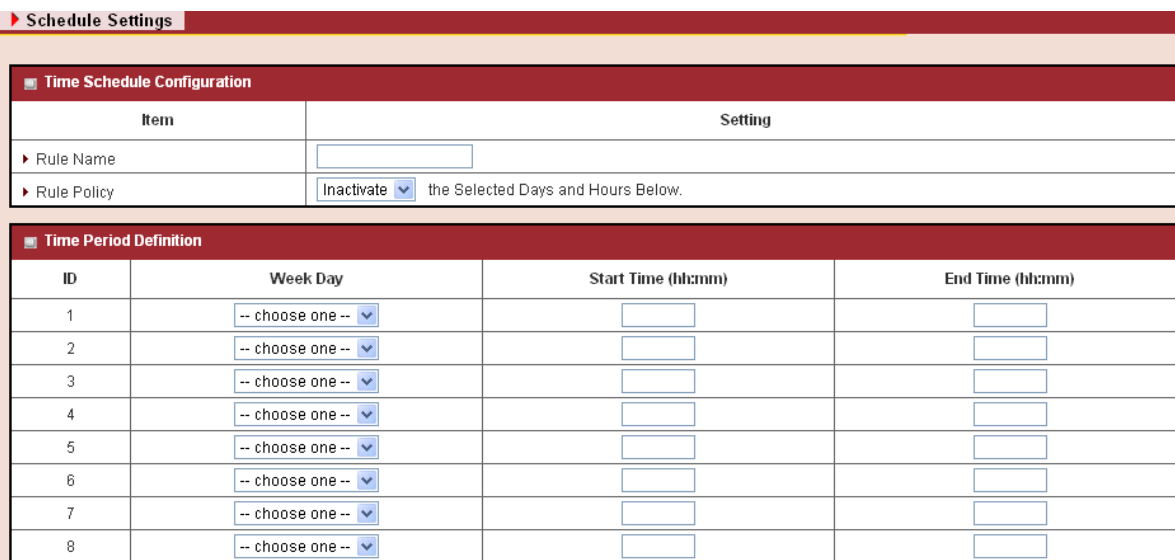


## 3.4.2 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed as below and they can be up to 100 rules.



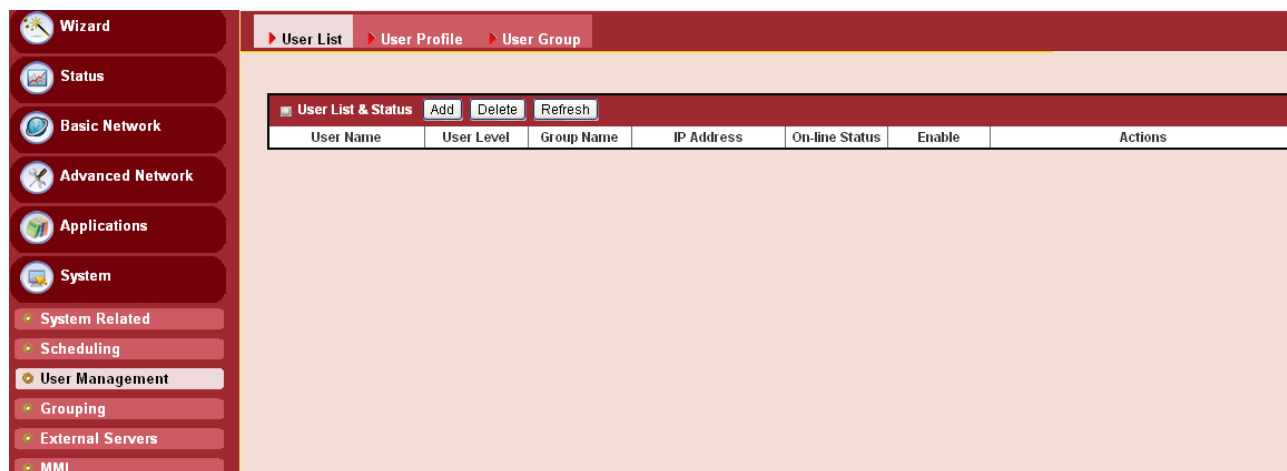
1. **Enable:** Enable or disable the scheduling function.
2. **Add New Rule:** To create a schedule rule, click the “Add New” button or the “Add New Rule” button at the bottom. When the next dialog box pops out you can edit the Name of Rule, Policy, and set the schedule time (Week day, Start Time and End Time). In a schedule rule, it collects 8 time periods to organize it. You also can specify the rule to define the enable timing (“Inactive except the selected days and hours below”) or disable timing (“Active except the selected days and hours below”).



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

### 3.4.3 User Management

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 account 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.



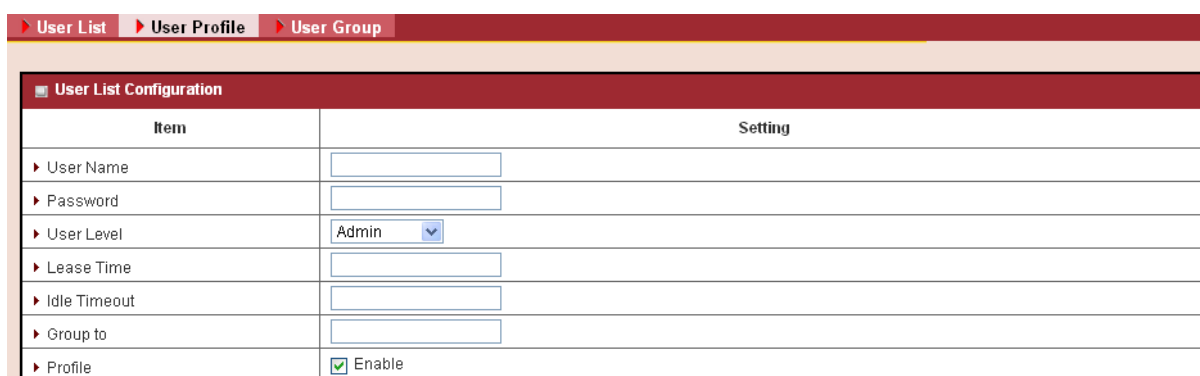
User account database is embedded in the device and accessible by the AAA server, like RADIUS, for user authentication. So, it has following feature set.

#### ■ Supports Multiple User Levels in User Management

- One user account includes following information: name, password, user level, lease time, idle timeout and the group that it belongs to.
- This device provides 4 different levels of users: Admin, Staff, Guest and Passenger.
- Remaining lease time and idle time are kept for each user account after they have logged in the gateway device successfully.
- Each individual can be one grouped by itself or join other defined groups to own common properties.
- Support the exporting and importing of user profiles.
- User groups with their own name can be bound with multiple services, like X-Auth, NAS\*, RADIUS, VPN, Accounting & Billing, SNMPv3 and CLI.
- Administrator can define the access policy and bandwidth control in a flexible way for a user object in a rule. The user object can be an individual user or a user group.

### 3.4.3.1 User List

User List can show the list of all user accounts and their status of on-line or offline in this window. You can add one new rule by clicking on the “Add” command button. But also you can modify some existing user accounts by clicking corresponding “Edit” command buttons at the end of each account record in the User List. Besides, unnecessary accounts can be removed by checking the “Select” box for those accounts and then clicking on the “Delete” command button at the User List caption. The showing of user status can be refreshed in a period that is defined by you.

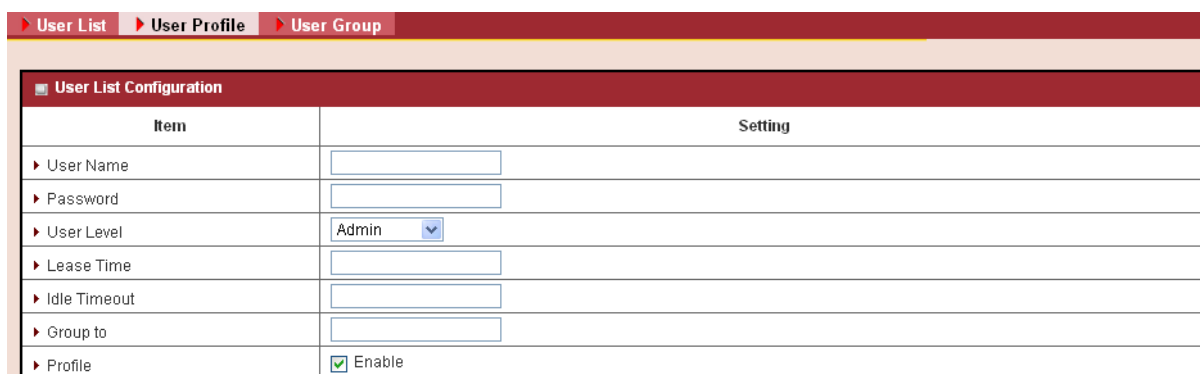


Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ User Level	Admin ▼
▶ Lease Time	<input type="text"/>
▶ Idle Timeout	<input type="text"/>
▶ Group to	<input type="text"/>
▶ Profile	<input checked="" type="checkbox"/> Enable

User List displays the user name, user level, membership group name, IP address, on-line status and activity status as shown in the above screen shot. There are some additional command buttons in the Action field of User List table.

### 3.4.3.2 User Profile

It supports the adding of one new user account or the editing of one existing user profile. There are some parameters that need to be specified in one user profile. They are User Name, Password, User Level, Lease Time, Idle Timeout, Group to and finally, the user profile enable.



Item	Setting
▶ User Name	<input type="text"/>
▶ Password	<input type="text"/>
▶ User Level	Admin ▼
▶ Lease Time	<input type="text"/>
▶ Idle Timeout	<input type="text"/>
▶ Group to	<input type="text"/>
▶ Profile	<input checked="" type="checkbox"/> Enable

- 1. User Name:** The name of user account.
- 2. Password:** The password of user account.

3. **User Level:** Supports 4 levels for you to select, including “Admin”, “Staff”, “Guest” and “Passenger”. Admin level of user account can let the user configure the device with fully control ability. Staff level of users can access both the Intranet resources and the Internet resources. Guest level of user account can use limited bandwidth to access Internet, but can’t access the Intranet. Passenger level of user account is for mobile users to use the device to access the Internet. He will use fair and average bandwidth utilization with other passengers.
4. **Lease Time:** The subscribed time for the user account to login the device.
5. **Idle Timeout:** To logout the user account if he is idle for the time longer than the Idle Timeout.
6. **Group to:** To select an existing group to let the user join. The user also can be an individual group with him only.
7. **Profile Enable:** Check it if the user profile wants to be active.

### 3.4.3.3 User Group

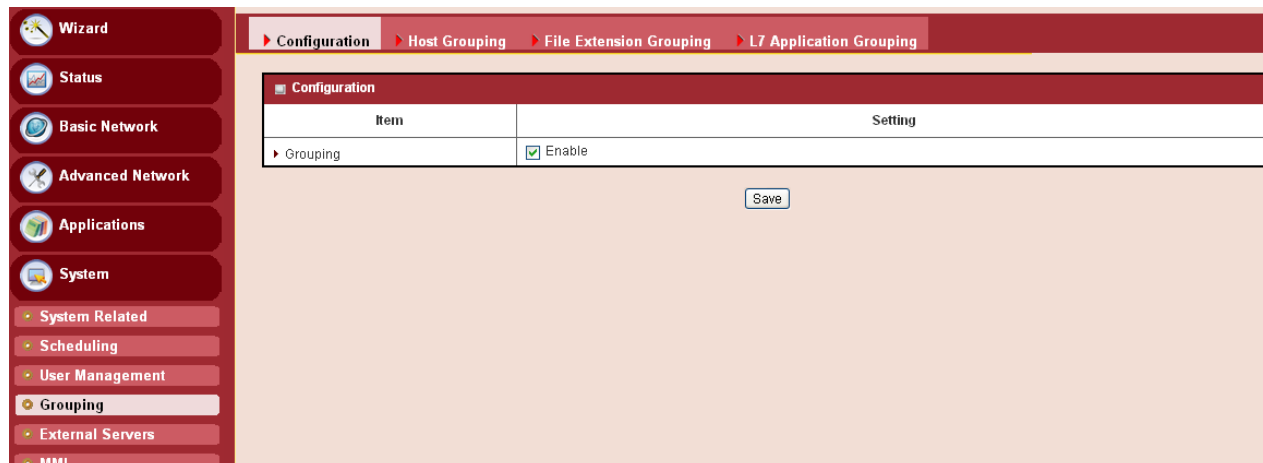
It supports the grouping of several user accounts to be one user group with common properties. There are some parameters that need to be specified in one user group. They are Group Name, Group Members, Bound Services, QoS & BWM Property, Policy Routing Property and finally, the user group enable.

User List User Profile User Group	
User Group Configuration	
Item	Setting
Group Name	<input type="text"/>
Multiple User Members	<input type="button" value="Choice"/>
Multiple Bound Services	<input type="checkbox"/> X-Auth <input type="checkbox"/> NAS <input type="checkbox"/> RADIUS <input type="checkbox"/> VPN
QoS & BWM Property	Individual Control <input type="button" value="v"/> Set MINR : <input type="text"/> MAXR : <input type="text"/> Mbps <input type="button" value="v"/>
Policy Routing Property	Routing Interface : <input type="button" value="v"/> WAN-1
Group	<input checked="" type="checkbox"/> Enable

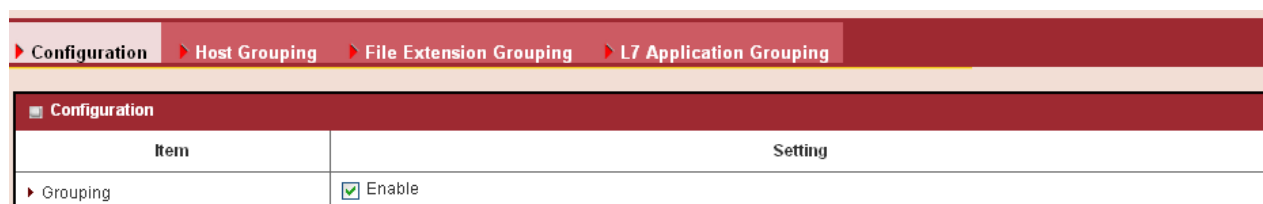
1. **Group Name:** The name of user group.
2. **Multiple User Members:** Click on the “Choice” to select multiple user accounts to join the group.
3. **Multiple Bound Services:** Supports 6 kinds of applications to be bound with the user group. So, the bound service can use the group object or all user account objects in the group.
4. **QoS & BWM Property:** Can define the guaranteed and limited bandwidth usage for the group. Either individual or group to obey and own the property.
5. **Policy Routing Property:** Can define the routing interface via that all packets from the group members.
6. **Group Enable:** Check it if the group profile wants to be active.

### 3.4.4 Grouping

This device supports three types of objects to be grouped. They are host objects, file extension objects and L7 Application objects. One “Enable” Check box provides user to activate the grouping function for all types of objects.



#### 3.4.4.1 Grouping Configuration

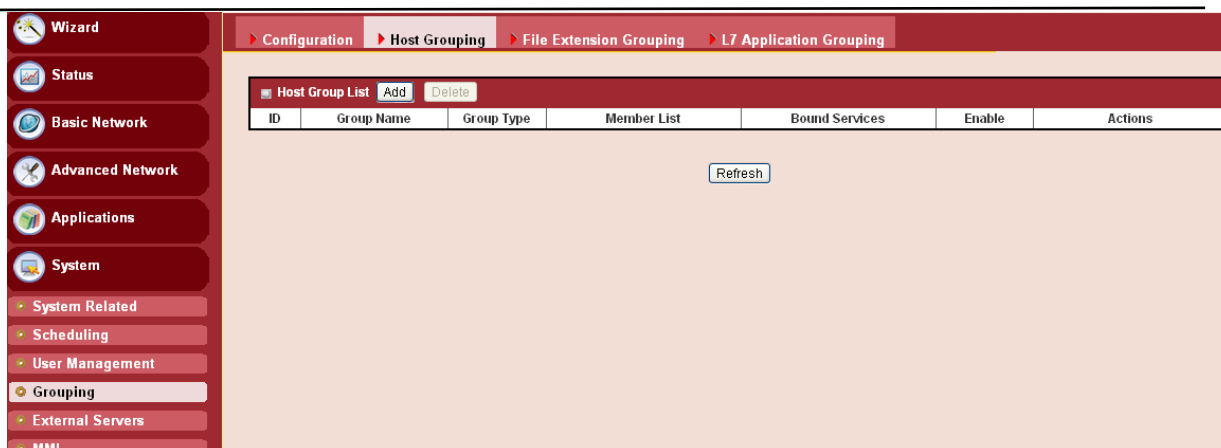


1. **Grouping:** Check the “Enable” box to activate the grouping function.

#### 3.4.4.2 Host Grouping

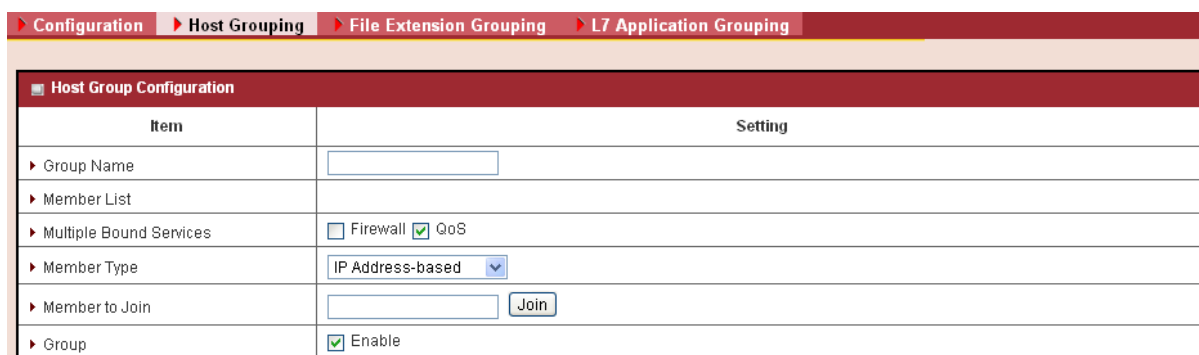
##### 3.4.4.2.1 Host Group List

Host Group List can show the list of all host groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the “Add” command button. But also you can modify some existing host groups by clicking corresponding “Edit” command buttons at the end of each group record in the Host Group List. Besides, unnecessary groups can be removed by checking the “Select” box for those groups and then clicking on the “Delete” command button at the Host Group List caption.



1. **Add:** Click on the button to add one host group.
2. **Delete:** Click on the button to delete the host groups that are specified in advance by checking on the “Select” box of those groups.
3. **Edit:** Click on the button to edit the host group.
4. **Select:** Select the host group to delete.

### 3.4.4.2.2 Host Group Configuration



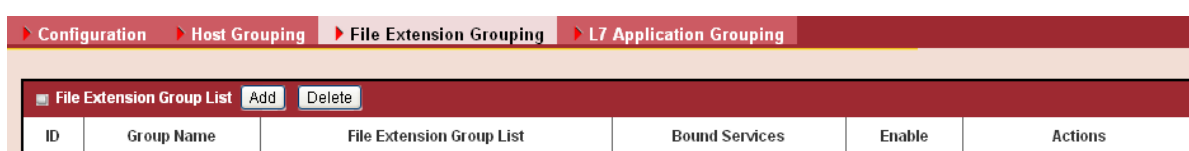
Item	Setting
Group Name	<input type="text"/>
Member List	<input type="text"/>
Multiple Bound Services	<input type="checkbox"/> Firewall <input checked="" type="checkbox"/> QoS
Member Type	IP Address-based
Member to Join	<input type="text"/> <input type="button" value="Join"/>
Group	<input checked=""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

1. **Group Name:** Define the name of group.
2. **Member List:** Shows the list of members that have joined the group. A delete button ‘⊗’ is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services:** The defined group object can be used in various applications, like Firewall or QoS & BWM.
4. **Member to Join:** To define a member by using IP address or MAC address. Choose “IP Address-based” or “MAC Address-based” first and then type specific value for the member. Click on the “Join” button to join the member in the group.
5. **Group:** Check the “Enable” box to activate the group definition.

### 3.4.4.3 File Extension Grouping

#### 3.4.4.3.1 File Extension Group List

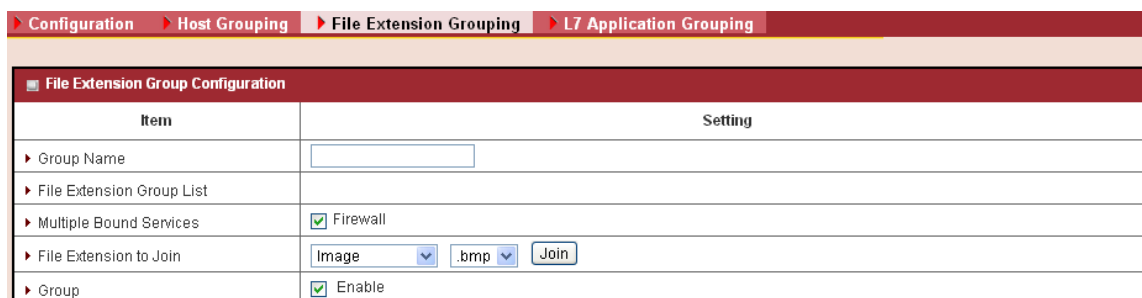
File Extension Group List can show the list of all file extension groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the “Add” command button. But also you can modify some existing file extension groups by clicking corresponding “Edit” command buttons at the end of each group record in the File Extension Group List. Besides, unnecessary groups can be removed by checking the “Select” box for those groups and then clicking on the “Delete” command button at the File Extension Group List caption.



ID	Group Name	File Extension Group List	Bound Services	Enable	Actions
----	------------	---------------------------	----------------	--------	---------

1. **Add:** Click on the button to add one file extension group.
2. **Delete:** Click on the button to delete the file extension groups that are specified in advance by checking on the “Select” box of those groups.
3. **Edit:** Click on the button to edit the file extension group.
4. **Select:** Select the file extension group to delete.

#### 3.4.4.3.2 File Extension Group Configuration



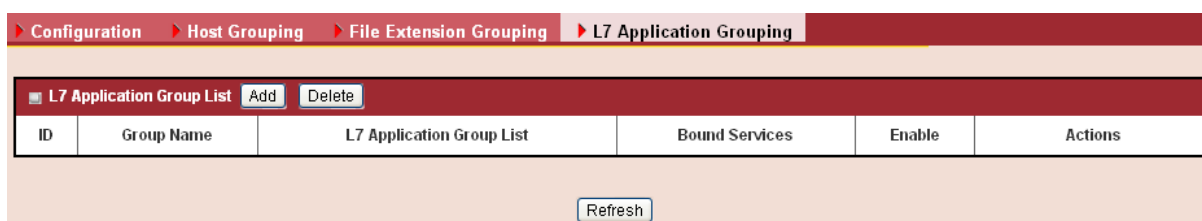
Item	Setting
Group Name	<input type="text"/>
File Extension Group List	
Multiple Bound Services	<input checked="" type="checkbox"/> Firewall
File Extension to Join	Image <input type="button" value="Join"/> .bmp <input type="button" value="Join"/>
Group	<input checked="" type="checkbox"/> Enable

1. **Group Name:** Define the name of group.
2. **Member List:** Shows the list of members that have joined the group. A delete button ⊗ is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services:** The defined group object can be used in various applications, like Firewall or QoS & BWL.
4. **Member to Join:** To define a member by selecting a file extension type category and a file extension name. File extension categories include “Image”, “Video”, “Audio”, “Java”, “Compression” and “Execution”. And each category has its own list of file extension objects, like “.exe”. Choose one to join the group by clicking on the “Join” button.
5. **Group:** Check the “Enable” box to activate the group definition.

### 3.4.4.4 L7 Application Grouping

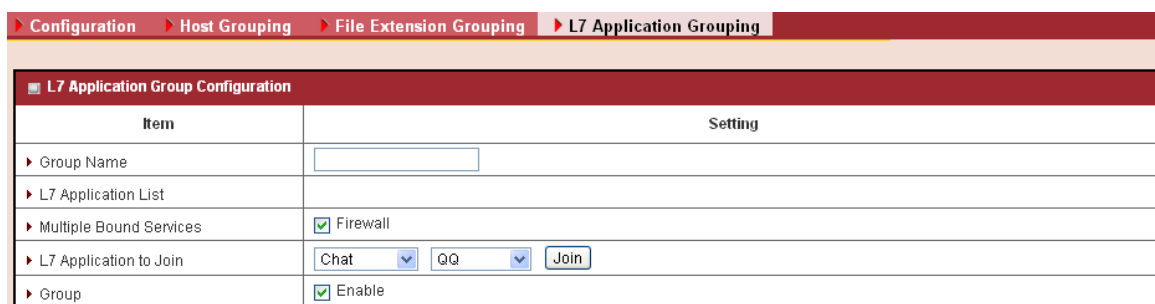
#### 3.4.4.4.1 L7 Application Group List

L7 Application Group List can show the list of all file extension groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the “Add” command button. But also you can modify some existing file extension groups by clicking corresponding “Edit” command buttons at the end of each group record in the File Extension Group List. Besides, unnecessary groups can be removed by checking the “Select” box for those groups and then clicking on the “Delete” command button at the File Extension Group List caption.



1. **Add:** Click on the button to add one L7 application group.
2. **Delete:** Click on the button to delete the L7 application groups that are specified in advance by checking on the “Select” box of those groups.
3. **Edit:** Click on the button to edit the L7 application group.
4. **Select:** Select the file extension group to delete.

#### 3.4.4.3.2 L7 Application Group Configuration



1. **Group Name:** Define the name of the group.
2. **Member List:** Shows the list of members that have joined the group. A delete button ⊗ is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services:** The defined group object can be used in various applications, like Firewall or QoS & BWM.
4. **Member to Join:** To define a member by selecting a L7 application category and an application name. L7 application categories include “Chat”, “P2P”, “Proxy” and “Streaming”. And each category has its own list of L7 application objects, like “eMule”.

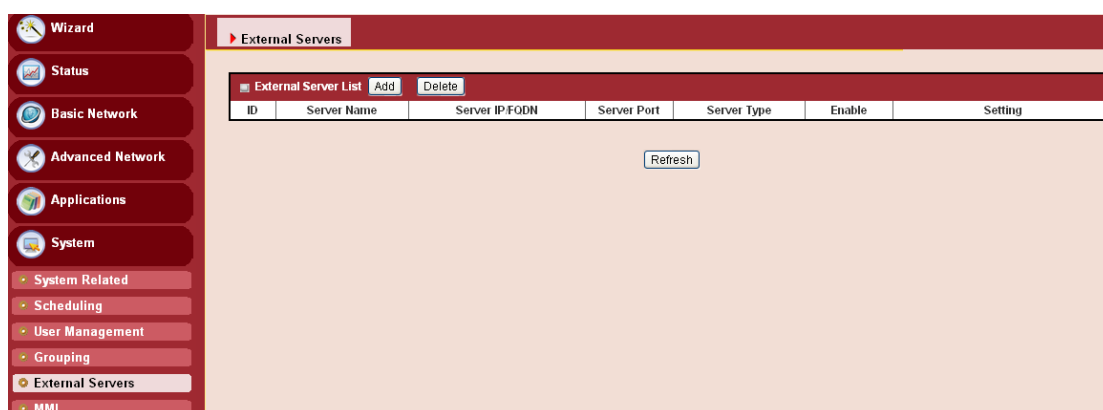


Choose one to join the group by clicking on the “Join” button.

5. **Group:** Check the “Enable” box to activate the group definition.

### 3.4.5 External Servers

This device supports six types of external server objects to be created. They are Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. These objects can be used in other applications of system, like system log emailing to email server or sending to syslog server in **System >> System Related >> System Status**, captive portable function in **Applications >> Captive Portable**, SMS forwarding to email server or syslog server in **Applications >> Mobile Applications >> SMS**, AP Management alerting system in **Applications >> AP Management**, and IO Management alerting handler in **Applications >> IO Management**. Above usage examples depend on the provided functions of different product models.



#### 3.4.5.1 External Server List

External Server List can show the list of all defined external server objects and their attributes in this window. You can add one new external server object by clicking on the “Add” command button. But also you can modify some existing external server objects by clicking corresponding “Edit” command buttons at the end of each object record in the External Server List. Besides, unnecessary objects can be removed by checking the “Select” box for those objects and then clicking on the “Delete” command button at the External Server List caption.

External Servers						
External Server List						
ID	Server Name	Server IP/FQDN	Server Port	Server Type	Enable	Setting
<div> <input type="button" value="Add"/> <input type="button" value="Delete"/> </div>						
<div> <input type="button" value="Refresh"/> </div>						

1. **Add:** Click on the button to add one external server object.
2. **Delete:** Click on the button to delete the external server objects that are specified in advance by checking on the “Select” box of those objects.
3. **Edit:** Click on the button to edit the external server object.
4. **Select:** Select the external server object to delete.

### 3.4.5.2 External Server Configuration

External Server Configuration	
Item	Setting
Server Name	<input type="text"/>
Server IP/FQDN	<input type="text"/>
Server Port	<input type="text"/>
Server Type	<div> Email Server <input type="button" value="v"/> </div> <div> User Name: <input type="text"/> </div> <div> Password: <input type="text"/> </div> <div> Primary: </div> <div> Shared Key: <input type="text"/> </div> <div> Authentication Protocol: CHAP <input type="button" value="v"/> </div> <div> Secondary: </div> <div> Shared Key: <input type="text"/> </div> <div> Authentication Protocol: CHAP <input type="button" value="v"/> </div> <div> Domain: <input type="text"/> </div> <div> Base DN: <input type="text"/> </div> <div> Identity: <input type="text"/> </div> <div> Password: <input type="text"/> </div> <div> Workgroup: <input type="text"/> </div> <div> Login URL: <input type="text"/> </div> <div> Shared Secret: <input type="text"/> </div> <div> NAS/Gateway ID: <input type="text"/> </div> <div> Location ID: <input type="text"/> </div> <div> Location Name: <input type="text"/> </div>
Server	<input type="checkbox"/> Enable
<div> <input type="button" value="Save"/> </div>	

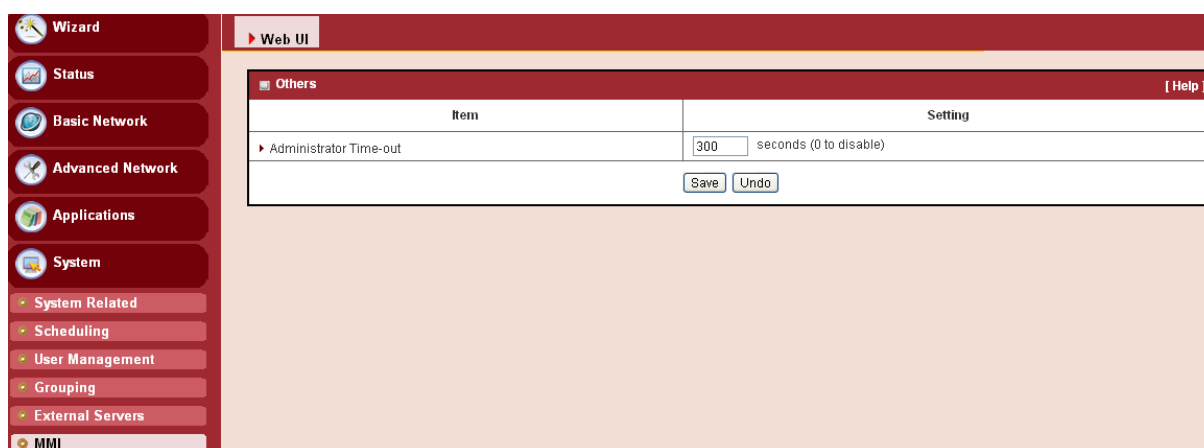
1. **Server Name:** Define the name of external server object.
2. **Server IP/FQDN:** Specify the IP address or domain name of external server.
3. **Server Port:** Specify the service port of external server.
4. **Server Type:** Select one server type from the option list of “Email Server”, “Syslog Server”, “RADIUS Server”, “Active Directory Server”, “LDAP Server” and “UAM Server”. Based on your selection, there are several parameters that need to be specified. When you select “Email Server” option for the Server Type, you must specify two more

parameters, “User Name” and “Password”. For “Syslog Server”, no more parameter is required. For “RADIUS Server”, you can specify primary RADIUS server and secondary RADIUS server for redundancy. For each server, following parameters need to be specified: Shared Key, Authentication Protocol (CHAP or PAP), Session Timeout (1~60 Mins) and Idle Timeout (1~15 Mins). For “Active Directory” Server, you must specify one more parameter, “Domain”. For “LDAP” Server, one more parameter, Base Domain Name. For “NT Domains” Server, one more parameter: “Workgroup”. For “UAM” Server, following parameters must be provided: “Login URL”, “Shared Secret”, “NAS/Gateway ID”, “Location ID” and “Location Name”. Among them, Location Name is optional.

5. **Server:** Check the “Enable” box to activate the external server object.

## 3.4.6 MMI

### 3.4.6.1 Web UI



Item	Setting
Administrator Time-out	300 seconds (0 to disable)

Save Undo

You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

## CHAPTER 4 Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the Wireless Access Controller. You can refer to the following if you are having problems.

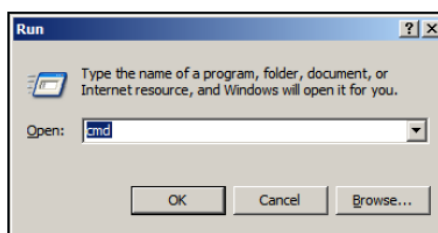
### 1 Why can't I configure the router even when the cable is plugged and the LED is lit?

Do a Ping test to make sure that the Wireless Access Controller is responding.

*Note: It is recommended that you use an Ethernet connection to configure it*

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 this wireless access controller. It will show four replies if you ping correctly.

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

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

1. Go to **Start > Right click on "My Computer" > Properties**.
2. Select the **Hardware Tab**.

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

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

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

## 3 How to reset to default?

1. Ensure that the wireless access controller 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 wireless access controller 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.smartlink.co.in](http://www.smartlink.co.in)