

## User's Manual

**MH-3400**

# *Gigabit Multi-Homing VPN Security Router*



## Copyright

Copyright© 2012 by PLANET Technology Corp. 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 PLANET.

PLANET 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 hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

## CE mark Warning

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

## Federal Communication Commission Interference Statement

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

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

## FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1)

This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

## R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## WEEE Caution



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## 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 manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## Customer Service

For information on customer service and support for the Gigabit Multi-Homing VPN Security Router, please refer to the following Website URL:

<http://www.planet.com.tw>

Before contacting customer service, please take a moment to gather the following information:

- ◆ Gigabit Multi-Homing VPN Security Router serial number and MAC address
- ◆ Any error messages that displayed when the problem occurred
- ◆ Any software running when the problem occurred
- ◆ Steps you took to resolve the problem on your own

## Revision

User's Manual for PLANET Gigabit Multi-Homing VPN Security Router

Model: MH-3400

Rev: 1.0 (January, 2012)

## Table of Contents

<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
<b>1.1 FEATURES</b> .....	<b>1</b>
<b>1.2 PACKAGE CONTENTS</b> .....	<b>2</b>
<b>1.3 PHYSICAL SPECIFICATION</b> .....	<b>2</b>
<b>1.4 SPECIFICATION</b> .....	<b>4</b>
<b>CHAPTER 2: INSTALLATION PROCEDURE</b> .....	<b>6</b>
<b>2.1 SYSTEMATIC SETTING PROCESS</b> .....	<b>6</b>
<b>2.2 SETTING FLOW CHART</b> .....	<b>7</b>
<b>CHAPTER 3: HARDWARE INSTALLATION</b> .....	<b>9</b>
<b>3.1 VPN ROUTER NETWORK CONNECTION</b> .....	<b>9</b>
<b>CHAPTER 4: LOGIN VPN SECURITY ROUTER</b> .....	<b>11</b>
<b>CHAPTER 5: SYSTEM STATUS</b> .....	<b>13</b>
<b>5.1 HOME PAGE</b> .....	<b>13</b>
<b>5.1.1 WAN Status</b> .....	<b>13</b>
<b>5.1.2 Physical Port Status</b> .....	<b>14</b>
<b>5.1.3 System Information</b> .....	<b>15</b>
<b>5.1.4 Firewall Status</b> .....	<b>15</b>
<b>5.1.5 VPN Status</b> .....	<b>16</b>
<b>5.1.6 Log Setting Status</b> .....	<b>16</b>
<b>5.2 CHANGE AND SET LOGIN PASSWORD AND TIME</b> .....	<b>16</b>
<b>5.2.1 Password Setting</b> .....	<b>16</b>
<b>5.2.2 Time</b> .....	<b>18</b>
<b>CHAPTER 6: NETWORK</b> .....	<b>20</b>
<b>6.1 NETWORK CONNECTION</b> .....	<b>20</b>
<b>6.1.1 Host Name and Domain Name</b> .....	<b>20</b>
<b>6.1.2 LAN Setting</b> .....	<b>21</b>
<b>6.1.3 WAN &amp; DMZ Settings</b> .....	<b>23</b>
<b>6.2 MULTI- WAN SETTING</b> .....	<b>36</b>
<b>6.2.1 Load Balance Mode</b> .....	<b>36</b>
<b>6.2.2 Network Detection Service</b> .....	<b>43</b>
<b>6.2.3 Protocol Binding</b> .....	<b>45</b>

<b>CHAPTER 7: PORT MANAGEMENT</b> .....	<b>54</b>
7.1 SETUP .....	54
7.2 PORT STATUS .....	55
7.3 IP/ DHCP .....	56
7.4 DHCP STATUS .....	58
7.5 IP & MAC BINDING .....	59
7.6 IP GROUPING .....	62
7.7 PORT GROUP MANAGEMENT .....	65
<b>CHAPTER 8: QOS (QUALITY OF SERVICE)</b> .....	<b>66</b>
8.1 BANDWIDTH MANAGEMENT .....	66
8.1.1 The Maximum Bandwidth provided by ISP .....	67
8.1.2 QoS .....	68
8.1.3 Smart QoS .....	71
8.1.4 Exception IP address .....	73
8.2 SESSION CONTROL .....	74
<b>CHAPTER 9 : FIREWALL</b> .....	<b>76</b>
9.1 GENERAL POLICY .....	76
9.2 ACCESS RULE .....	79
9.2.1 Default Rule .....	79
9.2.2 Add New Access Rule .....	80
9.3 URL FILTER .....	82
<b>CHAPTER 10 : VPN (VIRTUAL PRIVATE NETWORK)</b> .....	<b>86</b>
10.1. DISPLAY ALL VPN SUMMARY .....	86
10.1.1. Add a New VPN Tunnel .....	89
10.1.1.1 Gateway to Gateway Setting .....	89
10.1.1.2 Client to Gateway Setting .....	99
10.1.2. PPTP Setting .....	105
10.1.3. VPN Pass Through .....	107
11.1 DMZ HOST/ PORT RANGE FORWARDING .....	108
11.2 UPNP .....	111
11.3 ROUTING .....	112
11.3.1 Dynamic Routing .....	112
11.3.2 Static Routing .....	113
11.4 ONE TO ONE NAT .....	115
11.5 DDNS- DYNAMIC DOMAIN NAME SERVICE .....	118
11.6 MAC CLONE .....	120
<b>CHAPTER 12: SYSTEM TOOL</b> .....	<b>121</b>

---

12.1 DIAGNOSTIC.....	121
12.2 FIRMWARE UPGRADE .....	122
12.3 CONFIGURATION BACKUP .....	122
12.4 SNMP .....	123
12.5 SYSTEM RECOVER .....	124
12.6 HIGH AVAILABILITY .....	124
<b>CHAPTER 13. LOG .....</b>	<b>129</b>
13.1 SYSTEM LOG .....	129
13.2 SYSTEM STATISTIC .....	134
13.3 TRAFFIC STATISTIC.....	135
13.4 IP/ PORT STATISTIC.....	137
<b>APPENDIX A : CONFIGURE THE 3G USB INTERFACE .....</b>	<b>139</b>
<b>STEP 1: USB/3G CONNECTION SETTING .....</b>	<b>140</b>
<b>STEP 2: CHECK IP ADDRESS FOR USB/3G CONNECTION. ....</b>	<b>143</b>
<b>STEP 3: CHECK 3G INFO FROM SERVICE PROVIDER .....</b>	<b>144</b>
<b>STEP 4: CONFIGURE ADVANCE SETTING .....</b>	<b>147</b>
<b>STEP 5: SEND SYSTEM LOG VIA SMS MESSAGE.....</b>	<b>150</b>



## Chapter 1: Introduction

As Internet becomes essential for your business, the only way to prevent your Internet connection from failure is to have more than one connection. PLANET's Gigabit Multi-Homing VPN Security Router, MH-3400, reduces the risks of potential shutdown if one of the Internet connections fails. Moreover, it allows you to perform load-balancing by distributing the traffic through three or four WAN connections.

In addition to a multi-homing device, PLANET's Gigabit Multi-Homing VPN Security Router provides a complete security solution in a box. The policy-based firewall, content filtering function and VPN connectivity with 3DES and AES encryption make it a perfect product for your network security. No more complex connection and settings for integrating different security products on the network is required.

Bandwidth management function is also supported to offers network administrators an easy yet powerful means to allocate network resources based on business priorities, and to shape and control bandwidth usage.

### 1.1 Features

- ◆ **Multi-WAN Auto Backup:** The MH-3400 can monitor each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- ◆ **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including "Auto Load Balance", "Unbinding WAN Balance" and "Strategy Routing",. User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- ◆ **Inbound Load Balancing:** The MH-3400 provides the Inbound Load Balancing for enterprise's internal server. The Inbound Load Balancing can reduce the server loading and system crash risks, in order to improve the server working efficiency.
- ◆ **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including Ping of Death, SYN Flooding, Land attack, IP Spoofing, etc. The access rule function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- ◆ **VPN Connectivity:** The security gateway support PPTP and IPSec VPN. With DES, 3DES and AES encryption and SHA-1 / MD5 authentication, the network traffic over public Internet is secured.
- ◆ **Content Filtering:** The security gateway can block network connection based on URLs, Scripts (The Java Applet, cookies and Active X), Restrict Application (MSN, Yahoo Messenger, QQ, PPSTREAM and PPTV) and Download/Upload blocking.
- ◆ **Multiple DHCP Server:** The multi DHCP server support 4 sets of Class C IP address, each server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- ◆ **QoS Bandwidth Management:** Featured Smart QoS with dynamic bandwidth management to automatically control P2P and video downloading and other bandwidth hogging to avoid bandwidth insufficient. Prioritizing different person/group or applications in bandwidth using for a better reasonable management.

- ◆ **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows users to alias a dynamic IP address to a static hostname.
- ◆ **Multiple NAT:** Multiple NAT allows local port to set multi-subnet and connect to the Internet through different WAN IP addresses.
- ◆ **Port Range Forwarding (Virtual Server):** The Port Forwarding and DMZ function can let you setup your servers in the Intranet and still provide services to the Internet users.
- ◆ **Easy Management:** Embedded Mirror Port to connect with monitoring devices to monitor online behavior. It also supporting remote management by web browser with user name and password to realize router management from remote places.
- ◆ **Log Feature:** The log and traffic statistic function can helping administrators to record the change/abnormal of the whole network status and take actions according to the log information.

## 1.2 Package Contents

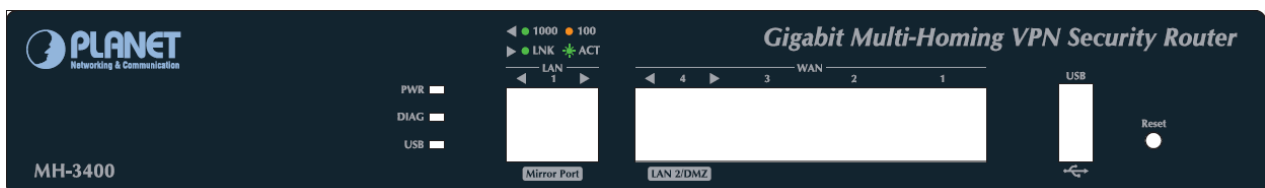
The following items should be included:

- MH-3400 x 1
- Power Cord x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Cat5 Cable x 1

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

## 1.3 Physical Specification

### Front Panel



### Rear View





## LED definition

LED	Color	Status	Description
PWR	Green	Steady	Power On
	Off	Off	Power Off
DIAG	Amber	Steady on	System is crashed.
		Blinking	System is on self-test after power on the device.
		Off	System is ready.
WAN/ DMZ: Link/Act	Green	Steady on	Port has been connected & Get IP
		Blinking	Transmit data.
		Off	Not get the IP address, even the port has been connected.
LAN: Link/Act	Green	Steady on	LAN port has been connected.
		Blinking	Transmit data.
LAN/WAN/DMZ: Speed	Green	Steady On	Works on 1000M
	Amber	Steady On	Works on 100M.
	Off	Off	Works on 10M.
USB: Link/Connect /Act	Green	Steady on	USB is connected and the device is supported.
		Blinking	Packets are transmitting through USB port
	Off	Off	Not connect with any USB device

## Button definition

Button	Description
Reset	Push 5 seconds for "Warm Start", and push 10 seconds for Factory Default.
Power	Rocker switch ,Internal 12V/1.65A

## 1.4 Specification

Product		Gigabit Multi-Homing VPN Security Router
Model		MH-3400
<b>Hardware</b>		
Ethernet	LAN	1~2 x 10/100/1000Mbps RJ-45 with LAN 1 configurable as LAN 1 / Mirror Port
	WAN	3~4 x 10/100/1000Mbps RJ-45 with WAN 4 configurable as WAN 4 / LAN2 / DMZ
	DMZ	1 x 10/100Mbps RJ-45 (WAN 4)
Button	Reset	1 x Reset button for reset to factory default setting
	Power	1 x Power on/off Switch
USB		1 x USB 2.0 Host
<b>Software</b>		
Multi-WAN Function		<ul style="list-style-type: none"> <li>● Inbound / Outbound Load Balance: by session and by IP</li> <li>● Protocol Binding</li> <li>● Network Service Detection</li> </ul>
Routing		<ul style="list-style-type: none"> <li>● Dynamic Route RIP v1/v2</li> <li>● Static Route</li> <li>● Strategic Route</li> </ul>
System Performance		<ul style="list-style-type: none"> <li>● Concurrent session :50000</li> <li>● Firewall performance :1Gbps</li> <li>● Corporation Size: SMB(clients 200~250)</li> <li>● 3DES performance:154Mbps</li> </ul>
Bandwidth Management		<ul style="list-style-type: none"> <li>● Session Limit</li> <li>● Priority QoS</li> <li>● Port-based QoS</li> <li>● QoS Schedule</li> </ul>
Firewall Security		<ul style="list-style-type: none"> <li>● NAT</li> <li>● One-to-One NAT</li> <li>● Multiple-to-One NAT</li> <li>● Stateful Packet Inspection(SPI) Firewall</li> <li>● Denial of Service (DoS) prevention</li> <li>● IP &amp; Port filtering</li> <li>● Block Website by Keyword, Content Filter</li> <li>● Firewall detection: Ping of Death, SYN Flooding, Land attack, IP Spoofing</li> <li>● Email Alert for Hacker Attack</li> <li>● IP&amp;MAC Binding</li> <li>● Support DMZ to protect your network: DMZ Host</li> <li>● Prevent ARP Attack on LAN</li> </ul>
Networking		<ul style="list-style-type: none"> <li>● Configurable DMZ</li> <li>● DHCP Server (support class C), client, dynamic IP, static IP,IP Grouping support</li> <li>● Multiple DHCP Server (support 4 sets of Class C)</li> <li>● PPPoE / Static IP/ DHCP Client</li> <li>● LAN MAC Clone</li> <li>● Multiple Subnet</li> <li>● Protocol: TCP /IP, ARP, ICMP, FTP/TFTP, IPv4</li> <li>● NAT with popular ALG support</li> <li>● Port forwarding(Virtual Server)</li> <li>● DNS Relay</li> <li>● DDNS: Support DynDNS,3322</li> <li>● Password protected configuration or management sessions for web access</li> <li>● Port Management – Speed/Duplex/Auto Negotiation/VLAN</li> <li>● Transparent Bridge</li> </ul>
USB Feature		<ul style="list-style-type: none"> <li>● 3G/3.5G Internet Access</li> <li>● 3G as WAN interface</li> <li>● Automatic failover between 3G and WAN</li> </ul>

		<ul style="list-style-type: none"> <li>● Load balancing between 3G and WAN</li> <li>● Auto/ manual throughput and time calculation mechanism for cost or dial-on demand (Cellular cost Control)</li> <li>● Signal strength display on front panel</li> <li>● Throughput measurement</li> <li>● APN and PIN code Support</li> </ul>
	Network Management	<ul style="list-style-type: none"> <li>● Comprehensive web based management and policy setting</li> <li>● SNMP v1/v2c</li> <li>● Monitoring, Logging, and Alarms of system activities</li> <li>● Firmware upgrade through Web browser</li> </ul>
VPN Support	VPN tunnel	<ul style="list-style-type: none"> <li>● Supports max 200 IPSec VPN Tunnels</li> <li>● Supports max 60 PPTP VPN Tunnels</li> </ul>
	IPSec VPN	<ul style="list-style-type: none"> <li>● IPSec H/W acceleration</li> <li>● Up to 2 Group VPNs support</li> <li>● Friendly VPN Tunnel Management</li> <li>● IKE: Pre-Shared keys</li> <li>● IPSec Encryption DES/3DES/AES128/AES192/AES256</li> <li>● IPSec Authentication MD5/SHA1</li> <li>● Support PMTU</li> <li>● NAT Traversal</li> <li>● Connect on Demand</li> <li>● DPD detection</li> <li>● VPN Hub</li> <li>● IP by DNS Resolved</li> <li>● View Log</li> <li>● IPSec, PPTP Pass through</li> </ul>
	PPTP VPN	<ul style="list-style-type: none"> <li>● PPTP Dial-in VPN 60 users</li> </ul>

## Chapter 2: Installation Procedure

In this chapter we are going to introduce hardware installation. Through the understanding of multi-WAN setting process, users can easily setup and manage the network, making VPN Router functioning and having best performance.

### 2.1 Systematic Setting Process

Users can set up and enable the network by utilizing bandwidth efficiently. The network can achieve the ideal efficientness, block attacks, and prevent security risks at the same time. Through the process settings, users can install and operate VPN Router easily. This simplifies the management and maintenance, making the user network settings be done at one time. The main process is as below:

**Step 1. Hardware installation**

**Step 2. Login**

**Step 3. Verify device specification and set up password and time**

**Step 4. Set WAN connection**

**Step 5. Set LAN connection: physical port and IP address settings**

**Step 6. Set QoS bandwidth management: avoid bandwidth occupation**

**Step 7. Set Firewall: prevent attack and improper access to network resources**

**Step 8. Other settings: UPnP, DDNS, MAC Clone**

**Step 9. Management and maintenance settings: Syslog, SNMP, and configuration backup**

**Step 10. VPN (Virtual Private Network)function setting**

**Step 11. Logout**

## 2.2 Setting Flow Chart

Below is the description for each setting process, and the correspondent contents and purposes.

#	Setting	Content	Purpose
1	Hardware installation	user's demand.	Install VPN Router hardware based on user physical requirements.
2	Login	Login the device with Web Browser.	Login VPN Router web-based UI.
3	Verify device specification	Verify Firmware version and working status.	Verify VPN Router specification, Firmware version and working status.
	Set password and time	Set time and re-new password.	Modify the login password considering safe issue. Synchronize the VPN Router time with WAN.
4	Set WAN connection	Verify WAN connection setting, bandwidth allocation, and protocol binding.	Connect to WAN. Configure bandwidth to optimize data transmission.
5	Set LAN connection: physical port and IP address settings	Set mirror port and VLAN. Allocate and manage LAN IP.	Provide mirror port, port management and VLAN setting functions. Support Static/DHCP IP allocation to meet different needs. IP group will simplify the management work.
6	Set QoS bandwidth management: avoid bandwidth occupation	Restrict bandwidth and session of WAN ports, LAN IP and application.	To assure transmission of important information, manage and allocate the bandwidth further to achieve best efficiency.
7	Set Firewall: prevent attack and improper access to network resources	Block attack, Set Access rule and restrict Web access.	Administrators can block BT to avoid bandwidth occupation, and enable access rules to restrict employee accessing internet improperly or using MSN, QQ and Skype during working time. They can also protect network from Worm or ARP attacking.
8	Advanced Settings:DMZ/Forwarding, UPnP, DDNS, MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone
9	Management and maintenance settings: Syslog, SNMP, and configuration backup	Monitor VPN Router working status and configuration backup.	Administrators can look up system log and monitor system status and inbound/outbound flow in real time.
10	VPN Virtual Private	Configure VPN tunnels,	Configure different types of VPN to meet

---

	Network function setting	e.g. PPTP.	different application environment.
11	Logout	Close configuration window.	Logout VPN Router web-based UI.

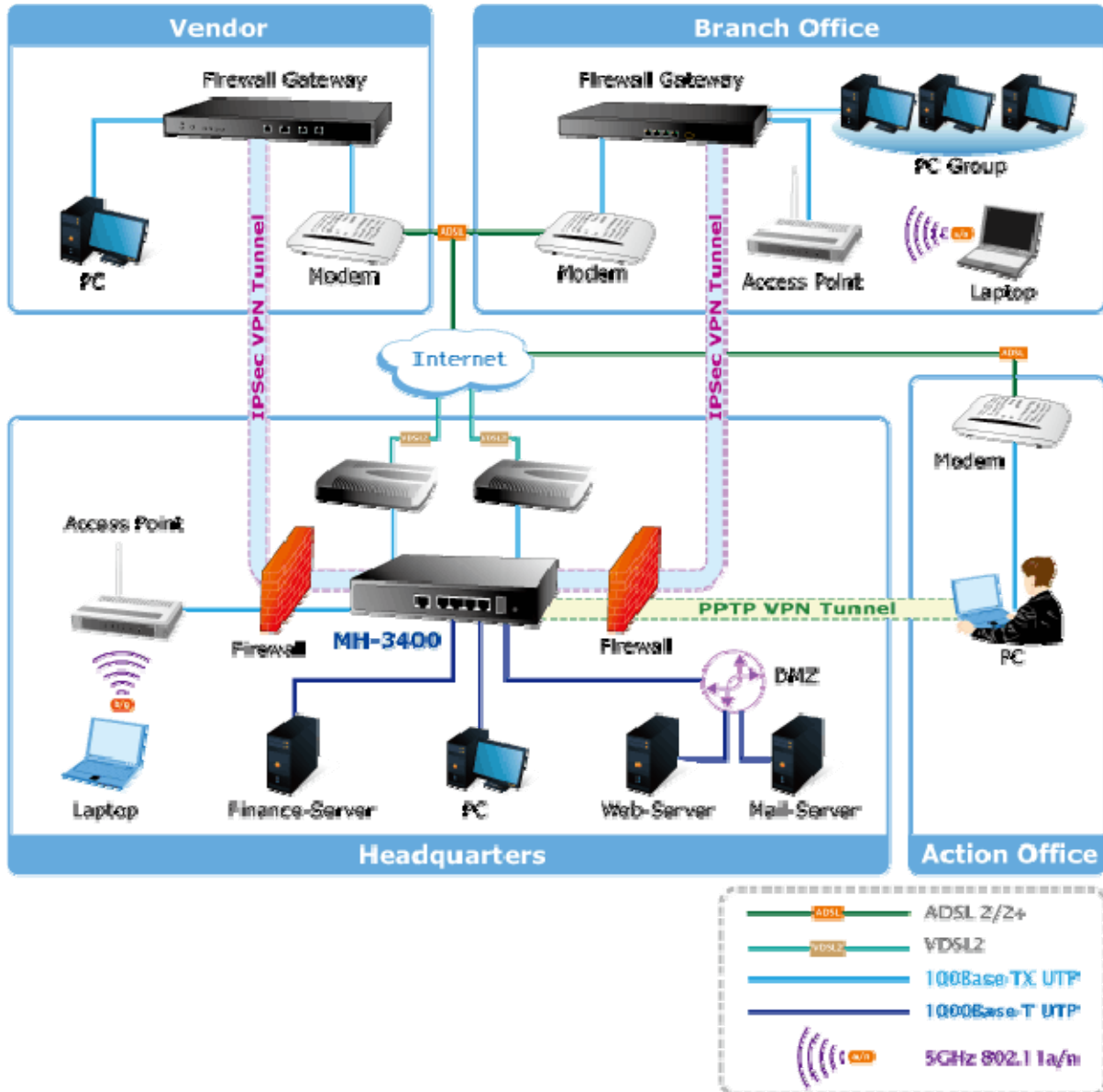
We will follow the process flow to complete the network setting in the following chapters.



## Chapter 3: Hardware Installation

In this chapter we are going to introduce hardware interface as well as physical installation. Safety Instruction

### 3.1 VPN Router Network Connection



**WAN Connection:** A WAN port can be connected with xDSL Modem, Fiber Modem, Switching Hub, or through an external router to connect to the Internet.

**LAN Connection:** The LAN port can be connected to a Switching Hub or directly to a PC. Users can use servers for monitoring or filtering through the port after "Physical Port Mangement" configuration is done.

**DMZ :** The DMZ port can be connected to servers that have legal IP addresses, such as Web servers, mail servers, etc.

## Chapter 4: Login VPN Security Router

This chapter is mainly introducing Web-based UI after connecting VPN Router.

First, check up VPN Router IP address by connecting to DOS through the LAN PC under VPN Security Router. Go to Start → Run, enter cmd to commend DOS, and enter ipconfig for getting Default Gateway address, as the graphic below, 192.168.1.1. Make sure Default Gateway is also the default IP address of VPN QoS Router.


```
C:\Documents and Settings\PM01>ipconfig

Windows IP Configuration

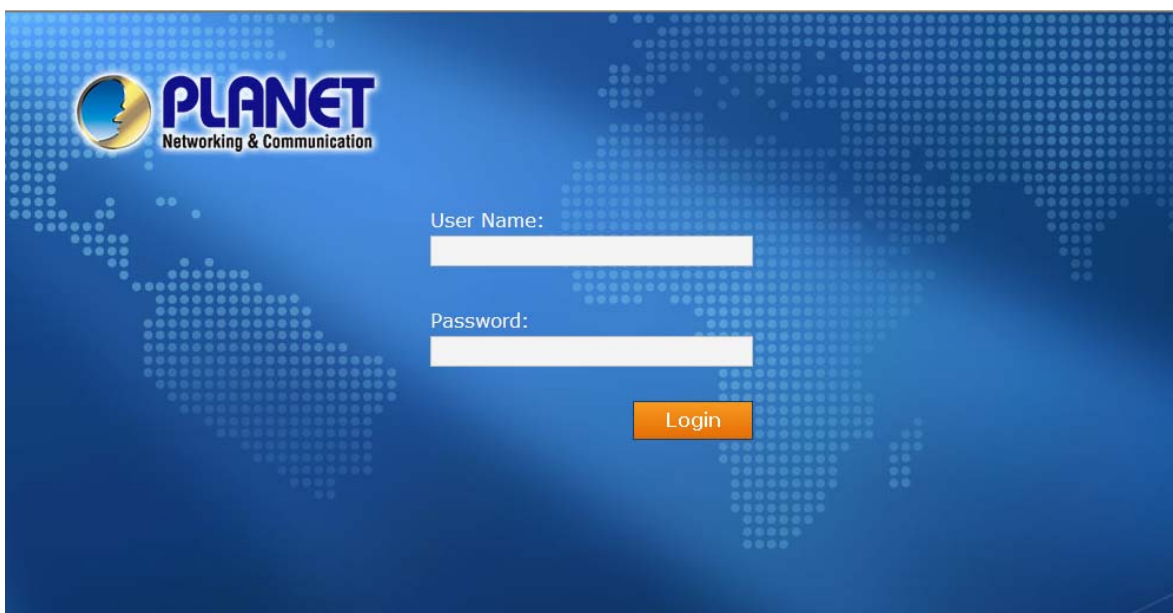
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : smb.com
    IP Address. . . . .                : 192.168.1.100
    Subnet Mask . . . . .              : 255.255.255.0
    IP Address. . . . .                : fe80::222:19ff:fe06:b981%9
    Default Gateway . . . . .          : 192.168.1.1


C:\Documents and Settings\PM01>
```

 <b>Attention</b>	When not getting IP address and default gateway by using “ipconfig”, or the received IP address is 0.0.0.0 and 169.X.X.X, we recommend that users should check if there is any problem with the circuits or the computer network card is connected nicely.
---	--

Then, open webpage browser, IE for example, and key in 192.168.1.1 in the website column. The login window will appear as below:



VPN Router default username and password are both “**admin**”. Users can change the login password in the setting later.

 <b>Attention</b>	For security, we strongly suggest that users must change password after login. Please keep the password safe, or you can not login to VPN Router. Press Reset button for more than 10 sec, all the setting will return to default.
---	--

After login, VPN Router web-based UI will be shown.

## Chapter 5: System Status

This chapter introduces the device specification and status after login as well as change password and system time settings for security.

### 5.1 Home Page

In the Home page, all VPN Security Router parameters and status are listed for users' reference.

#### 5.1.1 WAN Status

##### WAN Status

Interface	WAN 1	WAN 2	WAN 3	WAN 4	USB
WAN IP Address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
DNS	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
Downstream Bandwidth Usage	0	0	0	0	---
Upstream Bandwidth Usage	0	0	0	0	---
DDNS Setup	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled
Quality of Service	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connect	Release Renew	Release Renew	Release Renew	Release Renew	

Item	Description
WAN IP Address	Indicates the current IP configuration for WAN port.
Default Gateway	Indicates current WAN gateway IP address from ISP.
DNS	Indicates the current DNS IP configuration.
Downstream Bandwidth Usage(%)	Indicates the current downstream bandwidth usage (%) for each WAN.
Upstream Bandwidth Usage(%)	Indicates the current upstream bandwidth usage (%) for each WAN.
DDNS Setup	Indicates if Dynamic Domain Name is activated. The default configuration is "Off".
Quality of Service	Indicates how many QoS rules are set.
Manual Connect	When "Obtain an IP automatically" is selected, two buttons (Release and Renew) will appear. If a WAN connection, such as PPPoE or PPTP, is selected, "Disconnect" and "Connect" will appear.

## 5.1.2 Physical Port Status

### Physical Port Status

Port ID	1				
Interface	LAN				
Status	<a href="#">Connect</a>				
Port ID	Internet	Internet	Internet	Internet	USB
Interface	WAN 1	WAN 2	WAN 3	WAN 4	USB
Status	<a href="#">Enabled</a>	<a href="#">Enabled</a>	<a href="#">Enabled</a>	<a href="#">Enabled</a>	Enabled

The status of all system ports, including each connected and enabled port, will be shown on this Home page (see above table). Click the respective status button and a separate window will appear to show detailed data (including setting status summary and statistics) of the selected port.

**WAN 1 Information**

**Summary**

Type	10Base-T / 100Base-TX / 1000Base-T
Interface	WAN
Link Status	Down
Physical Port Status	Port Enabled
Priority	Normal
Speed	10 Mbps
Half/Full Duplex	Half
Auto Negotiation	Enabled

**Statistics**

Received Packets Count	0
Received Packets Byte Count	0
Transmitted Packets Count	0
Transmitted Packets Byte Count	0
Error Packets Count	0

The current port setting status information will be shown in the Port Information Table. Examples: type (10Base-T/100Base-TX/1000Base-T), interface (WAN/ LAN/ DMZ), link status (Up/ Down), physical port status (Port Enabled/ Port Disabled), priority (high or normal), speed status (10Mbps or 100Mbps), duplex status (Half/ Full), auto negotiation (Enabled or Disabled). The table also shows statistics of Receive/ Transmit Packets, Receive/Transmit Packets Byte Count as well as Error Packets Count.






### 5.1.3 System Information

#### System Information

LAN IP Address/Subnet Mask	192.168.1.1/255.255.255.0	Serial Number	0
Working Mode	Gateway	Firmware Version	v1.0.0 .01 (Mar 2 2011 20:30:04)
System Active Time	0 Days0 Hours1 Minutes7 seconds	Current Time	Thu Mar 3 2011 16:53:41
Sessions and CPU Usage Rate	N/A		
Memory Usage	N/A		
Total Session	N/A		

Advance

Item	Description		
<b>LAN IP Address/ Subnet Mask</b>	Identifies the current device IP address and subnet mask. The default is 192.168.1.1 and 255.255.255.0		
<b>Working Mode</b>	Indicates the current working mode. Can be Gateway or Router mode. The default is "Gateway" mode		
<b>System active time:</b>	Indicates how long the device has been running.		
<b>Serial Number:</b>	This number is the device serial number.		
<b>Firmware Version</b>	Information about the device present software version.		
<b>Current Time</b>	Indicates the device present time. <table border="1" data-bbox="502 1198 1428 1332"> <tbody> <tr> <td style="text-align: center;"> <b>Note</b></td> <td>To have the correct time, users must synchronize the device with the remote NTP server first.</td> </tr> </tbody> </table>	 <b>Note</b>	To have the correct time, users must synchronize the device with the remote NTP server first.
 <b>Note</b>	To have the correct time, users must synchronize the device with the remote NTP server first.		

### 5.1.4 Firewall Status

#### Security Status

Firewall	Status
SPI (Stateful Packet Inspection)	On
DoS (Denial of Service)	On
Block WAN Request	On
Prevent ARP Virus Attack	On
Remote Management	Off
Access Rule	0 rules set

Item	Description
------	-------------

<b>SPI (Stateful Packet Inspection)</b>	Indicates whether SPI (Stateful Packet Inspection) is on or off. The default configuration is "On".
<b>DoS (Denial of Service)</b>	Indicates if DoS attack prevention is activated. The default configuration is "On".
<b>Block WAN Request</b>	Indicates that denying the connection from Internet is activated. The default configuration is "On".
<b>Prevent ARP Virus Attack</b>	Indicates that preventing Arp virus attack is activated. The default configuration is "Off".
<b>Remote Management</b>	Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is "Off".
<b>Access Rule</b>	Indicates the number of access rule applied in VPN Security Router.

### 5.1.5 VPN Status

#### VPN Status

IPSec VPN Setting	Status
Tunnel(s) Used	0
Tunnel(s) Available	100

Item	Description
<b>VPN Setting Status</b>	Indicates VPN setting information in VPN Router.
<b>Tunnel(s) Used</b>	Indicates number of tunnels that have been configured in VPN (Virtual Private Network).
<b>Tunnel(s) Available</b>	Indicates number of tunnels that are available for VPN (Virtual Private Network).

### 5.1.6 Log Setting Status

#### Log

Send Log To	Disabled
-------------	----------

Item	Description
<b>Sent Log To</b>	Indicates if Syslog Server is Enabled or Disabled.

## 5.2 Change and Set Login Password and Time

### 5.2.1 Password Setting

When you login VPN Router setting window every time, you must enter the password. The default value for VPN Router username and password are both "admin". For security reasons, we strongly recommend that you must change your password after first login. Please keep the password safe, or you might not login to VPN Router. You can press Reset button for more than 10 sec, VPN Router will return back to default.

## Password Setup

User Name	admin
Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Item	Description
User Name	The default is "admin".
Old Password	Input the original password. ( The default is "admin". )
New User Name	Input the new user name. e.x. Planet
New Password	Input the new password.
Confirm New Password	Input the new password again for verification.
Apply	Click "Apply" to save the configuration.
Cancel	Click "Cancel" to leave without making any change. This action will be effective before "Apply" to save the configuration.

If users have already changed username and password, they should login with current username and password and input "admin" as new username and password if they have to return back to default.

### 5.2.2 Time

VPN Router can adjust time setting. Users can know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources. You can either select the embedded NTP Server synchronization function or set up a time reference.

**Set system time using a NTP server :** VPN Router has embedded NTP server, which will update the time spontaneously.

#### Network Time

- Set system time using a NTP server.  
 Set system time manually.

Time Zone	Beijing (GMT+08:00) <input type="button" value="v"/>
Daylight Saving	<input type="checkbox"/> Enabled from 06 (Month) 25 (Day) to 12 (Month) 25 (Day)
NTP Server	time.nist.gov

Item	Description
<b>Time Zone</b>	Select your location from the pull-down time zone list to show correct local time.
<b>Daylight Saving</b>	If there is <b>Daylight Saving Time</b> in your area, input the date range. The device will adjust the time for the Daylight Saving period automatically.
<b>NTP Server</b>	If you have your own preferred time server, input the server IP address.
<b>Apply</b>	After the changes are completed, click " <b>Apply</b> " to save the configuration.
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any change. This action will be effective before "Apply" to save the configuration.

**Select System Time Manually:** Input the correct time, date, and year in the boxes.

- Set system time using a NTP server.  
 Set system time manually.

17	<b>Hours</b>	0	<b>Minutes</b>	12	<b>seconds</b>
3	<b>Month</b>	3	<b>Day</b>	2011	<b>Year</b>

After the changes are completed, click "**Apply**" to save the configuration. Click "**Cancel**" to leave without making any change. This action will be effective before "Apply" to save the configuration.

## Chapter 6: Network

This Network page contains the basic settings. For most users, completing this general setting is enough for connecting with the Internet. However, some users need advanced information from their ISP. Please refer to the following descriptions for specific configurations.

### 6.1 Network Connection

Host Name :	<input type="text" value="4WAN_1LAN_IPSec_VPN_Router"/>	(Required by some ISPs)
Domain Name :	<input type="text" value="smb.com"/>	(Required by some ISPs)

#### LAN Setting

MAC Address	<input type="text" value="50"/> <input type="text" value="56"/> <input type="text" value="4D"/> <input type="text" value="32"/> <input type="text" value="30"/> <input type="text" value="30"/>	(Default:51-56-4d-32-30-30)
Device IP Address :	<input type="text" value="192.168.1.1"/>	Subnet Mask : <input type="text" value="255.255.255.0"/>
Multiple Subnet Setting:Disabled		

Unified IP Management

#### WAN Setting

Please choose how many WAN ports you prefer to use :  (Default: 4)

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	<a href="#">Edit</a>
WAN 2	Obtain an IP automatically	<a href="#">Edit</a>
WAN 3	Obtain an IP automatically	<a href="#">Edit</a>
WAN 4	Obtain an IP automatically	<a href="#">Edit</a>
USB	3G / 3.5G	<a href="#">Edit</a>

**Enable DMZ**

#### 6.1.1 Host Name and Domain Name

Host Name :	<input type="text" value="4WAN_1LAN_IPSec_VPN_Router"/>	(Required by some ISPs)
Domain Name :	<input type="text" value="smb.com"/>	(Required by some ISPs)

Device name and domain name can be input in the two boxes. Though this configuration is not necessary in most environments, some ISPs in some countries may require it.



## 6.1.2 LAN Setting

LAN setting is shown and can be configured in this page. The LAN MAC can be modified. When a new router replaces an old one, LAN MAC can be changed as MAC of the original device. Gateway ARP binding with LAN PCs won't need to be configured again. Click "Unified IP Management" to setup.

### LAN Setting

MAC Address 50 . 56 . 4D . 32 . 30 . 30 (Default:51-56-4d-32-30-30)	
Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0
Multiple Subnet Setting:Disabled	

Unified IP Management

This is configuration information for the device current LAN IP address. The default configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. It can be changed according to the actual network structure.

### Unified IP Management

LAN IP and IP segment group (DHCP) can be configured here.

### LAN Setting

Device IP Address	192 . 168 . 1 . 1	Subnet Mask	255 . 255 . 255 . 0
<b>Multiple Subnet Setting</b> <input type="checkbox"/> Multiple Subnet			
LAN IP Address <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Subnet Mask <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>			
<input type="button" value="Add to list"/>			
<div style="border: 1px solid gray; height: 80px; width: 100%;"></div>			
<input type="button" value="Delete selected Subnet"/>			

### LAN Setting

This is configuration information for the device current LAN IP address. The default configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. It can be changed according to the actual network structure.

## Multiple-Subnet Setting

Click “Add/Edit” to enter the configuration page, as shown in the following figure. Input the respective IP addresses and subnet masks.

This function enables users to input IP segments that differ from the router network segment to the multi-net segment configuration; the Internet will then be directly accessible. In other words, if there are already different IP segment groups in the Intranet, the Internet is still accessible without making any changes to internal PCs. Users can make changes according to their actual network structure.

## Dynamic IP

There are four set of Class C DHCP server. The defaults are enable. LAN PCs can get IP automatically without configured and recorded.

### Dynamic IP

Enable DHCP Server

	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
IP Range Starts	192,168,1,100	192,168,2,100	192,168,3,100	192,168,4,100
IP Range Ends	192,168,1,149	192,168,2,149	192,168,3,149	192,168,4,149

Item	Description
IP Range Start	The four default IP segments initial from 192.168.1.100, 192.168.2.100, 192.168.3.100, 192.168.4.100. Users can configure according actual demand.
IP Range End	The four default IP segments end at 192.168.1.149, 192.168.2.149, 192.168.3.149, 192.168.4.149. It means there are 50 IPs in one of segments. Users can configure according actual demand.

## 6.1.3 WAN & DMZ Settings

### WAN Setting

#### WAN Setting

Please choose how many WAN ports you prefer to use :  (Default: 4)

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	<a href="#">Edit</a>
WAN 2	Obtain an IP automatically	<a href="#">Edit</a>
WAN 3	Obtain an IP automatically	<a href="#">Edit</a>
WAN 4	Obtain an IP automatically	<a href="#">Edit</a>
USB	3G / 3.5G	<a href="#">Edit</a>

Item	Description
Interface	An indication of which port is connected.
Connection Type	Obtain an IP automatically, Static IP connection, PPPoE (Point-to-Point Protocol over Ethernet), PPTP (Point-to-Point Tunneling Protocol) or Transparent Bridge.
Config	A modification in an advanced configuration: Click Edit to enter the advanced configuration page.

#### Obtain an Automatic IP automatically

This mode is often used in the connection mode to obtain an automatic DHCP IP. This is the device system default connection mode. It is a connection mode in which DHCP clients obtain an IP address automatically. If having a different connection mode, please refer to the following introduction for selection of appropriate configurations. Users can also set up their own DNS IP address. Check the options and input the user-defined DNS IP addresses.

Interface:

WAN Connection Type:

Use the Following DNS Server Addresses

DNS Server(Required):  .  .  .

DNS Server(Optional):  .  .  .

Shared-Circuit WAN environment:  Yes  NO (Filter broadcast packets from WAN)

MTU:  Auto  Manual  bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from  :  to  :  (24-Hour Format)

Line-Dropped Scheduling:  minutes ahead line-dropped to start new session transferring

Backup Interface:

Item	Description
<b>Use the following DNS Server Addresses:</b>	Select a user-defined DNS server IP address.
<b>DNS Server:</b>	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable groups is two IP groups.
<b>Enable Line-Dropped Scheduling:</b>	<p>The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. <b>For example:</b></p> <p>The optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet.</p> <p>Therefore, to avoid a huge number of disconnection, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.</p>
<b>Line-Dropped Period</b>	Input the time rule for disconnection of this WAN service.
<b>Line-Dropped Scheduling</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU:</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

### Static IP

If an ISP issues a static IP (such as one IP or eight IP addresses, etc.), please select this connection mode and follow the steps below to input the IP numbers issued by an ISP into the relevant boxes.

**Interface:** WAN 1

WAN Connection Type : Static IP

WAN IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255 . 255 . 255 . 0

Default Gateway : 0 . 0 . 0 . 0

DNS Server(Required) : 0 . 0 . 0 . 0

DNS Server(Optional) : 0 . 0 . 0 . 0

Shared-Circuit WAN environment :  Yes  NO (Filter broadcast packets from WAN)

MTU :  Auto  Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling : 5 minutes ahead line-dropped to start new session transferring

Backup Interface : disable

Item	Description
<b>WAN IP address</b>	Input the available static IP address issued by ISP.
<b>Subnet Mask</b>	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
<b>Default Gateway</b>	Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.
<b>DNS Server</b>	Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
<b>Enable Line-Dropped Scheduling</b>	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.

<b>Line-Dropped Period</b>	Input the time rule for the disconnection of this WAN service.
<b>Line-Dropped Scheduling</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

## PPPoE

This option is for an ADSL virtual dial-up connection (suitable for ADSL PPPoE). Input the user connection name and password issued by ISP. Then use the PPP Over-Ethernet software built into the device to connect with the Internet. If the PC has been installed with the PPPoE dialing software provided by ISP, remove it. This software will no longer be used for network connection.

**Interface:** WAN 1

WAN Connection Type : PPPoE

UserName :

Password :

Connect on Demand: Max Idle Time  Min.

Keep Alive: Redial Period  Sec.

Shared-Circuit WAN environment :  Yes  NO (Filter broadcast packets from WAN)

MTU :  Auto  Manual  bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from  :  to  :  (24-Hour Format)

Line-Dropped Scheduling :  minutes ahead line-dropped to start new session transferring

Backup Interface :



Item	Description
<b>User Name</b>	Input the user name issued by ISP.
<b>Password</b>	Input the password issued by ISP.
<b>Connect on Demand</b>	This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break-off resulting from no packet transmissions is five minutes).
<b>Keep Alive</b>	This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is disconnected. It also enables a user to set up a time for redialing. The default is 30 seconds.
<b>Enable Line-Dropped Scheduling</b>	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
<b>Line-Dropped Period</b>	Input the time rule for the disconnection of this WAN service.
<b>Line-Dropped Scheduling</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click **“Apply”** to save the configuration, or click **“Cancel”** to leave without making any change.

## PPTP

This option is for the PPTP time counting system. Input the user's connection name and password issued by ISP, and use the built-in PPTP software to connect with the Internet.

**Interface:** WAN 1

WAN Connection Type : PPTP

WAN IP Address : 0 . 0 . 0 . 0

Subnet Mask : 255 . 255 . 255 . 0

Default Gateway : 0 . 0 . 0 . 0

UserName :

Password :

Connect on Demand: Max Idle Time 5 Min.

Keep Alive: Redial Period 30 Sec.

Shared-Circuit WAN environment :  Yes  NO (Filter broadcast packets from WAN)

MTU :  Auto  Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period : from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling : 5 minutes ahead line-dropped to start new session transferring

Backup Interface : disable

Item	Description
<b>WAN IP Address</b>	This option is to configure a static IP address. The IP address to be configured could be one issued by ISP. (The IP address is usually provided by the ISP when the PC is installed. Contact ISP for relevant information).
<b>Subnet Mask</b>	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
<b>Default Gateway Address</b>	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
<b>User Name</b>	Input the user name issued by ISP.

<b>Password</b>	Input the password issued by ISP.
<b>Connect on Demand</b>	This function enables the auto-dialing function to be used for a PPTP dial connection. When the client port attempts to connect with the Internet, the device will automatically connect with the default ISP auto dial connection; when the network has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break off when no packets have been transmitted is five minutes).
<b>Keep Alive</b>	This function enables the PPTP dial connection to redial automatically when the connection has been disconnected. Users can set up the redialing time. The default is 30 seconds.
<b>Enable Line-Dropped Scheduling</b>	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnection, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
<b>Line-Dropped Period</b>	Input the time rule for the disconnection of this WAN service.
<b>Line-Dropped Scheduling</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

### Transparent Bridge

If all Intranet IP addresses are applied as Internet IP addresses, and users don't want to substitute private network IP addresses for all Intranet IP addresses (ex. 192.168.1.X), this function will enable users to integrate existing networks without changing the original structure. Select the Transparent Bridge mode for the WAN connection mode. In this way, users will be able to connect normally with the Internet while keeping the original Internet IP addresses in Intranet IP configuration.

If there are two WANs configured, users still can select Transparent Bridge mode for WAN connection mode, and load balancing will be achieved as usual.

**Interface:** WAN 1

WAN Connection Type: Transparent Bridge ▼

WAN IP Address: 0 . 0 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS Server(Required): 0 . 0 . 0 . 0

DNS Server(Optional): 0 . 0 . 0 . 0

Internal LAN IP Range 1: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 2: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 3: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 4: 0 . 0 . 0 . 0 to 0

Internal LAN IP Range 5: 0 . 0 . 0 . 0 to 0

Shared-Circuit WAN environment:  Yes  NO (Filter broadcast packets from WAN)

MTU:  Auto  Manual 1500 bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from 0 : 0 to 1 : 0 (24-Hour Format)

Line-Dropped Scheduling: 5 minutes ahead line-dropped to start new session transferring

Backup Interface: disable ▼

Back
Apply
Cancel

Item	Description
<b>WAN IP Address</b>	Input one of the static IP addresses issued by ISP.
<b>Subnet Mask</b>	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
<b>Default Gateway Address</b>	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.

<b>DNS Server</b>	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
<b>Internal LAN IP Range</b>	Input the available IP range issued by ISP. If ISP issued two discontinuous IP address ranges, users can input them into Internal LAN IP Range 1 and Internal LAN IP Range 2 respectively.
<b>Enable Line-Dropped Scheduling</b>	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnections, users can activate this function to arrange new connections through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
<b>Line-Dropped Period:</b>	Input the time rule for the disconnection of this WAN service.
<b>Line-Dropped Scheduling:</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) .The default is "Auto".

After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

**Router Plus NAT Mode:**

When you apply a public IP address as your default gateway, you can setup this public IP address into a LAN PC, and this PC can use this public IP address to reach the Internet. Others PCs can use NAT mode to reach the Internet.

If this WAN network is enabled the Router plus NAT mode, you can still use load balancing function in this WAN network.

Interface: WAN 1

WAN Connection Type: Router Plus NAT Mode ▼

WAN IP Address:

Subnet Mask:

Default Gateway:

DNS Server(Required):

DNS Server(Optional):

LAN Default Gateway 1:

LAN (Public) IP Range 1:     to

LAN (Public) IP Range 2:     to

LAN Default Gateway 2:

LAN (Public) IP Range 1:     to

LAN (Public) IP Range 2:     to

LAN Default Gateway 3:

LAN (Public) IP Range 1:     to

LAN (Public) IP Range 2:     to

Shared-Circuit WAN environment:  Yes  NO (Filter broadcast packets from WAN)

MTU:  Auto  Manual  bytes

Enabled Line-Dropped Scheduling

Line-Dropped Period: from  :  to  :  (24-Hour Format)

Line-Dropped Scheduling:  minutes ahead line-dropped to start new session transferring

Backup Interface: disable ▼

Back

Apply

Cancel

Item	Description
WAN IP address	Enter the public IP address.
Subnet mask	Enter the public IP address subnet mask.

<b>WAN default gateway</b>	Enter the WAN default gateway, which provided by your ISP.
<b>DNS Servers</b>	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
<b>Intranet routing default gateway</b>	Enter one of IP addresses that provide by the ISP as your default gateway.
<b>Intranet IP addresses range</b>	Enter your IP addresses range, which IP addresses are provided by ISP. If you have multiple IP ranges, you need setup group1 and group 2. You can also setup the default gateway and IP range in the group 2.
<b>Enable Line-Dropped Scheduling</b>	The WAN disconnection schedule will be activated by checking this option. In some areas, there is a time limitation for WAN connection service. For example: the optical fiber service will be disconnected from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN disconnection, all the external connections that go through this WAN will be disconnected too. Only after the disconnected lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of disconnection, users can activate this function to arrange new connections to be made through another WAN to the Internet. In this way, the effect of any disconnection can be minimized.
<b>Line-Dropped Period</b>	Input the time rule for disconnection of this WAN service.
<b>Line-Dropped Scheduling</b>	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
<b>Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Link Backup Interface</b>	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
<b>Shared- Circuit WAN environment:</b>	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
<b>MTU</b>	MTU is abbreviation of Maximum Transmission Unit. "Auto" and "Manual" can be chosen. The default value is 1500. Different value could be set in different network environment. (e.g. ADSL PPPoE MTU: 1492) The default is "Auto".

Click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

## DMZ Setting

For some network environments, an independent Configurable DMZ port may be required to set up externally connected servers such as WEB and Mail servers. Therefore, the device supports a set of independent Configurable DMZ ports for users to set up connections for servers with real IP addresses. The DMZ ports act as bridges between the Internet and LANs.

### DMZ Setting

Interface	IP Address	Config.
DMZ	0.0.0.0	<a href="#">Edit</a>

Item	Description
IP address	Indicates the current default static IP address.
Config.	Indicates an advanced configuration modification: Click <b>Edit</b> to enter the advanced configuration page.

The DMZ configuration can be classified by Subnet and Range:

### Subnet

The DMZ and WAN located in different Subnets .For example: If the ISP issued 16 real IP addresses: 220.243.230.1-16 with Mask 255.255.255.240, users have to separate the 16 IP addresses into two groups: 220.243.230.1-8 with Mask 255.255.255.248, and 220.243.230.9-16 with Mask 255.255.255.248 and then set the device and the gateway in the same group with the other group in the DMZ.

Interface

Subnet
  Range (DMZ & WAN within same subnet)
  DMZ IP ranges are the same with WAN IP ranges in Router Plus NAT mode

Specify DMZ IP Address

Subnet Mask



### Range

DMZ and WAN are within same Subnet

Interface

Subnet
  Range (DMZ & WAN within same subnet)
  DMZ IP ranges are the same with WAN IP ranges in Router Plus NAT mode

Interface

IP Range for DMZ port     to

Item	Description
IP Range	Input the IP range located at the DMZ port.

After the changes are completed, click **“Apply”** to save the configuration, or click **“Cancel”** to leave without making any changes.

### DMZ IP ranges are the same with WAN IP ranges in Router Plus NAT mode:

Interface

Subnet
  Range (DMZ & WAN within same subnet)
  DMZ IP ranges are the same with WAN IP ranges in Router Plus NAT mode

Interface

LAN Default Gateway1:

LAN (Public) IP Range     to

LAN Default Gateway2:

LAN (Public) IP Range     to

LAN Default Gateway3:

LAN (Public) IP Range     to

Item	Description
LAN Default Gateway	Enter the LAN Default Gateway that you configured at Router Plus NAT Mode
LAN IP Range	Enter the usable static IP range that provide by ISP into the DMZ service IP range. If you have other IP range, you can setup the default gateway and IP range into group 2.

After the changes are completed, click **“Apply”** to save the configuration, or click **“Cancel”** to leave without making any changes

## 6.2 Multi- WAN Setting

### 6.2.1 Load Balance Mode

#### Mode

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session <input type="radio"/> By IP	<input type="radio"/> Advanced Function
Unbinding WAN Balance	Un-binding WAN Balance Mode:	<input type="radio"/> By Session <input type="radio"/> By IP	<input type="radio"/> Advanced Function
Strategy Routing	Mode:	<input type="radio"/> By Session <input type="radio"/> By IP	<input type="radio"/> Advanced Function
<input type="button" value="Set WAN Grouping"/>			
Strategy Routing		<input type="button" value="Disabled"/> ▼	<input type="button" value="Import IP Range"/>
Self-defined Strategy 1		<input type="button" value="Disabled"/> ▼	
Self-defined Strategy 2		<input type="button" value="Disabled"/> ▼	

#### Auto Load Balance Mode

When Auto Load Balance mode is selected, the device will use sessions or IP and the WAN bandwidth automatically allocate connections to achieve load balancing for external connections. The network bandwidth is set by what users input for it. For example, if the upload bandwidth of both WANs is 512Kbit/sec, the automatic load ratio will be 1:1; if one of the upload bandwidths is 1024Kbit/sec while the other is 512Kbit/sec, the automatic load ratio will be 2:1. Therefore, to ensure that the device can balance the actual network load, please input real upload and download bandwidths.

Item	Description
<b>Session Balance</b>	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
<b>IP Session Balance</b>	If "By IP" is selected, the WAN bandwidth will automatically allocate connections based on IP amount to achieve network load balance.

#### Note

For either session balancing or IP connection balancing, collocation with Protocol Binding will provide a more flexible application for bandwidth. Users can assign a specific Intranet IP to go through a specific service provider for connection, or assign an IP for a specific destination to go through the WAN users assign to connect with the Internet.

For example, if users want to assign IP 192.168.1.100 to go through WAN 1 when connecting with the Internet, or assign all Intranet IP to go through WAN 2 when connecting with servers with port 80, or assign all Intranet IP to go through WAN 1 when connecting with IP 211.1.1.1, users can do that by configuring "Protocol Binding".

#### Attention

When the Auto Load Balance mode is collocated with Protocol Binding, only IP addresses or servers that are configured in the connection rule will follow the rule for external connections; those which are not configured in the rule will still follow the device Auto Load Balance system.

Please refer to the explanations in 6.2.3 Configuring Protocol Binding for setting up Protocol Binding and for examples of collocating router modes with Protocol Binding.

### Unbinding WAN Balance Mode

This mode enables users to assign specific intranet IP addresses, destination application service ports or destination IP addresses to go through an assigned WAN for external connection. After being assigned, the specific WAN will only support those assigned Intranet IP addresses, specific destination application service ports, or specific destination IP addresses. Intranet IP, specific destination application service ports and specific destination IP that is not configured under the rules will go through other WANs for external connection. For unassigned WANs, users can select Load Balance mode and select session or IP for load balancing.

Item	Description
<b>Session Balance:</b>	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
<b>IP Balance:</b>	If "By IP" is selected, the WAN bandwidth will automatically allocate connections based on the number of IP addresses to achieve network load balance.



#### Note

Only when a device assignment is collocated with Protocol Binding can the balancing function be brought into full play. For example, an assignment requiring all Intranet IP addresses to go through WAN 1 when connecting with service port 80, or go through WAN 1 when connecting with IP 211.1.1.1, must be set up in the Protocol Binding Configuration.



#### Attention

When assigning mode is selected, as in the above example, the IP(s) or service provider(s) configured in the connection rule will follow the rule for external connections, but those which are not configured in the rule will still follow the device Load Balance system to go through other WAN ports to connect with the Internet.

Please refer to the explanations in **6.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding

### Strategy Routing Mode

If strategy Routing is selected, the device will automatically allocate external connections based on routing policy (Division of traffic between Telecom and Netcom is to be used in China) embedded in the device. All you have to do is to select the WAN (or WAN group) which is connected with Netcom; the device will then automatically dispatch the traffic for Netcom through that WAN to connect with the Internet and dispatch traffic for Telecom to go through the WAN connected with Telecom to the Internet accordingly. In this way, the traffic

for Netcom and Telecom can be divided.

### Set WAN Grouping

If more than one WAN is connected with Netcom, to apply a similar division of traffic policy to these WANs, a combination for the WANs must be made. Click “Set WAN Grouping”; an interactive window as shown in the figure below will be displayed.

The screenshot shows a configuration window titled "Set WAN Grouping". On the left side, there is a "Name" label followed by a text input box. Below that is the "Interface" section, which contains four checkboxes: "WAN 1", "WAN 2", "WAN 3", and "USB". To the right of these checkboxes is a large, empty rectangular area intended for a list of selected WANs. At the bottom of the window, there are five buttons: "Add to list", "Delete selected", "Apply", "Cancel", and "Exit".

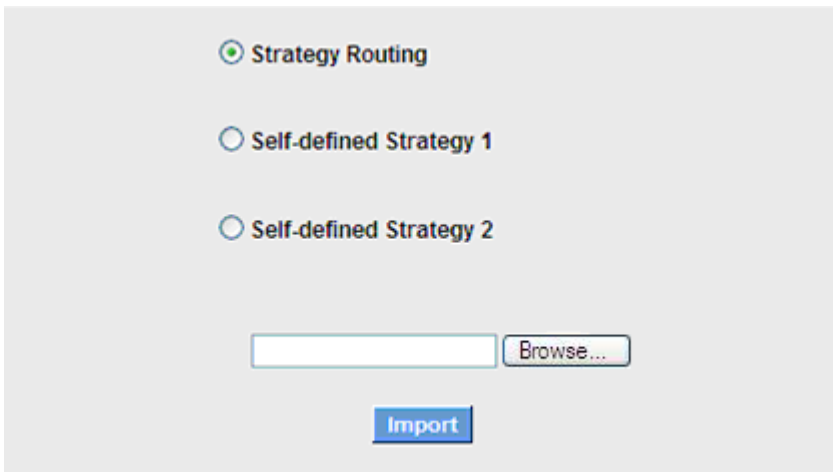
Item	Description
<b>Name</b>	To define a name for the WAN grouping in the box, such as “Education” etc. The name is for recognizing different WAN groups.
<b>Interface</b>	Check the boxes for the WANs to be added into this combination.
<b>Add To List</b>	To add a WAN group to the grouping list.
<b>Delete selected Item</b>	To remove selected WANs from the WAN grouping.
<b>Apply</b>	Click “Apply” to save the modification.
<b>Close</b>	Click “Cancel” to cancel the modification. This only works before “Apply” is clicked.

After the configuration is completed, in the China Netcom Policy window users can select WANs in combination to connect with Netcom.

## Import Strategy

A division of traffic policy can be defined by users too. In the "Import Strategy" window, select the WAN or WAN group (ex. WAN 1) to be assigned and click the "Import IP Range" button; the dialogue box for document importation will be displayed accordingly.

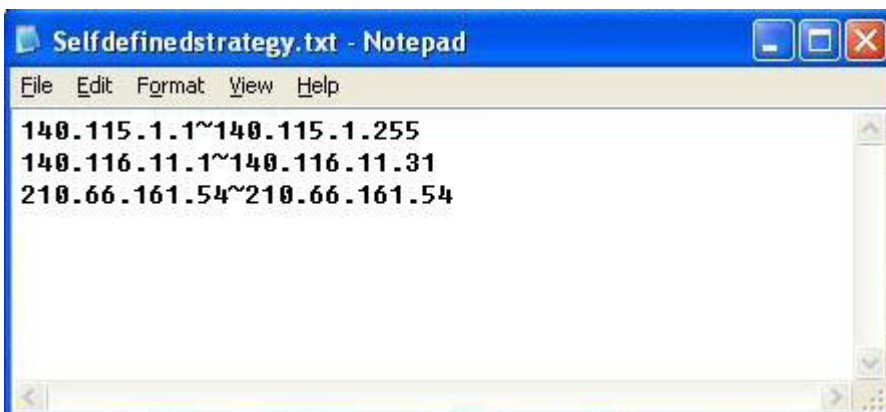
A policy document is an editable text document. It may contain a destination IP users designated. After the path for document importation has been selected, click "Import", and then at the bottom of the configuration window click "Apply". The device will then dispatch the traffic to the assigned destination IP through the WAN (ex. WAN 1) or WAN grouping users designated to the Internet.



To build a policy document users can use a text-based editor, such as Notepad, which is included with Windows system. Follow the text format in the figure below to key in the destination IP addresses users want to assign.

For example, if the destination IP address range users want to designate is 140.115.1.1 ~ 140.115.1.255, key in 140.115.1.1 ~ 140.115.1.255 in Notepad. The next destination IP address range should be keyed in the next line. Attention! Even if only one destination IP address is to be assigned, it should follow the same format.

For example, if the destination IP address is 210.66.161.54, it should be keyed in as 210.66.161.54~210.66.161.54. After the document has been saved (the extension file name is .txt), users can import the IP range of self-defined strategy.



**Note**

China Netcom strategy and self-defined strategy can coexist. However, if a destination IP is assigned by both China Netcom strategy and self-defined strategy, China Netcom strategy will take priority. In other words, traffic to that destination IP will be transmitted through the WAN (or WAN group) under China Netcom strategy.

**Session Balance Advanced Function**

In general, session balance is to equally and randomly distribute the session connections of each intranet IP. For some special connections, for example, web banking encrypted connection (Https or TCP443), is required to connect from the same WAN IP. If one intranet IP visits web banking website and the connection is distributed into different WAN IP addresses, there will be disconnection or failure. Session balance advanced function targets at solving this issue.

Session balance advanced function can set the same intranet IP keeps having sessions from the same WAN IP for some specific service protocols. Other service protocols can still adopt the original balance mechanism to distribute the sessions equally and randomly. With the original session balance efficiency, advanced function can ensure the connection running without error for some special service protocols.

**Mode**

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session	<a href="#">Advanced Function</a>	<input type="radio"/> By IP
Unbinding WAN Balance	Un-binding WAN Balance Mode:	<input type="radio"/> By Session	<a href="#">Advanced Function</a>	<input type="radio"/> By IP
Strategy Routing	Mode:	<input type="radio"/> By Session	<a href="#">Advanced Function</a>	<input type="radio"/> By IP
<a href="#">Set WAN Grouping</a>				
Strategy Routing		Disabled	<a href="#">Import IP Range</a>	
Self-defined Strategy 1		Disabled		
Self-defined Strategy 2		Disabled		

Click "Advanced Function" to enter the setting window:

Destination Auto Binding  
 User Define Dest. IP or Port Auto Binding

---

**No Aging Time**

Protocol :  ▾

Port Range :  to


TCP[1863~1863]  
 TCP[5050~5050]  
 UDP[8000~8005]


---

Item	Description
<b>Destination Auto Binding</b>	Indicates that the session will be connected with the same WAN IP when the destination IP is in the same Class B range.

For example, there are WAN1-1 200.10.10.1 and WAN2- 200.10.10.2, and two intranet IP addresses. When 192.168.1.100 visits Internet 61.222.81.100 for the first time, the connection is through WAN1- 200.10.10.1. If the next destination is to 61.222.81.101 (in the same Class B range), the connection will also be through WAN1- 200.10.10.1. If the destination is to other IP not in the same Class B range as 61.222.81.100, the session will be distributed in the original session balance mechanism.

When the other intranet IP 192.168.1.101 visits 61.222.81.101 for the first time, the connection is through WAN2- 200.10.10.2. If the next destination is to 61.222.81.100 (in the same Class B range), the connection will also be through WAN2 200.10.10.2. If the destination is to other IP not in the same Class B range as 61.222.81.100), the session will be distributed in the original session balance mechanism.

 <b>Note</b>	<p>Not all intranet IP will visit the same Class B range with the same WAN IP. It depends on which WAN the first connection goes to. If the destination IP is in the same Class B range, the connection will go through with the same WAN IP based on the first time learning.</p>
--	--

Item	Description
<p><b>User Define Dis. Or Port Auto Binding</b></p>	<p>Indicates that the intranet IP will connect through the same WAN IP when the service ports are self- defined. You can self- define the service ports and destination IP. (If the destination IP is set as 0.0.0.0 to 0, this represents that the destination is to any IP range.)</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center; vertical-align: middle;">   <b>Note</b> </p> <p>You can only choose either <b>Destination Auto Binding</b> or <b>User Define Dis. Or Port Auto Binding</b>.</p> </div>

Take default rules for example:

Destination Auto Binding  
 User Define Dest. IP or Port Auto Binding

---

Service : All Traffic [TCP&UDP/1~65535] ▼

Service Management

Dest. IP ▼  .  .  .

Enable :

Add to list

HTTPS [TCP/443~443]->0.0.0.0~0.0.0.0

Delete selected Entry

---

Apply
Cancel
Exit



When any intranet IP connects with TCP443 port or any destination (0.0.0.0 to 0 represents any destination), it will go through the same WAN IP. As for which WAN will be selected, this follows the first- chosen WAN IP distributed by the original session balance mechanism.

For example, there are two intranet IP- 192.168.100.1 and 192.168.100.2. When these intranet IPs first connects with TCP443 port, 192.168.100.1 will go through WAN1, and 192.168,100.2 will go through WAN2. Afterwards, 192.168.100.1 will go through WAN1 when there are TCP443 port connections. 192.168.100.2 will go through WAN2 when there are TCP443 port connections. This rule is by default. You can delete or add rules to meet your connection requirement.

## 6.2.2 Network Detection Service

This is a detection system for network external services. If this option is selected, information such “**Retry**” or “**Retry Timeout**” will be displayed. If two WANs are used for external connection, be sure to activate the NSD system, so as to avoid any unwanted break caused by the device misjudgment of the overload traffic for the WAN.

### ▶ Network Service Detection

Interface	WAN 1
<input checked="" type="checkbox"/> Enable	
Retry count	5
Retry timeout	30 seconds
When Fail	Remove the Connection
<input checked="" type="checkbox"/> When In <input type="checkbox"/> OR <input checked="" type="checkbox"/> Out bandwidth is over 1 %, regarded as normal.	
<input checked="" type="checkbox"/> Default Gateway	
<input type="checkbox"/> ISP Host	
<input type="checkbox"/> Remote Host	
<input type="checkbox"/> DNS Lookup Host	

Item	Description
<b>Interface</b>	Select the WAN Port that enables Network Service Detection.
<b>Retry</b>	This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured “Retry Times”, it will be judged as “External Connection Disconnected”.
<b>Retry Timeout</b>	Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.
<b>When Fail</b>	<b>(1) Generate the Error Condition in the System Log:</b> If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections.

	<p>This option is suitable under the condition that one of the WAN connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination.</p> <p>For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 is not to support these destinations, users should select this option. When the WAN1 connection is disconnected, packets for 10.0.0.1~10.254.254.254 cannot be transmitted through WAN 2, and there is no need to remove the connection when WAN 1 is disconnected.</p> <p><b>(2) Keep System Log and Remove the Connection:</b> If an ISP connection failure is detected, no error message will be recorded in the System Log. The packet transmitted through this WAN will be shifted to the other WAN automatically, and be shifted back again when the connection for the original WAN is repaired and reconnected.</p> <p>This option is suitable when one of the WAN connections fails and the traffic going through this WAN to the destination IP should go through the other WAN to reach the destination. In this way, when any of the WAN connections is broken, other WANs can serve as a backup; traffic can be shifted to a WAN that is still connected.</p>
<b>Default Gateway</b>	<p>The local default communication gateway location, such as the IP address of an ADSL router, will be input automatically by the device. Therefore, users just need to check the option if this function is needed. Attention! Some gateways of an ADSL network will not affect packet detection. If users have an optical fiber box, or the IP issued by ISP is a public IP and the gateway is located at the port of the net café rather than at the IP provider's port, do not activate this option.</p>
<b>ISP Host</b>	<p>This is the detected location for the ISP port, such as the DNS IP address of ISP. When configuring an IP address for this function, make sure this IP is capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port)</p>
<b>Remote Host</b>	<p>This is the detected location for the remote Network Segment. This Remote Host IP should better be capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port).</p>
<b>DNS Lookup</b>	<p>This is the detect location for DNS. (Only a web address such as</p>
<b>Host</b>	<p>www.hinet.net is acceptable here. Do not input an IP address.) In addition, do not input the same web address in this box for two different WANs.</p>



In the load balance mode for Assigned Routing, the first WAN port (WAN1) will be saved for the traffic of the IP addresses or the application service ports that are not assigned to other WANs (WAN2, WAN3, and WAN4). Therefore, in this mode, we recommend assigning one of the connections to the first WAN. When other WANs (WAN2, WAN3, or WAN4) are broken and connection error remove (Remove the Connection) has been selected for the connection detection system, traffic will be shifted to the first WAN (WAN1). In addition, if the first WAN (WAN1) is broken, the traffic will be shifted to other WANs in turn. For example, the traffic will be shifted to WAN2 first; if WAN2 is broken too, the traffic will be shifted to WAN3, and so on.

### 6.2.3 Protocol Binding

The VPN router can set up to four WAN interface, the bandwidth and whether can connect to the internet will effect the router load-balancing feature for each WAN, so the bandwidth setting and line detect is must be correct for each WAN interface.

In “WAN Setting, click “Edit” to enter the WAN interface configure window. In “Bandwidth Management “ can adjust the bandwidth for each WAN interface.

## WAN Setting

### WAN Setting

Please choose how many WAN ports you prefer to use :  (Default: 4)

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	<a href="#">Edit</a>
WAN 2	Obtain an IP automatically	<a href="#">Edit</a>
WAN 3	Obtain an IP automatically	<a href="#">Edit</a>
WAN 4	Obtain an IP automatically	<a href="#">Edit</a>
USB	3G / 3.5G	<a href="#">Edit</a>


## Bandwidth Management

### The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 2	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 3	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 4	<input type="text" value="10000"/>	<input type="text" value="10000"/>
USB	<input type="text" value="256"/>	<input type="text" value="2048"/>

## Protocol Binding

Users can define specific IP addresses or specific application service ports to go through a user-assigned WAN for external connections. For any other unassigned IP addresses and services, WAN load balancing will still be carried out.

 <b>Note</b>	<p>In the load balance mode of Assigned Routing, the first WAN (WAN1) cannot be assigned. It is to be saved for the IP addresses and the application Service Ports that are not assigned to other WANs (WAN2, WAN3, and WAN4) for external connections. In other words, the first WAN (WAN1) cannot be configured with the Protocol Binding rule. This is to avoid a condition where all WANs are assigned to specific Intranet IP or Service Ports and destination IP, no more WAN ports will be available for other IP addresses and Service Ports.</p>
--	---

### Protocol Binding

Show Priority

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Source IP 192 . 168 . 1 .  to

Dest. IP  .  .  .  to

Interface : WAN 1

Enabled :

Move Up
Add to list
Move Down

Delete selected item

Show Table
Apply
Cancel

Item	Description
<b>Service</b>	This is to select the Binding Service Port to be activated. The default (such as ALL-TCP&UDP 0~65535, WWW 80~80, FTP 21 to 21, etc.) can be selected from the pull-down option list. The default Service is All 0~65535.

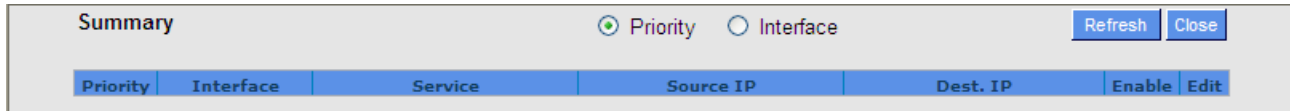
	Option List for Service Management: Click the button to enter the Service Port configuration page to add or remove default Service Ports on the option list.
<b>Source IP</b>	Users can assign packets of specific Intranet virtual IP to go through a specific WAN port for external connection. In the boxes here, input the Intranet virtual IP address range; for example, if 192.168.1.100~150 is input, the binding range will be 100~150. If only specific Service Ports need to be designated, while specific IP designation is not necessary, input "0" in the IP boxes.
<b>Destination IP</b>	In the boxes, input an external static IP address. For example, if connections to destination IP address 210.11.1.1 are to be restricted to WAN1, the external static IP address 210.1.1.1 ~ 210.1.1.1 should be input. If a range of destinations is to be assigned, input the range such as 210.11.1.1 ~ 210.11.255.254. This means the Class B Network Segment of 210.11.x.x will be restricted to a specific WAN. If only specific Service Ports need to be designated, while a specific IP destination assignment is not required, input "0" into the IP boxes.
<b>Interface</b>	Select the WAN for which users want to set up the binding rule.
<b>Enable</b>	To activate the rule.
<b>Add To List</b>	To add this rule to the list.
<b>Delete selected application</b>	To remove the rules selected from the Service List.
<b>Moving Up &amp; Down</b>	The priority for rule execution depends on the rule order in the list. A rule located at the top will be executed prior to those located below it. Users can arrange the order according to their priorities.

**Note**

The rules configured in Protocol Binding will be executed by the device according to their priorities too. The higher up on the list, the higher the priority of execution.

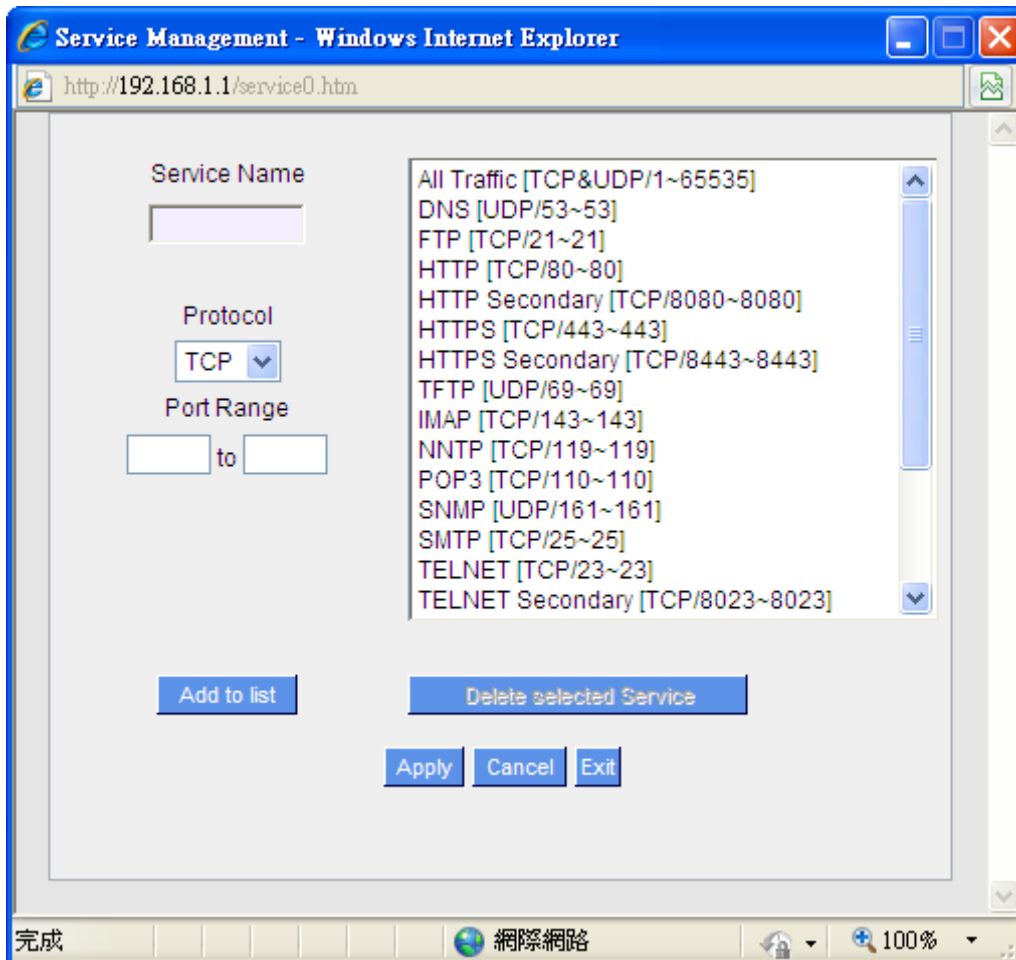
## Show Table

Click the “Show Table” button. A dialogue box as shown in the following figure will be displayed. Users can choose to sort the list by priorities or by interface. Click “Refresh” and the page will be refreshed; click “Close” and the dialogue box will be closed.



## Add or Remove Service Port

If the Service Port users want to activate is not in the list, users can add or remove service ports from “Service Port Management” to arrange the list, as described in the following:



Item	Description
<b>Service Name</b>	In this box, input the name of the Service Port which users want to activate, such as BT, etc.
<b>Protocol</b>	This option list is for selecting a packet format, such as TCP or UDP for the Service Ports users want to activate.
<b>Port range</b>	In the boxes, input the range of Service Ports users want to add.
<b>Add To List</b>	Click the button to add the configuration into the Services List. Users can add

	up to 100 services into the list.
<b>Delete selected service</b>	To remove the selected activated Services.
<b>Apply</b>	Click the “ <b>Apply</b> ” button to save the modification.
<b>Cancel</b>	Click the “ <b>Cancel</b> ” button to cancel the modification. This only works before “ <b>Apply</b> ” is clicked.

**Auto Load Balancing mode when enabled**

The collocation of the Auto Load Balance Mode and the Auto Load Mode will enable more flexible use of bandwidth. Users can assign specific Intranet IP addresses to specific destination application service ports or assign specific destination IP addresses to a WAN users choose for external connections.

**Example 1:How do I set up Auto Load Balance Mode to assign the Intranet IP 192.168.1.100 to WAN2 for the Internet?**

As in the figure below, select “All Traffic” from the pull-down option list “Service”, and then in the boxes of “Source IP” input the source IP address “192.168.1.100” to “100”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode.

Protocol Binding

[Show Priority](#)

Service : All Traffic [TCP&UDP/1~65535] ▼

[Service Management](#)

Source IP ▼ 192 . 168 . 1 . 100 to 100

Dest. IP ▼ 0 . 0 . 0 . 0 to  
0 . 0 . 0 . 0

Interface : WAN 2 ▼

Enabled :

Move Up
Update this Application
Move Down

All Traffic [TCP&UDP/1~65535]->192.168.1.100~100(0.0.0.0~0.0.0.0)WAN 2

Delete selected item
Add

Show Table
Apply
Cancel

**Example 2: How do I set up Auto Load Balance Mode to keep Intranet IP 192.168.1.150 ~ 200 from going through WAN2 when the destination port is Port 80?**

As in the figure below, select “HTTP [TCP/80~80]” from the pull-down option list “Service”, and then in the boxes for “Source IP” input “192.168.1.150” to “200”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode.

**Protocol Binding**

Service : HTTP [TCP/80~80]

Service Management

Source IP : 192 . 168 . 1 . 150 to 200

Dest. IP : 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Interface : WAN 2

Enabled :

Move Up      Update this Application      Move Down

HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN 2

Delete selected item      Add

Show Table    Apply    Cancel

**Example 3: How do I set up Auto Load Balance Mode to keep all Intranet IP addresses from going through WAN2 when the destination port is Port 80 and keep all other services from going through WAN1?**

As in the figure below, there are two rules to be configured. The first rule: select “HTTP [TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of Source IP input “192.168.1.0” to “0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets to Port 80 through WAN2. However, with only the above rule, packets that do not go to Port 80 may be transmitted through WAN2; therefore, a second rule is necessary. The second rule: Select “All Ports [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then input “192.168.1.2 ~ 254” in the boxes of “Source IP”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to



include all Internet IP addresses). Select WAN1 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets that are not going to Port 80 to the Internet through WAN1.

### Protocol Binding

[Show Priority](#)

Service : HTTP [TCP/80~80] ▼

[Service Management](#)

Source IP ▼ 192 . 168 . 1 . 0 to 0

Dest. IP ▼ 0 . 0 . 0 . 0 to 0

0 . 0 . 0 . 0

Interface : WAN 2 ▼

Enabled :

[Move Up](#)
[Update this Application](#)
[Move Down](#)

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)WAN 2

All Traffic [TCP&UDP/1~65535]->192.168.1.2~254(0.0.0.0~0.0.0.0)WAN 1

[Delete selected item](#)
[Add](#)

[Show Table](#) [Apply](#) [Cancel](#)

### Configuring “Assigned Routing Mode” for load Balance

**IP Group:** This function allows users to assign packets from specific Intranet IP addresses or to specific destination Service Ports and to specific destination IP addresses through an assigned WAN to the Internet. After being assigned, the specific WAN will only support those assigned Intranet IP addresses, destination Service Ports, or destination IP addresses. Those which are not configured will go through other WANs for external connection. Only when this mode is collocated with “Assigned Routing” can it bring the function into full play.

**Example 1:**How do I set up the Assigned Routing Mode to keep all Intranet IP addresses from going through WAN2 when the destination is Port 80, and keep all other services from going through WAN1?

As in the figure below, select “HTTP[TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses).

Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. After the rule is set up, only packets that go to Port 80 will be transmitted through WAN2, while other traffics will be transmitted through WAN1.

### Protocol Binding

Service : HTTP [TCP/80~80]

Service Management

Source IP : 192 . 168 . 1 . 0 to 0

Dest. IP : 0 . 0 . 0 . 0 to 0

Interface : WAN 2

Enabled :

Move Up      Update this Application      Move Down

HTTP [TCP/80~80]->192.168.1.0~0(0.0.0.0~0.0.0.0)WAN 2
---

Delete selected item      Add

Show Table    Apply    Cancel

**Example 2: How do I configure Protocol Binding to keep traffic from all Intranet IP addresses from going through WAN2 when the destinations are IP 211.1.1.1 ~ 211.254.254.254 as well as the whole Class A group of 60.1.1.1 ~ 60.254.254.254, while traffic to other destinations goes through WAN1?**

As in the following figure, there are two rules to be configured. The first rule: Select “All Port [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). In the boxes for “Destination IP” input “211.1.1.1 ~ 211.254.254.254”. Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The second rule: Select “All Port [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). In the boxes of “Destination IP” input “211.1.1.1 ~ 60,254,254,254”. Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New”, and the rule will be added to the mode. After the rule has been set up, all traffic that is not going to the assigned destinations will only be transmitted through WAN1.

Protocol Binding

Show Priority

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Source IP 192 . 168 . 1 . 0 to 0

Dest. IP 211 . 1 . 1 . 1 to 211 . 254 . 254 . 254

Interface : WAN 2

Enabled :

Move Up
Update this Application
Move Down

All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)WAN 2

All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)WAN 2

Delete selected item
Add

Show Table
Apply
Cancel

## Chapter 7: Port Management

This chapter introduces how to configure ports and understand how to configure intranet IP addresses.

### 7.1 Setup

Through the device, users can easily manage the setup for WAN ports, LAN ports and the DMZ port by choosing the number of ports, speed, priority, duplex and enable/disable the auto-negotiation feature for connection setting of each port.

#### Port Setup

Please choose how many WAN ports you prefer to use :  (Default: 4)

Enable Port 1 as Mirror Port

Port ID	Interface	Disable	Priority	Speed	Half/Full Duplex	Auto Negotiation	Port VLAN
1	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	VLAN1
2	WAN 1	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
3	WAN 2	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
4	WAN 3	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	
5	DMZ	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enabled	

**Mirror Port** : Users can configure LAN 1 as mirror port by choosing “Enable Port 1 as Mirror Port”. All the traffic from LAN to WAN will be copied to mirror port. Administrator can control or filter the traffic through mirror port. Once this function is enabled, LAN 1 will be shown as Mirror Port in Physical Port Status, Home page.

Item	Description
<b>Disabled</b>	This feature allows users turn on/off the Ethernet port. If selected, the Ethernet port will be shut down immediately and no connection can be made. The default value is "on".
<b>Priority</b>	This feature allows users to set the high/low priority of the packet delivery for the Ethernet port. If it is set as High, the port has the first priority to deliver the packet. The default value is “Normal”.
<b>Speed</b>	This feature allows users to select the network hardware connection speed for the Ethernet port. The options are 10Mbps and 100Mbps.
<b>Duplex Status</b>	This feature allows users to select the network hardware connection speed working mode for the Ethernet. The options are full duplex and half duplex.
<b>Auto Neg.</b>	The Auto-Negotiation mode can enable each port to automatically adjust and gather the connection speed and duplex mode. Therefore, if Enabled

	Auto-Neg. selected, the ports setup will be done without any manual setting by administrators.
<b>VLAN</b>	<p>This feature allows administrators to set the LAN port to be one or more disconnected network sessions. All of them will be able to log on to the Internet through the device.</p> <p>Members in the same network session (within the same VLAN) can see and communicate with each other. Members in different VLAN will not know the existence of other members.</p>
<b>VLAN All</b>	<p>Set VLAN All port to be the public area of VLAN so that it can be connected to other VLAN networks. A server should be constructed for the intranet so that all VLAN group can visit this server. Set one of the network ports as VLAN All.</p> <p>Connect the server to VLAN All so that computers of different VLAN groups can be connected to this server. Moreover, the port where the administrator locates must be set as VLAN All so that it can be connected to the entire network to facilitate network management.</p>

## 7.2 Port Status

Port ID LAN 1 ▼

### Summary

Type	10Base-T / 100Base-TX / 1000Base-T
Interface	LAN
Link Status	Up
Physical Port Status	Port Enabled
Priority Setup	Normal
Speed	1000 Mbps
Half/Full Duplex	Full
Auto Negotiation	Enabled
Port VLAN	VLAN1

### Statistics

Received Packets Count	3191
Received Bytes Count	443391
Transmitted Packets Count	29018
Transmitted Bytes Count	7079145
Error Packets Count	0

Refresh

**Summary**

There are Network Connection Type, Interface, Link Status (Up/Down), Port Activity (Port Enabled), Priority Setting (High or Normal), Speed Status (10Mbps, 100Mbps or 1000Mbps), Duplex Status (half duplex or full duplex), Auto Neg. (Enabled/Disabled), and VLAN.

**Statistics**

The packet data of this specific port will be displayed. Data include receive/ transmit packet count, receive/ transmit packet Byte count and error packet count. Users may press the refresh button to update all real-time messages.

**7.3 IP/ DHCP**

With an embedded DHCP server, it supports automatic IP assignment for LAN computers. (This function is similar to the DHCP service in NT servers.) It benefits users by freeing them from the inconvenience of recording and configuring IP addresses for each PC respectively. When a computer is turned on, it will acquire an IP address from the device automatically. This function is to make management easier.

**Enabled DHCP Server**

**DHCP Dynamic IP**

Client Lease Time  Minutes

Subnet :	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server :	Enabled	Disabled	Disabled	Disabled
IP Range Starts :	192.168.1.100	192.168.2.100	192.168.3.100	192.168.4.100
IP Range Ends :	192.168.1.149	192.168.2.149	192.168.3.149	192.168.4.149
MAC Addresses Pool for this IP Range :	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>	<input type="button" value="Pool Table"/>

**DNS**

DNS(Required) 1:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
DNS(Optional) 2:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>

**WINS**

WINS Server:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
--------------	---

**DHCP Dynamic IP**

Item	Description
<b>Enable DHCP Server</b>	Check the option to activate the DHCP server automatic IP lease function. If the function is activated, all PCs will be able to acquire IP automatically. Otherwise, users should configure static virtual IP for each PC individually.
<b>Client lease Time</b>	This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Users can change it according to their needs. The time unit is minute.
<b>Range Start</b>	This is an initial IP automatically leased by DHCP. It means DHCP will start the lease from this IP. The default initial IP is 192.168.1.100.
<b>Range End</b>	This is the end IP automatically leased by DHCP. The default initial IP is 192.168.1.149.

**DNS (Domain Name Service)**

This is for checking the DNS from which an IP address has been leased to a PC port. Input the IP address of this server directly.

Item	Description
<b>DNS (Required) 1</b>	Input the IP address of the DNS server.
<b>DNS (Optional) 2</b>	Input the IP address of the DNS server.

**WINS:**

If there is a WIN server in the network, users can input the IP address of that server directly.

Item	Description
<b>WINS Server</b>	Input the IP address of WINS.
<b>Apply</b>	Click " <b>Apply</b> " to save the network configuration modification.
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any changes.

## 7.4 DHCP Status


This is an indication list of the current status and setup record of the DHCP server. The indications are for the administrator's reference when a network modification is needed.

### Status

Subnet :	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server :	192.168.1.1	192.168.2.1	192.168.3.1	192.168.4.1
Dynamic IP Used :	1	0	0	0
Static IP Used :	0	0	0	0
DHCP Available :	49	50	50	50
Total :	50	50	50	50

### Client Table

Subnet1 ▾

Host Name	IP Address	MAC Address	Client Lease Time	Delete
NB97008	192.168.1.100	00:1f:c6:7b:8a:bd	4 Minutes, 42 Seconds	

Refresh

Item	Description
DHCP Server	This is the current DHCP IP.
Dynamic IP Used	The amount of dynamic IP leased by DHCP.
Static IP Used	The amount of static IP assigned by DHCP.
IP Available	The amount of IP still available in the DHCP server.
Total IP	The total IP which the DHCP server is configured to lease.
Host Name	The name of the current computer.
IP Address	The IP address acquired by the current computer.
MAC Address	The actual MAC network location of the current computer.
Client Lease Time	The lease time of the IP released by DHCP.
Delete	Remove a record of an IP lease.



## 7.5 IP & MAC Binding

Administrators can apply IP & MAC Binding function to make sure that users can not add extra PCs for Internet access or change private IP addresses.

### IP&MAC binding

Static IP :  .  .  .

MAC Address :  -  -  -  -  -

Name :

Enabled :

Block MAC address on the list with wrong IP address  
 Block MAC address not on the list

There are two methods for setting up this function:

### Block MAC address not on the list

This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access. When this method is applied, please fill out Static IP with 0.0.0.0, as the figure below:

IP&MAC binding

Show new IP user

Static IP : 0 . 0 . 0 . 0  
MAC Address : - - - - -  
Name :  
Enabled :

Add to list

Delete selected item

- Block MAC address on the list with wrong IP address
- Block MAC address not on the list

Apply Cancel

IP & MAC Binding

IP&MAC binding

Show new IP user

Static IP : 0 . 0 . 0 . 0  
MAC Address : - - - - -  
Name :  
Enabled :

Add to list

Delete selected item

- Block MAC address on the list with wrong IP address
- Block MAC address not on the list

Apply Cancel

Item	Description
<b>Static IP:</b>	There are two ways to input static IP: 1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a specific assigned IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty. 2. If users want DHCP to assign a static IP for a PC every single time, users should input the IP address users want to assign to this computer in the boxes. The server or PC which is to be bound will then acquire a static virtual IP whenever it restarts.
<b>MAC Address:</b>	Input the static real MAC (the address on the network card) for the server or PC which is to be bound.
<b>Name:</b>	For distinguishing clients, input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
<b>Enabled:</b>	Activate this configuration.
<b>Add to list:</b>	Add the configuration or modification to the list.
<b>Delete selected item:</b>	Remove the selected binding from the list.
<b>Add:</b>	Add new binding.

Block MAC address on the list with wrong IP address: When this option is activated, MAC addresses which are not included in the list will not be able to connect with the Internet.

### Show New IP user:

This function can reduce administrator's effort on checking MAC addresses one by one for the binding. Furthermore, it is easy to make mistakes to fill out MAC addresses on the list manually. By checking this list, administrator can see all MAC addresses which have traffic and are not bound yet. Also, if administrators find that one specific bound MAC address is shown on the list, it means that the user changes the private IP address.

IP & MAC binding List				Submit	Select All	Refresh	Close
IP Address	MAC Address	Name	Enable				
192.168.1.100	00:1f:c6:7b:8a:bd	<input type="text"/>	<input type="checkbox"/>				



Item	Description
<b>Name</b>	Input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
<b>Enabled</b>	Choose the item to be bound.
<b>Apply</b>	Activate the configuration.
<b>Select All</b>	Choose all items on the list for binding.
<b>Refresh</b>	Refresh the list.
<b>Close</b>	Close the list.

## 7.6 IP Grouping

IP Group function can combine several IP addresses or IP address ranges into several groups. When you manage user internet access privileges by IP address, you can set up every management functions for users who have same internet access privileges in the same IP group in order to decrease the effort of setting rules for each IP address. For example, you can choose to set up QoS or Access Rule by IP grouping. Thus, you will simplify setting rules.

IP Grouping consists of Local IP Group and Remote IP Group. Local IP Group refers to LAN IP groups, and remote IP Group refers to WAN IP groups. Local IP Group list will automatically learn IP addresses having packets that pass through firewall. Moreover, if user changes the IP address, the IP in the list will change accordingly well. For IP information which is in group list, it won't update automatically along with IP list of the left side. Administrators need to modify it manually.

Item	Description
<b>User Edit IP</b>	The IP list will show the list which learns the IP addresses automatically on the left under side. You can also modify IP addresses manually.
<b>Name</b>	Input the name of IP address (or range) showed below.
<b>IP Address</b>	Input IP address (or range). For example, 192.168.1.200 ~ 250.
<b>Add to IP List</b>	After setting name and IP address, push this button to add the information into the IP list below. If this IP (or range) is already in the list, you can not add it again.

<b>Local Group Set</b>	You can choose from the IP list on the left side to set up a local IP group.
<b>IP Group</b>	Choose IP Group that you would like to modify. If you would like to add new groups, please push "Add new group" button.
<b>Group Name</b>	When you add new groups, please note if the group name is in the column.
<b>Delete Group</b>	Choose the group that you would like to delete from the pull- down list, and push the "Delete Group" button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
 button	You can choose several IPs from IP list on the left side, and push this button to have them added into the group the right side.
<b>Delete</b> 	Delete self- defined IP or IP range.
<b>Apply</b>	Click "Apply" to save the network configuration modification
<b>Cancel</b>	Click "Cancel" to leave without making any changes.

**Remote IP Group Management:**

Basically, Remote IP Group setups are exactly the same as Local IP Group setups. However, remote IP group does not have automatically learning functions. Instead, you need to define addresses, ranges and groups manually. For example, 220.130.188.1 to 200 (range).

The screenshot displays the Remote IP Group Management interface. It is divided into two main sections: 'User Edit IP' and 'Remote Group Set'.

**User Edit IP:** This panel contains a 'Name' field, an 'IP Address' field with four input boxes separated by dots, and a 'to' field. An 'Add to IP list' button is located at the bottom right.

**Remote Group Set:** This panel features an 'IP Group' dropdown menu, an 'Add Group' button, and a 'Delete Group' button.

Below these panels are two empty IP lists. The left list is titled 'IP List' and has columns for 'Name', 'IP Address', 'Edit', and 'Delete'. The right list is titled 'Group Name' and has columns for 'Name', 'IP Address', and 'Delete'. A double arrow button (>>) is positioned between the two lists, indicating a transfer function.

It is the same setting methods. You should set the IP address or the range of remote IP from the left side first, and choose to add IP address information from the left side into the remote group.

## 7.7 Port Group Management

Service ports can be grouping as IP grouping. It is convenient to set QoS, firewall access rules, and other functions.

**user edit port**

Name :

Protocol : TCP

Port Range:  to

Port List


Name	Protocol	Port	Delete
All Traffic	BOTH	1~65535	
DNS	UDP	53~53	
FTP	TCP	21~21	
HTTP	TCP	80~80	
HTTP Secondary	TCP	8080~8080	
HTTPS	TCP	443~443	
HTTPS Secondary	TCP	8443~8443	
TFTP	UDP	69~69	
IMAP	TCP	143~143	
NNTP	TCP	119~119	
POP3	TCP	110~110	
SNMP	UDP	161~161	
SMTP	TCP	25~25	

**Port Group Set**

Group :

Group Name :

Name	Protocol	Port	Delete

Item	Description
<b>User edit port</b>	Input the name, protocol, and port range for the specific service port.
<b>Name</b>	Name the Port in order to identify its property. For example, Virus 135.
<b>Protocol</b>	Choose the port protocol form the pull down list like TCP, UDP or TCP and UDP.
<b>Port Range</b>	Input the port range. For example, 135 to 135.
<b>Add to Port List</b>	After setting name, protocol and port range, push this button to add the information into the Port list below. This port can be from some port groups.
<b>Group Name</b>	When you add new groups, please note if the group name is in the column. For example, Virus.
<b>Delete Group</b>	Choose the group that you would like to delete from the pull- down list, and push the "Delete Group" button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
 button	You can choose several ports from Port list on the left side, and push this button to have them added into the group the right side.
<b>Delete</b>	Delete self- defined port or port range.
<b>Apply</b>	Click "Apply" to save the network configuration modification

## Chapter 8: QoS (Quality of Service)

QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IP addresses to save bandwidth or provide priority to specific applications or services, and also to enable other users to share bandwidth, as well as to ensure stable and reliable network transmission. To maximize the bandwidth efficiency, network administrators should take account of the practical requirements of a company, a community, a building, or a café, etc., and modify bandwidth management according to the network environment, application processes or services.

### 8.1 Bandwidth Management

#### The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	10000	10000
WAN 2	10000	10000
WAN 3	10000	10000
WAN 4	10000	10000
USB	256	2048

#### Quality of Service

Interface:  WAN 1  WAN 2  WAN 3  WAN 4  USB

Service: All Traffic [TCP&UDP/1~65535] ▼

Service Management

IP Address ▼: 0 . 0 . 0 . 0 to 0

Direction: Upstream ▼

Mini. Rate:  Kbit/sec    Max. Rate:  Kbit/sec

Bandwidth sharing:   
 Share total bandwidth with all IP addresses.   
 Assign bandwidth for each IP address.

Enabled:

Move Up
Add to list
Move Down

Delete selected item

Enabled Smart QoS



## Exception IP address

Interface :  WAN 1  WAN 2  WAN 3  WAN 4  USB

Source IP  .  .  .  to / Group :  test

.  .  .

Direction :  Do not control upstream bandwidth  
 Do not control downstream bandwidth  
 Do not control bi-direction bandwidth

Enabled :




### 8.1.1 The Maximum Bandwidth provided by ISP

#### The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN 1	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 2	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 3	<input type="text" value="10000"/>	<input type="text" value="10000"/>
WAN 4	<input type="text" value="10000"/>	<input type="text" value="10000"/>
USB	<input type="text" value="256"/>	<input type="text" value="2048"/>

In the boxes for WAN1 and WAN2 bandwidth, input the upstream and downstream bandwidth which users applied for from bandwidth supplier. The bandwidth QoS will make calculations according to the data users input. In other words, it will guarantee a minimum rate of upstream and downstream for each IP and Service Port based on the total actual bandwidth of WAN1 and WAN2. For example, if the upstream bandwidths of both WAN1 and WAN2 are 512Kbit/Sec, the total upstream bandwidth will be: WAN1 + WAN2 = 1024Kbit/Sec. Therefore, if there are 50 IP addresses in the Intranet, the minimum guaranteed upstream bandwidth for each IP would be 1024Kbit/50=20Kbit/Sec. Thus, 20Kbit/Sec can be input for "Mini. Rate" Downstream bandwidth can be calculated in the same way.

**Attention**

The rules configured in Protocol Binding will be executed by the device according to their priorities too. The higher up on the list, the higher the priority of execution. The unit of calculation in this example is Kbit. Some software indicates the downstream/upstream speed with the unit KB. 1KB = 8Kbit.

### 8.1.2 QoS

To satisfy the bandwidth requirements of certain users, the device enables users to set up QoS with Rate Control method.

#### Rate Control

The network administrator can set up bandwidth or usage limitations for each IP or IP range according to the actual bandwidth. The network administrator can also set bandwidth control for certain Service Ports. A guarantee bandwidth control for external connections can also be configured if there is an internal server.

#### Quality of Service

Interface :  WAN 1  WAN 2  WAN 3  WAN 4  USB

Service : All Traffic [TCP&UDP/1-65535]

**Service Management**

IP Address : 0 . 0 . 0 . 0 to 0

Direction : Upstream


Mini. Rate :  Kbit/sec    Max. Rate :  Kbit/sec


Bandwidth sharing :  Share total bandwidth with all IP addresses.  
 Assign bandwidth for each IP address.

Enabled :

**Move Up**                      **Add to list**                      **Move Down**

**Delete selected item**

Item	Description
<b>Interface</b>	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
<b>Service Port</b>	Select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select "All (TCP&UDP) 1~65535". If only FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
<b>IP Address</b>	This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 150". The rule will control IP addresses from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input "0" in the boxes of IP address. This means all Intranet IP addresses will be restricted. QoS can also control the range of Class B.
<b>Direction</b>	<p><b>Upstream:</b> Means the upload bandwidth for Intranet IP.</p> <p><b>Downstream:</b> Means the download bandwidth for Intranet IP.</p> <p>Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server.</p> <p>Server in LAN, Downstream: If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.</p>
<b>Min. &amp; Max. Rate(Kbit/Sec)</b>	<p><b>The minimum bandwidth:</b> The rule is to guarantee minimum available bandwidth.</p> <p><b>The maximum bandwidth:</b> This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule.</p> <div data-bbox="504 1697 1430 1798" style="border: 1px solid black; padding: 5px;">  <b>Attention</b> The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit. </div>
<b>Bandwidth Assign Type</b>	<p><b>Sharing total bandwidth with all IP addresses:</b> If this option is selected, all IP addresses or Service Ports will share the bandwidth range (from minimum to maximum bandwidth).</p> <p>Assign bandwidth for each IP address: If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum.). For</p>

	<p>example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.</p> <div style="border: 1px solid black; padding: 5px;"> <p style="text-align: center;"> <b>Attention</b></p> <p>If “Share-Bandwidth” is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small.</p> <p>For example, if users do not want an FTP to occupy too much bandwidth, users can select the “Share-Bandwidth Mode”, so that no matter how much users use FTPs to download information, the total occupied bandwidth is fixed.</p> </div>
<b>Enable</b>	Activate the rule.
<b>Add to list</b>	Add this rule to the list.
<b>Move up &amp; Move down</b>	QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. Usually the service ports which need to be restricted, such as BT, e-mule, etc., will be moved to the bottom of the list. The rules for certain IP addresses would then be moved upward.
<b>Delete selected items</b>	Remove the rules selected from the Service List.
<b>Show Table</b>	Display all the Rate Control Rules users made for the bandwidth. Click “Edit” to modify.
<b>Apply</b>	Click “Apply” to save the configuration
<b>Cancel</b>	Click “Cancel” to leave without making any change.

### Show Table

Summary										
Service	IP Address	Direction	Mini. Rate (Kbit/sec)	Max. Rate (Kbit/sec)	Bandwidth sharing	Enabled	Interface (WAN)	Edit		
<div style="text-align: right;"> <input checked="" type="radio"/> Rule    <input type="radio"/> Interface    Refresh    Close         </div>										

### 8.1.3 Smart QoS

**Enabled Smart QoS**

When the utility of any wan's bandwidth is over than  %, Enable Smart QoS(0: Always Enabled)

Each IP's upstream bandwidth threshold :  Kbit/sec

Each IP's downstream bandwidth threshold :  Kbit/sec

Each IP's Maximum bandwidth :

Upstream (WAN 1 :  Kbit/sec WAN 2 :  Kbit/sec  
 WAN 3 :  Kbit/sec WAN 4 :  Kbit/sec)  
 (USB :  Kbit/sec)

Downstream (WAN 1 :  Kbit/sec WAN 2 :  Kbit/sec  
 WAN 3 :  Kbit/sec WAN 4 :  Kbit/sec)  
 (USB :  Kbit/sec)

Penalty mechanism

Item	Description
<b>Enabled QoS</b>	Choose to apply QoS function.
<b>When the usage of any WAN's bandwidth is over___%, Enable Smart QoS</b>	Input the required rate value into the column. The default is 60%.
<b>Each IP's upstream bandwidth threshold (for all WAN)</b>	Input the max. upstream rate for intranet IPs.
<b>Each IP's downstream bandwidth threshold (for all WAN)</b>	Input the max. downstream rate for intranet IPs.
<b>If any IP's bandwidth is over maximum threshold, its maximum bandwidth will remain</b>	When any IP uses more bandwidth than the above upstream or downstream settings, the IP will be restricted for the following upstream or downstream bandwidth settings.
<b>Enabled Penalty Mechanism</b>	After choosing "Enabled Penalty Mechanism", the device will enable the penalty conditions internally. When the IP still uses more upstream or downstream bandwidth than the setting, the device will execute the penalty conditions automatically.
<b>Show Penalty List</b>	The IPs which are under penalty mechanism will be shown on the list.
<b>Scheduling</b>	If "Always" is selected, the rule will be executed around the clock. If "From..." is selected, the rule will be executed according to the configured time range. For example, if the time control is from

	Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.
--	---

**Advanced**

When the usage of certain WAN's bandwidth is under  %, then stop to add new punished IP

Enabled Session Control Mechanism

Every  second to detect whether internal IP's bandwidth are over than limit

If the punished IP still keep upper bounded limit on, then decrease its bandwidth to  %

When the usage of all WANs' bandwidth are lower than  % disable Smart QoS, and after  minutes to release punished IP

Item	Description
<b>When the usage of certain WAN's bandwidth is under __%, then stop to add new punished IP</b>	When the usage of certain WAN's bandwidth is under __%, will stop to punish the IP which is over the limit. While the bandwidth is over the certain percentage, penalty mechanism will be activated.
<b>Every __ second to detect whether internal IP's bandwidth are over than limit</b>	Detect usage of internal IP's bandwidth every __ second.
<b>If the punished IP still keep upper bounded limit on, then decrease its bandwidth to __%</b>	If the punished IP still keep over the limit, the limit badwidth will be decrease to __%.
<b>When the usage of all WANs' bandwidth are lower than __% disable Smart QoS, and after __minutes to release punished IP</b>	Smart QoS will be disabled when the usage of bandwidth is lower than __%. Punished IP will be released after __minute.

### 8.1.4 Exception IP address

If some users are allowed to avoid traffic management control, you can use this function to fulfill the requirement.

#### Exception IP address

Interface :  WAN 1  WAN 2  WAN 3  WAN 4  USB

Source IP  .  .  .  to / Group : test

Direction :  Do not control upstream bandwidth  
 Do not control downstream bandwidth  
 Do not control bi-direction bandwidth

Enabled :

Add to list

Delete selected item

Show Table Apply Cancel

Item	Description
WAN	Select WAN ports.
Source IP	Enter the exempted IP range, or select the exempted IP group.
Do not control Direction	Select do not control upload, download, or both of them.
Enabled	Enable this policy.
Add to List	Add this policy into the exempted list.
Delete Selected item	Delete selected list.
Apply	Click <b>“Apply”</b> button to saving configuration.
Cancel	Click <b>“Cancel”</b> button to reject modification.

## 8.2 Session control

Session management controls the acceptable maximum simultaneous sessions of Intranet PCs. This function is very useful for managing connection quantity when P2P software such as BT, Thunder, or emule is used in the Intranet causing large numbers of sessions. Setting up proper limitations on sessions can effectively control the sessions created by P2P software. It will also have a limiting effect on bandwidth usage.

In addition, if any Intranet PC is attacked by a virus like Worm.Blaster and sends a huge number of session requests, session control will restrict that as well.

### Session Control and Scheduling

#### Session Control

<input checked="" type="radio"/> Disabled	
<input type="radio"/> Single IP cannot exceed <input type="text" value="200"/> Session	
<input type="radio"/> Single IP cannot exceed TCP <input type="text" value="100"/> , UDP <input type="text" value="100"/> Session	
<input type="radio"/> When single IP exceed <input type="text" value="200"/> Session	<input type="radio"/> block this IP's new sessions for <input type="text" value="5"/> minutes
	<input type="radio"/> block this IP's all sessions for <input type="text" value="5"/> minutes

#### Scheduling

Apply this rule <input type="text" value="Always"/> <input type="button" value="v"/>	<input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="23"/> : <input type="text" value="59"/> (24-Hour Format)
<input checked="" type="checkbox"/> Everyday	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat

Item	Description
<b>Disabled</b>	Disable Session Control function.
<b>Single IP cannot exceed __ session</b>	This option enables the restriction of maximum external sessions to each Intranet PC. When the number of external sessions reaches the limit, to allow new sessions to be built, some of the existing sessions must be closed. For example, when BT or P2P is being used to download information and the sessions exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.
<b>When single IP exceed __</b>	<p><input checked="" type="radio"/> block this IP's new sessions for <input type="text" value="5"/> minutes</p> <p>If this function is selected, when the user's port session reach the limit, this user will not be able to make a new session for five minutes. Even if the previous session has been closed, new sessions cannot be made until the setting time ends.</p> <p><input type="radio"/> block this IP's all sessions for <input type="text" value="5"/> minutes</p> <p>If this function is selected, when the user's port connections reach the limit, all the</p>



	lines that this user is connected with will be removed, and the user will not be able to connect with the Internet for five minutes. New connections cannot be made until the delay time ends.
<b>Scheduling</b>	If "Always" is selected, the rule will be executed around the clock. If "From..." is selected, the rule will be executed according to the configured time range. For example, if the time control is from Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.
<b>Apply</b>	Click "Apply" to save the configuration.
<b>Cancel</b>	Click "Cancel" to leave without making any change.

## Exempted Service Port or IP Address

### Exempted Service Port or IP Address

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Source IP : . . . 0 to 0

Enabled :

Maximum connections limit :  Unlimited  Not exceed 300

Add to list

Delete selected item

Item	Description
<b>Service Port</b>	Choose the service port.
<b>IP Address</b>	Input the IP address range or IP group.
<b>Enabled</b>	Activate the rule.
<b>Add to list</b>	Add this rule to the list.
<b>Delete selected item</b>	Remove the rules selected from the Service List.
<b>Apply</b>	Click " <b>Apply</b> " to save the configuration.
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any change.

## Chapter 9 : Firewall

This chapter introduces firewall general policy, access rule, and content filter settings to ensure network security.

### 9.1 General Policy

The firewall is enabled by default. If the firewall is set as disabled, features such as SPI, DoS, and outbound packet responses will be turned off automatically. Meanwhile, the remote management feature will be activated. The network access rules and content filter will be turned off.

#### General Policy

Firewall	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
SPI (Stateful Packet Inspection)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
DoS (Denial of Service)	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Advanced Function
Block WAN Request	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	
Remote Management	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	Port 8080
Multicast Pass Through	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled	
Prevent ARP Virus Attack	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled	Router sends ARP 5 times per-second.

Apply Cancel

Item	Description
<b>Firewall</b>	This feature allows users to turn on/off the firewall.
<b>SPI (Stateful Packet Inspection)</b>	This enables the packet automatic authentication detection technology. The Firewall operates mainly at the network layer. By executing the dynamic authentication for each connection, it will also perform an alarming function for application procedure. Meanwhile, the packet authentication firewall may decline the connections which use non-standard communication protocol.
<b>DoS (Denial of Service)</b>	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and so on.
<b>Block WAN request</b>	If set as Enabled, then it will shut down outbound ICMP and abnormal packet responses in connection. If users try to ping the WAN IP from the external, this will not work because the default value is set as activated in order to decline the outbound responses.
<b>Remote Management</b>	To enter the device web- based UI by connecting to the remote Internet, this feature must be activated. In the field of remote browser IP, a valid external IP address (WAN IP) for the device should be filled in and the modifiable default control port should be adjusted (the default is set to 80, modifiable).
<b>Multicast Pass</b>	There are many audio and visual streaming media on the network. Broadcasting

<b>Through</b>	may allow the client end to receive this type of packet message format. This feature is off by default.
<b>Prevent ARP Virus Attack</b>	This feature is designed to prevent the intranet from being attacked by ARP spoofing, causing the connection failure of the PC. This ARP virus cheat mostly occurs in Internet cafes. When attacked, all the online computers disconnect immediately or some computers fail to go online. Activating this feature may prevent the attack by this type of virus.

### Advanced Setting

**Advance DoS Settings**

Packet Type	WAN Threshold	LAN Threshold
<input checked="" type="checkbox"/> TCP SYN Flood	Threshold counted by all packets <input type="text" value="15000"/> Packets/Sec	Threshold counted by all packets <input type="text" value="50000"/> Packets/Sec
		Single Destination IP Threshold <input type="text" value="5000"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="1000"/> Packets/Sec	Single Source IP Threshold <input type="text" value="5000"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="50"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input checked="" type="checkbox"/> UDP_Flood	Threshold counted by all packets <input type="text" value="15000"/> Packets/Sec	Threshold counted by all packets <input type="text" value="50000"/> Packets/Sec
		Single Destination IP Threshold <input type="text" value="5000"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="1000"/> Packets/Sec	Single Source IP Threshold <input type="text" value="5000"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="50"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input checked="" type="checkbox"/> ICMP_Flood	Threshold counted by all packets <input type="text" value="200"/> Packets/Sec	Threshold counted by all packets <input type="text" value="200"/> Packets/Sec
		Single Destination IP Threshold <input type="text" value="200"/> Packets/Sec
	Threshold counted by single IP packet <input type="text" value="50"/> Packets/Sec	Single Source IP Threshold <input type="text" value="50"/> Packets/Sec
	Block this IP when reach threshold <input type="text" value="5"/> Minutes	Block this IP when reach threshold <input type="text" value="1"/> Minutes
<input type="checkbox"/> Exception Source IP		IP Add <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> to /Group <input type="text" value="test"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		IP Add <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> to /Group <input type="text" value="test"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
<input type="checkbox"/> Exception Destination IP		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
		<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Firewall/DoS Log
Show Blocked IP
Apply
Cancel

Item	Description
<b>Packet Type</b>	This device provides three types of data packet transmission: TCP-SYN-Flood, UDP-Flood and ICMP-Flood.
<b>WAN Threshold</b>	When all packet values from external attack or from single external IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes ( the default is 5 minutes OBJ 176 ). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.
<b>LAN Threshold</b>	When all packet values from internal attack or from single internal IP attack reach the maximum amount (the default is 15000 packets/Sec and 2000 packets/Sec respectively), if these conditions above occurs, the IP will be blocked for 5 minutes (the default is 5 minutes). Users can adjust the threshold value and the blocking duration to effectively deal with external attack. The threshold value should be adjusted from high to low.
<b>Exempted Source IP</b>	Input the exempted source IP.
<b>Exempted Dest. IP</b>	Input the exempted Destination IP addresses.
<b>Apply</b>	Click " <b>Apply</b> " to save the configuration.
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any change.

### Firewall / DoS Log

**System Log**  
 Current Time: Fri Mar 4 17:36:25 2011 Firewall/DoS Log ▼ Refresh Close

Time ▲	Event-Type	Message

Show the Firewall/Log.

### Show Blocked IP

**Summary** Refresh Close

IP Address	Time(sec)

Show the blocked IP list and the remained blocked time.

## 9.2 Access Rule

Users may turn on/off the setting to permit or forbid any packet to access internet. Users may select to set different network access rules: from internal to external or from external to internal. Users may set different packets for IP address and communication port numbers to filter Internet access rules.

Network access rule follows IP address, destination IP address, and IP communications protocol status to manage the network packet traffic and make sure whether their access is allowed by the firewall.

### 9.2.1 Default Rule

The device has a user-friendly network access regulatory tool. Users may define network access rules. They can select to enable/ disable the network so as to protect all internet access. The following describes the internet access rules:

- All traffic from the LAN to the WAN is allowed - by default.
- All traffic from the WAN to the LAN is denied - by default.
- All traffic from the LAN to the DMZ is allowed - by default.
- All traffic from the DMZ to the LAN is denied - by default.
- All traffic from the WAN to the DMZ is allowed - by default.
- All traffic from the DMZ to the WAN is allowed - by default.

Users may define access rules and do more than the default rules. However, the following four extra service items are always on and are not affected by other user-defined settings.

- \* HTTP Service (from LAN to Device) is on by default (for management)
- \* DHCP Service (from LAN to Device) is set to on by default (for the automatic IP retrieval)
- \* DNS Service (from LAN to Device) is on by default (for DNS service analysis)
- \* Ping Service (from LAN to Device) is on by default (for connection and test)

### Access Rule

Jump to  /Page  entries per page [Next Page>>](#)

Priority	Enabled	Action	Service	Source Interface	Source	Destination	Time	Day	Edit	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN3	Any	Any	Always			

Add New Rule

Restore Default Rules

In addition to the default rules, all the network access rules will be displayed as illustrated above. Users may follow or self-define the priority of each network access rule. The device will follow the rule priorities one by one, so please make sure the priority for all the rules can suit the setting rules.

Item	Description
<b>Edit:</b>	Define the network access rule item
<b>Delete:</b>	Remove the item.
<b>Add New Rule:</b>	Create a new network access rule
<b>Return to Default Rule:</b>	Restore all settings to the default values and delete all the self-defined settings.

## 9.2.2 Add New Access Rule

### Service

Action :	Allow	
Service :	All Traffic [TCP&UDP/1-65535]	Service Management
Log :	No log	
Source Interface :	LAN	
Source IP :	ANY	
Dest. IP :	ANY	

### Scheduling

Apply this rule	Always		:		to		:		(24-Hour Format)						
<input type="checkbox"/>	Everyday	<input type="checkbox"/>	Sun	<input type="checkbox"/>	Mon	<input type="checkbox"/>	Tue	<input type="checkbox"/>	Wed	<input type="checkbox"/>	Thu	<input type="checkbox"/>	Fri	<input type="checkbox"/>	Sat

Item	Description
<b>Action</b>	Allow: Permits the pass of packets compliant with this control rule. Deny: Prevents the pass of packets not compliant with this control rule.
<b>Service Port</b>	From the drop-down menu, select the service that users grant or do not give permission.
<b>Service Port Management</b>	If the service that users wish to manage does not exist in the drop-down menu, press – Service Management to add the new service. From the pop-up window, enter a service name and communications protocol and port, and then click the “Add to list” button to add the new service.
<b>Log</b>	No Log: There will be no log record. Create Log when matched: Event will be recorded in the log.
<b>Interface</b>	Select the source port whether users are permitted or not (for example: LAN, WAN1,

	WAN2 or Any). Select from the drop-down menu.
<b>Source IP</b>	Select the source IP range (for example: Any, Single, Range, or preset IP group name). If Single or Range is selected, please enter a single IP address or an IP address within a session.
<b>Dest. IP</b>	Select the destination IP range (such as Any, Single, Range, or preset IP group name) If Single or Range is selected; please enter a single IP address or an IP address within a session.
<b>Scheduling</b>	Select "Always" to apply the rule on a round-the-clock basis. Select "from", and the operation will run according to the defined time.
<b>Apply this rule</b>	Select "Always" to apply the rule on a round-the-clock basis. If "From" is selected, the activation time is introduced as below
<b>... to ...</b>	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)
<b>Day Control</b>	"Everyday" means this period of time will be under control everyday. If users only certain days of a week should be under control, users may select the desired days directly.
<b>Apply</b>	Click "Apply" to save the configuration.
<b>Cancel</b>	Click "Cancel" to leave without making any change.

### 9.3 URL Filter

The device supports two webpage restriction modes: one is to block certain forbidden domains, and the other is to give access to certain web pages. Only one of these two modes can be selected.

- Block Forbidden Domains
- Accept Allowed Domains

- Forbidden Domains Enabled
- Enable Website Blocking by Domain Keywords

#### Block Forbidden Domain

Fill in the complete website such as www.sex.com to have it blocked.

- Block Forbidden Domains
- Accept Allowed Domains

- Forbidden Domains Enabled

#### Forbidden Domains

Item	Description
<b>Domain Name</b>	Enter the websites to be controlled such as www.playboy.com
<b>Add to list</b>	Click "Add to list" to create a new website to be controlled.
<b>Delete selected item</b>	Click to select one or more controlled websites and click this option to delete.



## Website Blocking by Keywords

Enable Website Blocking by Domain Keywords

### Website Blocking by Domain Keywords

Keywords

Add

Exception IP address v :  .  .  .  to

Group v test v IP Grouping

Add to list

Delete selected keywords

Item	Description
<b>Enabled</b>	Click to activate this feature. The default setting is disabled. For example: If users enter the string "sex", any websites containing "sex" will be blocked.
<b>Keywords ( Only for English keyword )</b>	Enter keywords.
<b>Add to List</b>	Add this new service item content to the list.
<b>Delete selected item</b>	Delete the service item content from the list
<b>Apply</b>	Click "Apply" to save the modified parameters.
<b>Cancel</b>	Click "Cancel" to cancel all the changes made to the parameters.

### Accept Allowed Domains

In some companies or schools, employees and students are only allowed to access some specific websites. This is the purpose of the function.

- Block Forbidden Domains
- Accept Allowed Domains

Allowed Domains Enabled

#### Allowed Domains

Item	Description
Enabled	Activate the function. The default setting is “Disabled.”
Domain Name	Input the allowed domain name, etc. www.google.com
Add to list	Add the rule to list.
Delete selected item	Users can select one or more rules and click to delete.
Apply	Activate the function. The default setting is “Disabled.”

### Content Filter Scheduling

Select “**Always**” to apply the rule on a round-the-clock basis. Select “**from**”, and the operation will run according to the defined time. For example, if the control time runs from 8 a.m. to 6 p.m., Monday to Friday, users may control the operation according to the following illustrated example.

#### Scheduling

---

Item	Description
<b>Always:</b>	Select " <b>Always</b> " to apply the rule on a round-the-clock basis. Select " <b>from</b> ", and the operation will run according to the defined time.
<b>...to...:</b>	Select " <b>Always</b> " to apply the rule on a round-the-clock basis. If " <b>From</b> " is selected, the activation time is introduced as below
<b>Day Control:</b>	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)

## Chapter 10 : VPN (Virtual Private Network)

### 10.1. Display All VPN Summary

#### Summary

PPTP Tunnel Number :	<input type="text" value="0"/> Tunnel(s) Used	<input type="text" value="60"/> Tunnel(s) Available	<a href="#">Detail</a>
VPN Tunnel Number :	<input type="text" value="0"/> Tunnel(s) Used	<input type="text" value="200"/> Tunnel(s) Available	<a href="#">Detail</a>

#### VPNTunnel(s)Status

Jump to  / Page  entries per page

No.	Account ID	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Control	Config.
-----	------------	--------	------------------------	----------------	-----------------	-------------------	---------	---------

This VPN Summary displays the real-time data with regard to VPN status. These data include: all tunnel numbers, setting parameters and Group VPN and so forth.

#### Summary

PPTP Tunnel Number :	<input type="text" value="0"/> Tunnel(s) Used	<input type="text" value="60"/> Tunnel(s) Available	<a href="#">Detail</a>
VPN Tunnel Number :	<input type="text" value="0"/> Tunnel(s) Used	<input type="text" value="200"/> Tunnel(s) Available	<a href="#">Detail</a>

**Detail:** Push this button to display the following information with regard to all current VPN configurations to facilitate VPN connection management.

WAN1 IP: 0.0.0.0 WAN2 IP: 0.0.0.0 WAN3 IP: 0.0.0.0 WAN4 IP:  
0.0.0.0 WAN5 IP: 0.0.0.0

No.	Account ID	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway
1	TEST1	waiting for connection	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.1.0 255.255.255.0	192.168.1.1

Close


**VPN Tunnel Status:**

The following describes VPN Tunnel Status, the current status of VPN tunnel in detail:




**VPNTunnel(s) Status**

1 Tunnel(s) Enabled      1 Tunnel(s) Defined

Jump to  / Page       entries per page

No.	Account ID	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Control	Config.
1	TEST1	waiting for connection	DES/MD5/1	192.168.1.0 255.255.255.0	192.168.1.0 255.255.255.0	192.168.1.1	<a href="#">Connect</a>	<a href="#">Edit</a> 

[Add Tunnel\(s\)](#)

Item	Description		
<b>Previous Page/Next Page, Jump to __/__ Page, __ Entries Per Page</b>	Click Previous page or Next page to view the desired VPN tunnel page. Or users can select the page number directly to view all VPN tunnel statuses, such as 3, 5, 10, 20 or All.		
<b>Tunnel No.</b>	To set the embedded VPN feature, please select the tunnel number. It supports up to 300 IPsec VPN tunnel Setting (gateway to gateway as well as client to gateway).		
<b>Status</b>	Successful connection is indicated as-(Connected). Failing hostname resolution is indicated as - (Hostname Resolution Failed). Resolving hostname is indicated as -(Resolving Hostname) Waiting to be connected is indicated as - (Waiting for Connection). If users select Manual setting for IPsec setup, the status message will display as "Manual" and there is no Tunnel test function available for this manual setting.		
<b>Account ID:</b>	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion should users have more than one tunnel settings. <table border="1" style="width: 100%; margin-top: 10px;"> <tr> <td style="text-align: center;"> <b>Note</b></td> <td>If this tunnel is to be connected to other VPN device (not this device), some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.</td> </tr> </table>	 <b>Note</b>	If this tunnel is to be connected to other VPN device (not this device), some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.
 <b>Note</b>	If this tunnel is to be connected to other VPN device (not this device), some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.		
<b>Phase2 Encrypt/Auth/Group:</b>	Displays settings such as encryption (DES/3DES), authentication (MD5/SHA1) and Group (1/2/5). If users select Manual setting for IPsec, Phase 2 DH group will not display.		
<b>Local Group</b>	Displays the setting for VPN connection secure group of the local end.		
<b>Remote Group</b>	Displays the setting for remote VPN connection secure group.		

<b>Remote Gateway</b>	Set the IP address to connect the remote VPN device. Please set the VPN device with a valid IP address or domain name.
<b>Control</b>	Click "Connect" to verify the tunnel status. The test result will be updated. To disconnect, click "Disconnect" to stop the VPN connection.
<b>Config</b>	Setting items include Edit and Delete icon. Click on Edit to enter the setting items and users may change the settings. Click on the trash bin icon and all the tunnel settings will be deleted.
<b>__ Tunnel(s) Enabled</b> <b>__ Tunnel(s) Defined</b>	This displays how many tunnels are enabled and how many tunnels are set.

### VPN Group Status:

If there is no setting for Group VPN, there will be no display of VPN Group status.

#### VPNGroupStatus

GroupName	ConnectedTunnel (s)	Phase2 Enc/Auth/Grp	Local Group	Remote Client	Remote ClientStatus	Control	Config.
-----------	---------------------	---------------------	-------------	---------------	---------------------	---------	---------

AddTunnel(s)

Item	Description
<b>Group Name</b>	Displays the tunnel name of the Group VPN that is connected.
<b>Connected Tunnels</b>	Displays the VPN Groups tunnel numbers.
<b>Phase2 Encrypt/Auth/DH</b>	Displays settings such as encryption (DES/3DES), authentication (MD5/SHA1) and Group (1/2/5).If users select Manual setting for IPsec, Phase 2 DH group will not be displayed.
<b>Local Group</b>	Displays the VPN connection secure setting for the local group.
<b>Remote Client</b>	Displays the name of this group for remote VPN Connection secure group setting.
<b>Remote Client Status</b>	Click on <b>Detail List</b> , and more information such as Group Name, IP address and the connection time will be displayed.
<b>Control</b>	Click <b>Connect</b> to verify the status of the tunnel. The test result will be updated in this status.
<b>Config</b>	As illustrated below, configurations include Edit and Delete icon. Click on <b>Edit</b> to enter the setting items to be changed. Click on the trash bin icon , and all the tunnel settings will be deleted.

### 10.1.1. Add a New VPN Tunnel

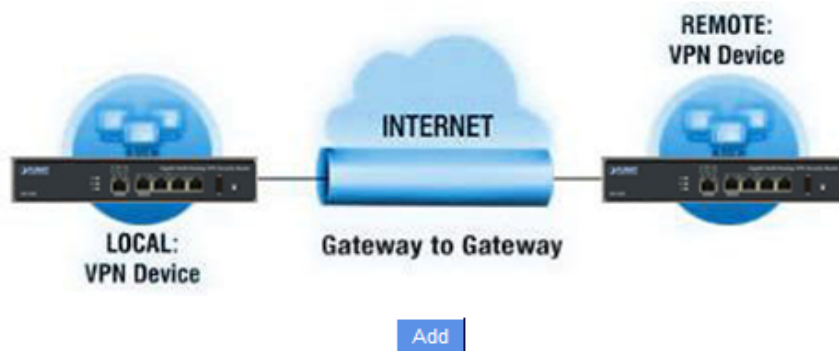
The device supports Gateway to Gateway tunnel or Client to Gateway tunnel.

The VPN tunnel connections are done by 2 VPN devices via the Internet. When a new tunnel is added, the setting page for Gateway to Gateway or Client to Gateway will be displayed.

#### Gateway to Gateway

Click "Add" to enter the setting page of Gateway to Gateway.

##### [Gateway to Gateway](#)



#### Client to Gateway

Click "Add" to enter the setting page of Client to Gateway.


##### [Client to Gateway](#)



The following instructions will guide users to set a VPN tunnel between two devices.

#### 10.1.1.1 Gateway to Gateway Setting

Tunnel(s) No.	<input type="text" value="1"/>
Tunnel(s) Name :	<input type="text"/>
Interface:	<input type="text" value="WAN 1"/>
Enabled :	<input checked="" type="checkbox"/>

Item	Description
<b>Tunnel No.</b>	Set the embedded VPN feature, please select the Tunnel number.
<b>Tunnel Name</b>	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  <b>Note</b> If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled. </div>
<b>Interface</b>	From the pull-down menu, users can select the Interface for this VPN tunnel.
<b>Enabled</b>	Click to activate the VPN tunnel. This option is set to activate by default. Afterwards, users may select to activate this tunnel feature.

## Local VPN Group Setting

### Local VPN Group Setting

Local Security Gateway Type:	IP Only
IP Address:	0 . 0 . 0 . 0
Local Security Group Type:	Subnet
IP Address:	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0

This Local Security Gateway Type must be identical with that of the remote type (Remote Security Gateway Type).

Item	Description
<b>Local Security</b>	This local gateway authentication type comes with five operation modes, which are:
<b>Gateway Type</b>	<p>IP only IP + Domain Name (FQDN) Authentication  IP + E-mail Addr. (USER FQDN) Authentication Dynamic IP + Domain Name (FQDN) Authentication Dynamic IP + E-mail Addr. (USER FQDN) Authentication. Dynamic IP address + Email address name</p> <p><b>(1) IP only:</b>  If users decide to use IP only, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> Local Security Gateway Type: IP Only  IP Address: 0 . 0 . 0 . 0 </div> <p><b>(2) IP + Domain Name(FQDN) Authentication:</b>  If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do</p>



further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.

Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address:	0 . 0 . 0 . 0
Domain Name:	

**(3) IP + E-mail Addr. (USER FQDN) Authentication.**

If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Local Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address:	0 . 0 . 0 . 0
E-mail:	@

**(4) Dynamic IP + Domain Name(FQDN) Authentication:**

If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.

Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name:	

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.**

If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; If users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.

Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication
E-mail:	@

**Local Security Group Type**

This option allows users to set the local VPN connection access type. The following offers a few items for local settings. Please select and set appropriate parameters:  
 1. IP address This option allows the only IP address which is entered to build the VPN tunnel.

Local Security Group Type:	IP Address
IP Address:	192 . 168 . 1 . 0

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

**2. Subnet**

This option allows local computers in this subnet can be connected to the VPN tunnel.

<b>Local Security Group Type:</b>	Subnet <input type="button" value="v"/>
<b>IP Address:</b>	192 . 168 . 1 . 0
<b>Subnet Mask:</b>	255 . 255 . 255 . 0

Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

## Remote Group Setup

### Remote VPN Group Setting

Remote Security Gateway Type:	IP Only
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Remote Security Group Type:	Subnet
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask:	255 . 255 . 255 . 0

This remote gateway authentication type (Remote Security Gateway Type) must be identical to the remotely-connected local security gateway authentication type (Local Security Gateway Type).

Item	Description								
Remote Security Gateway Type	<p>This remote gateway authentication type comes with five operation modes, which are:  <b>IP only</b>-Authentication by use of IP only <b>IP + Domain Name (FQDN) Authentication</b>, -IP + Domain name <b>IP + E-mail Addr. (USER FQDN) Authentication</b>, -IP + Email address <b>Dynamic IP + Domain Name (FQDN) Authentication</b>, -Dynamic IP address + Domain name <b>Dynamic IP + E-mail Addr. (USER FQDN) Authentication</b>. Dynamic IP address + Email address name</p> <p><b>(1) IP only:</b>                      If users select the IP Only type, entering this IP allows users to gain access to this tunnel.</p> <div data-bbox="406 1227 1430 1323" data-label="Form"> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>IP Only</td> </tr> <tr> <td>IP Address</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> </table> </div> <p>If the IP address of the remote client is unknown, choose IP by DNS Resolved, allowing DNS to translate IP address. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.</p> <div data-bbox="406 1514 1430 1610" data-label="Form"> <table border="1"> <tr> <td>Remote Security Gateway Type:</td> <td>IP Only</td> </tr> <tr> <td>IP by DNS Resolved</td> <td><input type="text"/></td> </tr> </table> </div> <p><b>(2) IP + Domain Name(FQDN) Authentication:</b>                      If users select IP + domain name, please enter IP address and the domain name to be verified. FQDN refers to the combination of host name and domain name. Users may enter any name that corresponds to the domain name of FQDN. This IP address and domain name must be identical to those of the remote VPN security gateway setting type to establish successful connection.</p>	Remote Security Gateway Type:	IP Only	IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Remote Security Gateway Type:	IP Only	IP by DNS Resolved	<input type="text"/>
Remote Security Gateway Type:	IP Only								
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>								
Remote Security Gateway Type:	IP Only								
IP by DNS Resolved	<input type="text"/>								

Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Domain Name:	<input type="text"/>

If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translate the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

Remote Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP by DNS Resolved	<input type="text"/>
Domain Name:	<input type="text"/>

**(3) IP + E-mail Addr. (USER FQDN) Authentication:**

If users select IP address and E-mail type, entering the IP address and the E-mail allows users to gain access to this tunnel.

Remote Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
E-mail:	<input type="text"/> @ <input type="text"/>

If the remote IP address is unknown, choose IP by DNS Resolved, allowing DNS to translated the IP address. This domain name must be available on the Internet. When users finish the setting, the corresponding IP address will be displayed under the remote gateway of Summary.

Remote Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP by DNS Resolved	<input type="text"/>
E-mail:	<input type="text"/> @ <input type="text"/>

**(4) Dynamic IP + Domain Name(FQDN) Authentication:**

If users use dynamic IP address to connect with the device, users may select the combination of the dynamic IP address, host name and domain name.

Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name:	<input type="text"/>

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.**

If users use dynamic IP address to connect with the device, users may select this type to link to VPN. When the remote VPN gateway requires connection to facilitate VPN connection, the device will start authentication and respond to the VPN tunnel connection; Please enter the E-Mail to the empty space.

Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication
E-mail:	<input type="text"/> @ <input type="text"/>

<b>Remote Security</b>	This option allows users to set the remote VPN connection access type. The following
------------------------	--

<b>Group Type</b>	<p>offers a few items for remote settings. Please select and set appropriate parameters:</p> <p><b>(1) IP address</b> This option allows the only IP address which is entered to build the VPN tunnel.</p> <div data-bbox="408 349 1401 470"> <table border="1"> <tr> <td>Remote Security Group Type:</td> <td>IP Address ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> </table> </div> <p>Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.2.1 can establish connection.</p> <p><b>(2) Subnet</b> This option allows local computers in this subnet can be connected to the VPN tunnel.</p> <div data-bbox="408 674 1401 860"> <table border="1"> <tr> <td>Remote Security Group Type:</td> <td>Subnet ▾</td> </tr> <tr> <td>IP Address:</td> <td><input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></td> </tr> <tr> <td>Subnet Mask:</td> <td>255 . 255 . 255 . 0</td> </tr> </table> </div> <p>Reference: When this VPN tunnel is connected, only computers with the session of 192.168.2.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.</p>	Remote Security Group Type:	IP Address ▾	IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Remote Security Group Type:	Subnet ▾	IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Subnet Mask:	255 . 255 . 255 . 0
Remote Security Group Type:	IP Address ▾										
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>										
Remote Security Group Type:	Subnet ▾										
IP Address:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>										
Subnet Mask:	255 . 255 . 255 . 0										

## IPSec Setup

If there is any encryption mechanism, the encryption mechanism of these two VPN tunnels must be identical in order to create connection. And the transmission data must be encrypted with IPSec key, which is known as the encryption "key". The device provides the IKE automatic encryption mode- IKE with Preshared Key (automatic).

## Encryption Management Protocol

When users set this VPN tunnel to use authentication mode, users must set the parameter of this exchange password with that of the remote

## IPSec Setting

Keying Mode:	IKE with Preshared Key ▾
Phase1 DHGroup :	Group 1 ▾
Phase1 Encryption:	DES ▾
Phase1 Authentication:	MD5 ▾
Phase1 SA Life Time:	0 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DHGroup :	Group 1 ▾
Phase2 Encryption:	DES ▾
Phase2 Authentication:	MD5 ▾
Phase2 SA Life Time:	0 seconds
Preshared Key:	<input type="text"/>

Advanced +

### Use IKE Protocol

Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the key will not be able to get the Phase 2 key in such a short period of time.

Item	Description
<b>Perfect Forward Secrecy:</b>	When users check the PFS option don't forget to activate the PFS function of the VPN device and the VPN Client as well.
<b>Phase 1/ Phase 2 DH Group</b>	This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
<b>Phase 1/ Phase 2 Encryption</b>	This option allows users to set this VPN tunnel to use any encryption mode. Note that this parameter must be identical to that of the remote encryption parameter: DES (64-bit encryption mode), 3DES (128-bit encryption mode), AES (the standard of using security code to encrypt information). It supports 128-bit, 192-bit, and 256-bit encryption keys.
<b>Phase 1/Phase 2 Authentication</b>	This authentication option allows users to set this VPN tunnel to use any authentication mode. Note that this parameter must be identical to that of the remote authentication mode: "MD5" or "SHA1".
<b>Phase 1 SA Life Time</b>	The life time for this exchange code is set to 28800 seconds (or 8hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
<b>Phase2 SA Life Time</b>	The life time for this exchange code is set to 3600 seconds (or 1hours) by default. This allows the automatic generation of other exchange password within the valid time of the

	VPN connection so as to guarantee security.
<b>Preshared Key</b>	For the Auto (IKE) option, enter a password of any digit or characters in the text of "Pre-shared Key" (the example here is set as test), and the system will automatically translate what users entered as exchange password and authentication mechanism during the VPN tunnel connection. This exchange password can be made up of up to 30 characters.

## Advanced Setting- for IKE Protocol Only

### Advanced

- Aggressive Mode  
 Keep-Alive  
 NAT Traversal  
 Dead Peer Detection(DPD) Interval  seconds  
 Heart Beat, Remote Host ...  
Interval  seconds,Retry  count

The advanced settings include Main Mode and Aggressive mode. For the Main mode, the default setting is set to VPN operation mode. The connection is the same to most of the VPN devices.

Item	Description
<b>Aggressive Mode</b>	This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
<b>Keep Alive</b>	If this option is selected, VPN tunnel will keep this VPN connection. This is mostly used to connect the remote node of the branch office and headquarter or used for the remote dynamic IP address.
<b>NAT Traversal</b>	This option allowed the VPN connection can penetrate the NAT which in front of the router.
<b>Dead Peer Detection (DPD)</b>	If this option is selected, the connected VPN tunnel will regularly transmit HELLO/ACK message packet to detect whether there is connection between the two ends of the VPN tunnel. If one end is disconnected, the device will disconnect the tunnel automatically and then create new connection. Users can define the transmission time for each DPD message packet, and the default value is 10 seconds.
<b>Heart Beat</b>	If this option is selected, the system periodically sends ICMP to the VPN tunnel remote server host, the remote server will receive a packet after packet response. If the number of detected more than the value you set, and VPN remote server did not respond, the

system will determine the VPN tunnel is disconnected. If you create a VPN tunnel for the active side, the system will automatically rebuild the VPN tunnel again; and if you are a passive one, the system will wait for the other re-establish the VPN tunnel.

**Remote Host** : Remote network nodes to detect the location, the server address is best to be fast and stable response (proposal can fill in the VPN remote Sever LAN IP, please do not enter the server address which can not respond to ICMP).

**Time interval** : External connection detect ping timeout (seconds), default is 30 seconds. When the VPN tunnel established, every 30 seconds send ICMP detect the connection status with the server.

**Retry Count** : Ping retries, default is five. If the ping retry count exceeds the number of the remote server is not responding, then determine the VPN line break.






### 10.1.1.2 Client to Gateway Setting

The following describes how an administrator builds a VPN tunnel between devices. Users can set this VPN tunnel to be used by one client. Only one tunnel will be set and used by a group of clients, which allows easy setting.

#### Situation in Tunnel

Tunnel(s) No.	<input type="text" value="1"/>
Tunnel(s) Name :	<input type="text"/>
Interface:	<input type="button" value="WAN 1"/>
Enabled :	<input checked="" type="checkbox"/>

Item	Description		
<b>Tunnel No.</b>	Set the embedded VPN feature, please select the Tunnel number.		
<b>Tunnel Name</b>	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <table border="0"> <tr> <td style="text-align: center; vertical-align: middle;"> <b>Note</b></td> <td>If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.</td> </tr> </table> </div>	 <b>Note</b>	If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.
 <b>Note</b>	If this tunnel is to be connected to the other VPN device, some device requires that the tunnel name is identical to the name of the host end to facilitate verification. This tunnel can thus be successfully enabled.		
<b>Interface</b>	Users may select which port to be the node for this VPN channel. They can be applied for VPN connections.		
<b>Enabled</b>	Click to <b>Enable</b> to activate the VPN tunnel. This option is set to Enable by default. After users set up, users may select to activate this tunnel feature.		

#### Local VPN Group Setting

This local gateway authentication type (Local Security Gateway Type) must be identical with that of the remote type (Remote Security Gateway Type).

Item	Description
<b>Local Security Gateway Type:</b>	This local gateway authentication type comes with five operation modes, which are: <b>IP only</b> - Authentication by the use of IP only <b>IP + Domain Name (FQDN) Authentication</b> , -IP + Domain name <b>IP + E-mail Addr. (USER FQDN) Authentication</b> , -IP + Email address <b>Dynamic IP + Domain Name (FQDN) Authentication</b> , -Dynamic IP address + Domain name <b>Dynamic IP + E-mail Addr. (USER FQDN) Authentication</b> . Dynamic IP address + Email address name <b>(1) IP only:</b> If users decide to use <b>IP only</b> , entering the IP address is the only way to gain access to

this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Local Security Gateway Type:	IP Only
IP Address:	0 . 0 . 0 . 0

**(2) IP + Domain Name(FQDN) Authentication:**

If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.

Local Security Gateway Type:	IP + Domain Name(FQDN) Authentication
IP Address:	0 . 0 . 0 . 0
Domain Name:	

**(3) IP + E-mail Addr. (USER FQDN) Authentication.**

If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further settings.

Local Security Gateway Type:	IP + E-mail(User FQDN) Authentication
IP Address:	0 . 0 . 0 . 0
E-mail:	

**(4) Dynamic IP + Domain Name(FQDN) Authentication:**

If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.

Local Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name:	

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.**

If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; if users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.

Local Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication
E-mail:	

<b>Local Security Group Type:</b>	This option allows users to set the local VPN connection access type. The following offers a few items for local settings. Please select and set appropriate parameters:
-----------------------------------	--

1. IP address This option allows the only IP address which is entered to build the VPN tunnel.

Local Security Group Type:	IP Address
IP Address:	192 . 168 . 1 . 0

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.1.0 can establish connection.

## 2. Subnet

This option allows local computers in this subnet to be connected to the VPN tunnel.

Local Security Group Type:	Subnet
IP Address:	192 . 168 . 1 . 0
Subnet Mask:	255 . 255 . 255 . 0

Reference: When this VPN tunnel is connected, only computers with the session of 192.168.1.0 and with subnet mask as 255.255.255.0 can connect with remote VPN.

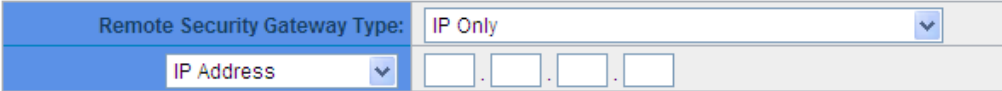
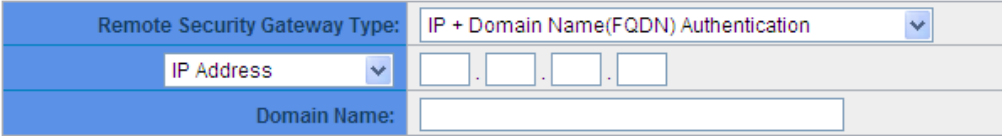
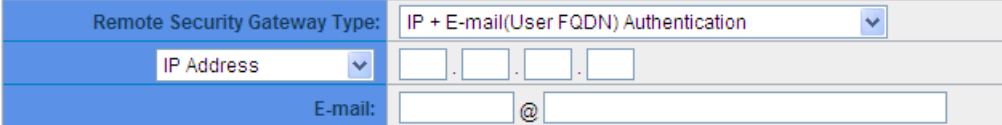
## Remote VPN Group Setting

### Remote VPN Group Setting

Remote Security Gateway Type: IP Only

IP Address: . . .

This remote gateway authentication type (Remote Security Gateway Type) must be identical to the remotely-connected local security gateway authentication type (Local Security Gateway Type).

Item	Description
<b>Remote Security Gateway Type:</b>	<p>This local gateway authentication type comes with five operation modes, which are: <b>IP only</b> <b>IP + Domain Name (FQDN) Authentication</b> <b>IP + E-mail Addr. (USER FQDN) Authentication</b> <b>Dynamic IP + Domain Name (FQDN) Authentication</b> <b>Dynamic IP + E-mail Addr. (USER FQDN) Authentication</b></p> <p><b>(1) IP only:</b></p> <p>If users decide to use <b>IP only</b>, entering the IP address is the only way to gain access to this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.</p>  <p><b>(2) IP + Domain Name(FQDN) Authentication:</b></p> <p>If users select IP + domain name type, please enter the domain name and IP address. The WAN IP address will be automatically filled into this space. Users don't need to do further settings. FQDN refers to the combination of host name and domain name and can be retrieved from the Internet, i.e. vpn.server.com. This IP address and domain name must be identical to those of the VPN secure gateway setting type to establish successful connection.</p>  <p><b>(3) IP + E-mail Addr. (USER FQDN) Authentication.</b></p> <p>If users select IP address and E-mail, enter the IP address and E-mail address to gain access to this tunnel and the WAN IP address will be automatically filled into this space. Users don't need to do further settings.</p>  <p><b>(4) Dynamic IP + Domain Name(FQDN) Authentication:</b></p> <p>If users use dynamic IP address to connect to the device, users may select this option to link to VPN. If the remote VPN gateway requires connection to the device for VPN</p>

connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.

Remote Security Gateway Type:	Dynamic IP + Domain Name(FQDN) Authentication
Domain Name:	<input type="text"/>

**(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.**

If users use dynamic IP address to connect to the device, users may select this option to connect to VPN without entering IP address. When VPN Gateway requires for VPN connection, the device will start authentication and respond to VPN tunnel connection; if users select this option to link to VPN, enter E-Mail address to the empty field for E-Mail authentication.

Remote Security Gateway Type:	Dynamic IP + E-mail(User FQDN) Authentication
E-mail:	<input type="text"/> @ <input type="text"/>

### IPSec Setup

If there is any encryption mechanism, the encryption mechanism of these two VPN tunnels must be identical in order to create connection. And the transmission data must be encrypted with IPSec key, which is known as the encryption "key". The device provides the IKE automatic encryption mode- IKE with Preshared Key (automatic).

### Encryption Management Protocol

When users set this VPN tunnel to use authentication mode, users must set the parameter of this exchange password with that of the remote

#### IPSec Setting

Keying Mode:	IKE with Preshared Key
Phase1 DHGroup :	Group 1
Phase1 Encryption:	DES
Phase1 Authentication:	MD5
Phase1 SA Life Time:	0 seconds
Perfect Forward Secrecy	<input checked="" type="checkbox"/>
Phase2 DHGroup :	Group 1
Phase2 Encryption:	DES
Phase2 Authentication:	MD5
Phase2 SA Life Time:	0 seconds
Preshared Key:	<input type="text"/>

Advanced +

## IKE Protocol

Click the shared key generated by IKE to encrypt and authenticate the remote user. If PFS (Perfect Forward Secrecy) is enabled, the Phase 2 shared key generated during the IKE coordination will conduct further encryption and authentication. When PFS is enabled, hackers using brute force to capture the key will not be able to get the Phase 2 key in such a short period of time.

Item	Description
<b>Perfect Forward Secrecy</b>	When users check the PFS option, don't forget to activate the PFS function of the VPN device and the VPN Client as well.
<b>Phase 1/ Phase 2 DH Group</b>	This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
<b>Phase 1/ Phase 2 Encryption</b>	This option allows users to set this VPN tunnel to use any encryption mode. Note that this parameter must be identical to that of the remote encryption parameter: DES (64-bit encryption mode), 3DES (128-bit encryption mode), AES (the standard of using security code to encrypt information). It supports 128-bit, 192-bit, and 256-bit encryption keys.
<b>Phase 1/Phase 2 Authentication</b>	This authentication option allows users to set this VPN tunnel to use any authentication mode. Note that this parameter must be identical to that of the remote authentication mode: "MD5" or "SHA1".
<b>Phase 1 SA Life Time</b>	The life time for this exchange code is set to 28800 seconds (or 8hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.
<b>Phase2 SA Life Time</b>	The life time for this exchange code is set to 3600 seconds (or 1hours) by default. This allows the automatic generation of other exchange password within the valid time of the VPN connection so as to guarantee security.

## Advanced Setting- for IKE Preshared Key Only

### Advanced

- Aggressive Mode  
 NAT Traversal  
 Dead Peer Detection(DPD) Interval  seconds

Apply

Cancel

The advanced settings include Main Mode and Aggressive mode. For the Main mode, the default setting is set to VPN operation mode. The connection is the same to most of the VPN devices.

Item	Description
Aggressive Mode:	This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
NAT Traversal	This option allowed the VPN connection can penetrate the NAT which in front of the router.
Dead Peer Detection (DPD)	If this option is selected, the connected VPN tunnel will regularly transmit HELLO/ACK message packet to detect whether there is connection between the two ends of the VPN tunnel. If one end is disconnected, the device will disconnect the tunnel automatically and then create new connection. Users can define the transmission time for each DPD message packet, and the default value is 10 seconds

### 10.1.2. PPTP Setting

It supports the PPTP of Window XP/ 2000 to create point-to-point tunnel protocol for single- device users to create VPN connection.

Enable PPTP Server

### PPTP IP Address Range

IP Range Starts: 192.168.1.150

IP Range Ends: 192.168.1.179

Unified IP Management

### New User Account

0 User(s) Defined

User Name :

New Password :

Confirm Password :

IP Address :  Automatically

Assign IP Address :  .  .  .

Add to list

Delete selected users

Item	Description
<b>Enabled PPTP Server</b>	When this option is selected, the point-to-point tunnel protocol PPTP server can be enabled.
<b>PPTP IP Address Range</b>	Please enter PPTP IP address range so as to provide the remote users with an entrance IP into the local network. <b>Enter Range Start:</b> Enter the value into the last field. <b>Enter Range End:</b> Enter the value into the last field.
<b>Username</b>	Please enter the name of the remote user.
<b>New Password</b>	Enter the password.
<b>Confirm Password</b>	Confirm again by entering the new password.
<b>Add to list</b>	Add a new account and password.
<b>Delete selected item</b>	Delete Selected Item.

### All PPTP Status

Displays all successfully connected users, including username, remote IP address, and PPTP address.



### Connection List

0 Tunnel(s) Used 60 Tunnel(s) Available

User Name	Remote Address	PPTP IP Address
-----------	----------------	-----------------

Apply Cancel

### 10.1.3. VPN Pass Through

#### VPN Pass Through

IPSec Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
PPTP Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
L2TP Pass Through :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Apply Cancel

Item	Description
<b>IPSec Pass Through</b>	If this option is <b>enabled</b> , the PC is allowed to use VPN-IPSec packet to pass in order to connect to external VPN device.
<b>PPTP Pass Through</b>	If this option is <b>enabled</b> , the PC is allowed to use VPN- PPTP packet to pass in order to connect with external VPN device.
<b>L2TP Pass Through</b>	If this option is <b>enabled</b> , the PC end is allowed to use VPN- L2TP packet to pass in order to connect with external VPN device.

After modification, push “**Apply**” button to save the network setting or push “**Cancel**” to keep the settings unchanged.

## Chapter 11: Advanced Function

### 11.1 DMZ Host/ Port Range Forwarding

#### DMZ Host

DMZ Private IP Address 192.168.1.0

#### Port Range Forwarding

Service : All Traffic [TCP&UDP/1~65535]

Service Management

IP Address : . . .

Interface : ANY

Enabled :

Add to list

Delete selected application

Show Table Apply Cancel

#### 11.1.1 DMZ Host

When the NAT mode is activated, sometimes users may need to use applications that do not support virtual IP addresses such as network games. We recommend that users map the device actual WAN IP addresses directly to the Intranet virtual IP addresses, as follows:

If the "DMZ Host" function is selected, to cancel this function, users must input "0" in the following "DMZ Private IP". This function will then be closed. After the changes are completed, click "Apply" to save the network configuration modification, or click "Cancel" to leave without making any changes.

### 11.1.2 Port Range Forwarding

Setting up a Port Forwarding Virtual Host: If the server function (which means the server for an external service such as WWW, FTP, Mail, etc) is contained in the network, we recommend that users use the firewall function to set up the host as a virtual host, and then convert the actual IP addresses (the Internet IP addresses) with Port 80 (the service port of WWW is Port 80) to access the internal server directly. In the configuration page, if a web server address such as 192.168.1.50 and the Port 80 has been set up in the configuration, this web page will be accessible from the Internet by keying in the device actual IP address such as, <http://211.243.220.43>.

At this moment, the device actual IP will be converted into "192.168.1.50" by Port 80 to access the web page.

In the same way, to set up other services, please input the server TCP or UDP port number and the virtual host IP addresses.

#### Port Range Forwarding

Service : All Traffic [TCP&UDP/1~65535]

IP Address :

Interface : ANY

Enabled :

Item	Description
<b>Service</b>	To select from this option the default list of service ports of the virtual host that users want to activate. Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and 21~21 for FTP. Please refer to the list of default service ports.
<b>IP Address</b>	Input the virtual host IP address.
<b>Interface</b>	Select the WAN port.
<b>Enabled</b>	Activate this function.
<b>Service Management</b>	Add or remove service ports from the list of service ports.
<b>Add to list</b>	Add to the active service content.

## Service Port Management

The services in the list mentioned above are frequently used services. If the service users want to activate is not in the list, we recommend that users use "Service Port Management" to add or remove ports, as follows:

Item	Description
<b>Service Name</b>	Input the name of the service port users want to activate on the list, such as E-donkey, etc.
<b>Protocol</b>	To select whether a service port is TCP or UDP.
<b>Port Range</b>	To activate this function, input the range of the service port locations users want to

	activate.
<b>Add to list</b>	Add the service to the service list.
<b>Delete selected item</b>	To remove the selected services.
<b>Apply</b>	Click the “Apply” button to save the modification.
<b>Cancel</b>	Click the “Cancel” button to cancel the modification. This only works before “Apply” is clicked.
<b>Close</b>	Quit this configuration window.

## 11.2 UPnP

UPnP (Universal Plug and Play) is a protocol set by Microsoft. If the virtual host supports UPnP system (such as Windows XP), users could also activate the PC UPnP function to work with the device.

### UPnP Setup

Show Table

Apply

Cancel

Item	Description
<b>Service Port</b>	Select the UPnP service number default list here; for example, WWW is 80~80, FTP is 21~21. Please refer to the default service number list.
<b>Host Name or IP Address</b>	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.
<b>Enabled</b>	Activate this function.
<b>Service Port Management</b>	Add or remove service ports from the management list.

<b>Add to List</b>	Add to active service content.
<b>Delete Selected Item</b>	Remove selected services.
<b>Show Table</b>	This is a list which displays the current active UPnP functions.
<b>Apply</b>	Click "Apply" to save the network configuration modification.

### 11.3 Routing

In this chapter we introduce the Dynamic Routing Information Protocol and Static Routing Information Protocol.

#### Dynamic Routing

Working Mode:	<input checked="" type="radio"/> Gateway <input type="radio"/> Router
RIP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Receive RIP versions :	None
Transmit RIP versions :	None

#### Static Routing

Dest. IP :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway :	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Hop Count :	<input type="text"/>
Interface :	LAN
<input type="button" value="Add to list"/>	
<div style="border: 1px solid gray; height: 100px; width: 100%;"></div>	
<input type="button" value="Delete selected item"/>	

#### 11.3.1 Dynamic Routing

The abbreviation of Routing Information Protocol is RIP. There are two kinds of RIP in the IP environment – RIP I and RIP II. Since there is usually only one router in a network, ordinarily just

Static Routing will be used. RIP is used when there is more than one router in a network, and if an administrator doesn't want to assign a path list one by one to all of the routers, RIP can help refresh the paths. RIP is a very simple routing protocol, in which Distance Vector is used. Distance Vector determines transmission distance in accordance with the number of routers, rather than based on actual session speed. Therefore, sometimes it will select a path through the least number of routers, rather than through the fastest routers.

### Dynamic Routing

Working Mode:	<input checked="" type="radio"/> Gateway <input type="radio"/> Router
RIP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Receive RIP versions :	None <input type="button" value="v"/>
Transmit RIP versions :	None <input type="button" value="v"/>

Item	Description
<b>Working Mode</b>	Select the working mode of the device: NAT mode or Router mode.
<b>RIP</b>	Click "Enabled" to open the RIP function.
<b>Receive RIP versions</b>	Use Up/Down button to select one of "None", "RIPv1", "RIPv2", "Both RIPv1 and v2" as the "TX" function for transmitting dynamic RIP.
<b>Transmit RIP versions</b>	Use Up/Down button to select one of "None", "RIPv1", "RIPv2-Broadcast", "RIPv2-Multicast" as the "RX" function for receiving dynamic RIP.

### 11.3.2 Static Routing

When there are more than one router and IP subnets, the routing mode for the device should be configured as static routing. Static routing enables different network nodes to seek necessary paths automatically. It also enables different network nodes to access each other. Click the button "**Show Routing Table**" (as in the figure) to display the current routing list.

## Static Routing

Dest. IP :  .  .  .   
 Subnet Mask :  .  .  .   
 Default Gateway :  .  .  .   
 Hop Count :   
 Interface : LAN




Item	Description
<b>Dest. IP</b> <b>Subnet Mask</b>	Input the remote network IP locations and subnet that is to be routed. For example, the IP/subnet is 192.168.2.0/255.255.255.0.
<b>Gateway</b>	The default gateway location of the network node which is to be routed.
<b>Hop Count</b>	This is the router layer count for the IP. If there are two routers under the device, users should input "2" for the router layer; the default is "1". (Max. is 15.)
<b>Interface</b>	This is to select "WAN port" or "LAN port" for network connection location.
<b>Add to List</b>	Add the routing rule into the list.
<b>Delete Selected Item</b>	Remove the selected routing rule from the list.
<b>Show Table</b>	Show current routing table.
<b>Apply</b>	Click " <b>Apply</b> " to save the network configuration modification
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any changes.



### 11.4 One to One NAT

As both the device and ATU-R need only one actual IP, if ISP issued more than one actual IP (such as eight ADSL static IP addresses or more), users can map the remaining real IP addresses to the intranet PC virtual IP addresses. These PCs use private IP addresses in the Intranet, but after having One to One NAT mapping, these PCs will have their own public IP addresses.

**For example**, if there are more than 2 web servers requiring public IP addresses, administrators can map several public IP addresses directly to internal private IP addresses.

**Example** :Users have five available IP addresses - 210.11.1.1~5, one of which, 210.11.1.1, has been configured as a real IP for WAN, and is used in NAT. Users can respectively configure the other four real IP addresses for Multi-DMZ, as follows:

210.11.1.2 . 192.168.1.3

210.11.1.3 . 192.168.1.4

210.11.1.4 . 192.168.1.5

210.11.1.5 . 192.168.1.6

**Attention**

The device WAN IP address can not be contained in the One-to-One NAT IP configuration.

Enable One-to-One NAT

One to One NAT

**Add Range**


Private Range Begin:

Public Range Begin:

Range Length:

Enable Multiple to One NAT

Item	Description
<b>Enabled One to One NAT</b>	To activate or close the One-to-One NAT function. (Check to activate the function).
<b>Private IP Range Begin</b>	Input the Private IP address for the Intranet One-to-One NAT function.
<b>Public IP Range Begin</b>	Input the Public IP address for the Internet One-to-One NAT function.
<b>Range Length</b>	The numbers of final IP addresses of actual Internet IP addresses. (Please do not include IP addresses in use by WANs.)
<b>Add to List</b>	Add this configuration to the One-to-One NAT list.
<b>Delete Selected Item</b>	Remove a selected One-to-One NAT list.
<b>Apply</b>	Click " <b>Apply</b> " to save the network configuration modification.
<b>Cancel</b>	Click "Cancel" to leave without making any changes.

 <b>Attention</b>	<p>One-to-One NAT mode will change the firewall working mode. If this function has been set up, the Internet IP server or PC which is mapped with a LAN port will be exposed on the Internet.</p> <p>To prevent Internet users from actively connecting with the One-on-One NAT server or PC, please set up a proper denial rule for access, as described Firewall.</p>
---	---

### Multiple to One NAT

Enable Multiple to One NAT

#### Multiple to One NAT

Private IP Range: ... to .

Representative Public IP: ...

Interface: WAN 1 ▼

Item	Description
<b>Enable Multiple to One NAT</b>	Click to enable multiple to one NAT function.
<b>Private IP Range</b>	Input intranet IPs for NAT mapping.
<b>Respective Public IP</b>	Input the respective public IP addresses. This should go along with the following interface selection. If the IP address is not within the interface ranges, the setting will not work.
<b>Interface</b>	Select the mapping interface. If the WAN IP above is not within the interface range, the setting will not work.
<b>Add to List</b>	Add this configuration to the One-to-One NAT list.
<b>Delete selected</b>	Remove a selected One-to-One NAT list.

<b>range</b>	
<b>Apply</b>	Click "Apply" to save the network configuration modification.
<b>Cancel</b>	Click "Cancel" to leave without making any changes.

### 11.5 DDNS- Dynamic Domain Name Service

**DDNS** supports the dynamic web address transfer for 3322.org、DynDNS.org and DtDNS.com. This is for VPN connections to a website that is built with dynamic IP addresses, and for dynamic IP remote control. For example, the actual IP address of an ADSL PPPoE time-based system or the actual IP of a cable modem will be changed from time to time. To overcome this problem for users who want to build services such as a website, it offers the function of dynamic web address transfer. This service can be applied from www.3322.org, www.dyndns.org, or www.dtdns.com, and these are free.

Also, in order to solve the issue that DDNS server is not stable, the device can update the dynamic IP address with different services at the same time.

#### DDNS Setup

Interface	Status	Host Name	Config.
WAN 1	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	<a href="#">Edit</a>
WAN 2	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	<a href="#">Edit</a>
WAN 3	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	<a href="#">Edit</a>
WAN 4	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	<a href="#">Edit</a>
USB	Dyndns Disabled 3322 Disabled	Dyndns:--- 3322:---	<a href="#">Edit</a>

Select the WAN port to which the configuration is to be edited, for example, WAN 1. Click the hyperlink to enter and edit the settings.

Interface: WAN 1

DynDNS.org

User Name:	<input type="text"/>	<input type="button" value="Register"/>
Password:	<input type="password"/>	
Host Name:	<input type="text"/>	<input type="text"/>
Internet IP Address:	0.0.0.0	
Status:	DDNS function is disabled or No Internet connection.	

3322.org

User Name:	<input type="text"/>	<input type="button" value="Register"/>
Password:	<input type="password"/>	
Host Name:	<input type="text"/>	<input type="text"/>
Internet IP Address:	0.0.0.0	
Status:	DDNS function is disabled or No Internet connection.	

Item	Description
<b>Interface</b>	This is an indication of the WAN port the user has selected.
<b>DDNS</b>	Check either of the boxes before DynDNS.org, 3322.org and DtDNS.com to select one of the four DDNS website address transfer functions.
<b>Username</b>	The name which is set up for DDNS. Input a complete website address such as abc.abcdns.org.cn as a user name for abcDDNS.
<b>Password</b>	The password which is set up for DDNS.
<b>Host Name</b>	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.
<b>Internet IP Address</b>	Input the actual dynamic IP address issued by the ISP.
<b>Status</b>	An indication of the status of the current IP function refreshed by DDNS.
<b>Apply</b>	After the changes are completed, click " <b>Apply</b> " to save the network configuration modification.
<b>Cancel</b>	Click " <b>Cancel</b> " to leave without making any changes.

## 11.6 MAC Clone

Some ISP will request for a fixed MAC address (network card physical address) for distributing IP address, which is mostly suitable for cable mode users. Users can input the network card physical address (MAC address: 00-xx-xx-xx-xx-xx) here. The device will adopt this MAC address when requesting IP address from ISP.

### MAC Clone

Interface	MAC Address	Config.
WAN 1	50-56-4D-32-30-31	<a href="#">Edit</a>
WAN 2	50-56-4D-32-30-32	<a href="#">Edit</a>
WAN 3	50-56-4D-32-30-33	<a href="#">Edit</a>
WAN 4	50-56-4D-32-30-34	<a href="#">Edit</a>

Select the WAN port to which the configuration is to be edited; click the hyperlink to enter and edit its configuration. Users can input the MAC address manually. Press “Apply” to save the setting, and press “Cancel” to remove the setting. Default MAC address is the WAN MAC address.

Interface WAN 1

User Defined WAN MAC Address :	<input checked="" type="radio"/> <span style="border: 1px solid gray; padding: 2px;">50</span> <span style="border: 1px solid gray; padding: 2px;">56</span> <span style="border: 1px solid gray; padding: 2px;">4D</span> <span style="border: 1px solid gray; padding: 2px;">32</span> <span style="border: 1px solid gray; padding: 2px;">30</span> <span style="border: 1px solid gray; padding: 2px;">31</span>
	Default: 50-56-4D-32-30-31
MAC Address from this PC	<input type="radio"/> 00-1F-C6-7B-8A-BD

## Chapter 12: System Tool

### System Tool

This chapter introduces the management tool for controlling the device and testing network connection. For security consideration, we strongly suggest to change the password. Password and Time setting is in Chapter 5.2.

#### 12.1 Diagnostic

The device provides a simple online network diagnostic tool to help users troubleshoot network-related problems. This tool includes **DNS Name Lookup** (Domain Name Inquiry Test) and **Ping** (Packet Delivery/Reception Test).

DNS Lookup  Ping

Ping host or IP address

#### DNS Name lookup

On this test screen, please enter the host name of the network users want to test. For example, users may enter www.yahoo.com.tw and press "Go" to start the test. The result will be displayed on this page.

DNS Lookup  Ping

Look up domain name    
 Name: www.yahoo.com.tw  
 Address: 203.84.219.114

#### Ping

DNS Lookup  Ping


Ping host or IP address    
 Status: Test Succeeded  
 Packets: 4/4 transmitted,4/4 received,0 % loss  
 Round Trip Time: Minimum = 3.2 ms  
 Maximum = 3.7 ms  
 Average = 3.4 ms

This item informs users of the status quo of the outbound session and allows the user to know the existence of computers online.

On this test screen, please enter the host IP that users want to test such as 168.95.1.1 Press "Go" to start the test. The result will be displayed on this screen.

## 12.2 Firmware Upgrade

Users may directly upgrade the device firmware on the Firmware Upgrade page. Please confirm all information about the software version in advance. Select and browse the software file, click "**Firmware Upgrade Right Now**" to complete the upgrade of the designated file.

 <b>Attention</b>	Please read the warning before firmware upgrade. Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.
---	---

### Firmware Upgrade

**Warning**

1. Choosing previous firmware versions will restore all settings to default.
2. Firmware upgrading may take a few minutes, don't turn off power or press reset.
3. Don't close the window or disconnect during upgrading process.
4. Please suspend on-line traffics when upgrading the new firmware.

Firmware Version : v1.0.0 .01 (Mar 3 2011 17:05:09)

1

## 12.3 Configuration Backup

### Import Configuration File

### Export Configuration File

#### Import Configuration File

This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to **import** the file.

#### Export Configuration File

This feature allows users to backup all parameter settings. Click "Export" and select the location to save the "config.exp" file.



## 12.4 SNMP

Simple Network Management Protocol (SNMP) refers to network management communications protocol and it is also an important network management item. Through this SNMP communications protocol, programs with network management (i.e. SNMP Tools-HP Open View) can help communications of real-time management. The device supports standard SNMP v1/v2c and is consistent with SNMP network management software so as to get hold on to the operation of the online devices and the real-time network information.

### SNMP Setup

Enabled SNMP

System Name	4WAN_1LAN_IPSec_VPN_Router
System Contact	
System Location	
Get Community Name	public
Set Community Name	private
Trap Community Name	public
Send SNMP Trap to	

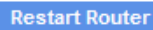
Apply Cancel

Item	Description
<b>Enabled</b>	Activate SNMP feature. The default is activated.
<b>System Name</b>	Set the name of the device such as Planet.
<b>System Contact</b>	Set the name of the person who manages the device (i.e. John).
<b>System Location</b>	Define the location of the device (i.e. Taipei).
<b>Get Community Name</b>	Set the name of the group or community that can view the device SNMP data. The default setting is "Public".
<b>Set Community Name</b>	Set the name of the group or community that can receive the device SNMP data. The default setting is "Private".
<b>Trap Community Name</b>	Set user parameters (password required by the Trap-receiving host computer) to receive Trap message.
<b>Send SNMP Trap to</b>	Set one IP address or Domain Name for the Trap-receiving host computer.
<b>Apply</b>	Press " <b>Apply</b> " to save the settings.
<b>Cancel</b>	Press " <b>Cancel</b> " to keep the settings unchanged.

## 12.5 System Recover

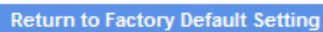
Users can restart the device with System Recover button.

### Restart



Restart Router

### Factory Default

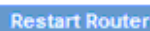


Return to Factory Default Setting

## Restart

As the figure below, if clicking “Restart Router” button, the dialog block will pop out, confirming if users would like to restart the device.

### Restart



Restart Router

#### Message from webpage

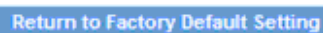


Are you sure you want to restart router?

OK

Cancel

### Factory Default



Return to Factory Default Setting

## Return to Factory Default Setting

If clicking “Return to Factory Default Setting”, the dialog block will pop out, if the device will return to factory default. It's recommended to save the current configuration before upgrading firmware. After firmware upgraded, import the configuration file after returning to factory default to ensure system stable. (Please refer to 12.3)

## 12.6 High Availability

High Availability is adopted in the network that requires fault tolerance and backup mechanism. Two similar devices are used to be the backup for each other. One of these devices is employed for major network transmitting, and the other redundant device will take over when the master device fails to assure that network transmitting and services never break down. Therefore, administrators will have more opportunity and time to deal with the master device problems.

Besides general HA, Planet also provides advanced HA function that enables two devices to operate simultaneously. It brings full cost efficiency without making another device idle. It does not have to be the same model. All of Planet devices which support HA can achieve the function.

### High Availability

High Availability	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
	<input type="checkbox"/> WAN Network Service Detection	
Mode:	<input checked="" type="radio"/> Hardware Backup Mode	<input type="radio"/> Two devices are operating simultaneously
Operation:	<input checked="" type="radio"/> Master Mode	<input type="radio"/> Backup Mode
	Master / Slave Mode setting Of two devices must be different	
Status:	Disable	

Apply

Cancel

Item	Description
High Availability	<p><b>Enable:</b> Activate HA function.</p> <p><b>Disable:</b> Disable HA function.</p>
Mode	<p><b>(1) Hardware Backup Mode</b></p> <p>It is the general backup mode. The master device takes responsibility of network transmitting and the other one is set as idle. When the master device fails transmitting, it will send out the message to the idle device for taking over network transmitting immediately.</p> <p><b>(2) Two devices are operating simultaneously</b></p> <p>Two devices operate outbound linking simultaneously, but they are still separated as Master device and Backup device. In normal situation, Master device is major DHCP IP issuer, and Backup device will disable DHCP issuing automatically. When Master device fails transmitting, the Backup device will take over all outbound links and enable DHCP server to provide IP addresses.</p>

Following is the description of the two different modes.

<b>High Availability</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Mode:</b>	<input checked="" type="radio"/> Hardware Backup Mode	<input type="radio"/> Two devices are operating simultaneously
<b>Operation:</b>	<input checked="" type="radio"/> Master Mode	<input type="radio"/> Backup Mode
Master / Slave Mode setting Of two devices must be different		
<b>Status:</b>	Normal	
<b>Status of the backup device:</b>	Normal	

Item	Description
<b>Operation-Master Mode</b>	Indicates the master device will operate for all outbound links. When the master device fails transmitting, the backup device will take over.
<b>Status</b>	“Status- Normal” indicates the device operates well.
<b>Status of the backup device</b>	Indicates status of backup device. If the status is normal, administrators can login the device remotely to manage. (Remote Management should be enabled). “Status- Abnormal” indicates the backup device can not be detected or does exist, and need to inspect the backup device actual status.

<b>High Availability</b>	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<b>Mode:</b>	<input checked="" type="radio"/> Hardware Backup Mode	<input type="radio"/> Two devices are operating simultaneously
<b>Operation:</b>	<input type="radio"/> Master Mode	<input checked="" type="radio"/> Backup Mode
Master / Slave Mode setting Of two devices must be different		
<b>LAN IP of the backup device:</b>	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="5"/>	
<b>MAC Address of the backup device:</b>	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	
<b>Status:</b>	Normal	

Item	Description
<b>Operation-Backup Mode</b>	Indicates the backup device will take over when the master fails transmitting. WAN and LAN IP setting in backup device should be the same as those of master device. The backup device should not be in charge of network transmitting and DHCP server. ※ If the original LAN IP addresses are issued by Master device, DHCP server setting of Backup device should be the same as Master device. The Backup

	device can keep DHCP functioning and there will be no LAN disconnection.
<b>LAN IP of the backup device</b>	Input LAN IP of Master mode, which is backed up.
<b>MAC Address of the backup device</b>	Input Master device MAC address, which is backed up.
<b>Status</b>	<p>“Status- Normal” indicates the status is idle. Master device operates normally.</p> <p>“Status- Backup” indicates the device takes over all the network transmitting. The status will return to “Normal” when Master device boots normally and send a message to the backup device. Then, the status will return to Normal, which the backup device remains idle.</p>

**Two devices are operating simultaneously:**

**High Availability**  Enable  Disable

**Mode:**  Hardware Backup Mode  Two devices are operating simultaneously

**Operation:**  Master Mode (DHCP Enable)  Slave Mode (DHCP Disable)

Master / Slave Mode setting Of two devices must be different

**WAN Backup:**  WAN 1  WAN 2  WAN 3  WAN 4  WAN 5  
 (The checked WAN are not working in this device.)

**LAN Gateway Backup:**

**MAC Address of the backup device:**

**Status:** Normal

Item	Description
<b>Operation-Master Mode</b>	Besides operating network with another device, Master device is also the DHCP server to issue LAN IP addresses. Although Slave device also supports outbound linking, its DHCP server is disabled.
<b>WAN Backup (The Checked WANs are not working in this device.)</b>	The checked WANs will works in the other device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in the other device, WAN3 and WAN4 should be checked.
<b>LAN Gateway Backup</b>	Input LAN IP of Slave device. The IP should be different from LAN IP of Master device.
<b>MAC Address of the</b>	Input LAN MAC of Slave device. It should be different from LAN MAC of Master

<b>backup device</b>	device.
<b>Status</b>	“Status-Normal” means both two devices operate normally. “Status-Backup” indicates Slave mode has problems, and the device enables backup to take over WAN

**High Availability**  Enable  Disable

**Mode:**  Hardware Backup Mode  Two devices are operating simultaneously

**Operation:**  Master Mode (DHCP Enable)  Slave Mode (DHCP Disable)

Master / Slave Mode setting Of two devices must be different

**WAN Backup:**  WAN 1  WAN 2  WAN 3  WAN 4  
 (The checked WAN are not working in this device.)

**LAN Gateway Backup:**

**MAC Address of the backup device:**

**Status:** Normal

Item	Description
<b>Operation-Slave Mode</b>	<p>Although working with master device, Backup device's DHCP server is disabled. LAN users need to transmit traffic through the WAN on Slave device. You should add LAN IP of Slave device into Master device DHCP server default gateway, which is DHCP server IP address.</p> <p>For example, if the DHCP server's IP of Master device is 192.168.1.1, and the subnet mask is 255.255.255.0, Slave device should be in the same subnet, ex. 192.168.1.2.</p>
<b>WAN Backup (The Checked WANs are not working in this device.)</b>	The checked WANs will work in another device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in another, WAN3 and WAN4 should be checked.
<b>LAN Gateway Backup</b>	Input the LAN IP of Master device. It should be different from Slave device's IP. (Must be in the same subnet.)
<b>MAC Address of the backup device</b>	Input the LAN MAC of Master device. It should be different from Slave device's LAN MAC.
<b>Status</b>	“Status-Normal” indicates both devices work normally; “Status-Backup” indicates the Backup device is enabled for backing up Master device to take over WAN connection and DHCP issuing function.

## Chapter 13. Log

From the log management and look up, we can see the relevant operation status, which is convenient for us to facilitate the setup and operation.

### 13.1 System Log

Its system log offers three options: system log, E-mail alert, and log setting.

#### Send SMS

Enable  USB

Dial Number :

Link UP  Link Down  Authentication Fail  System Startup

#### Syslog Configuration

Enable Syslog

Syslog Server :  Name or IP Address

#### Log Setting

Alert Log		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> Unauthorized Login Attempt	

General Log		
<input type="checkbox"/> Deny Policies	<input type="checkbox"/> Allow Policies	<input checked="" type="checkbox"/> Authorized Login







## System Log

### Syslog Configuration

Enable Syslog

Syslog Server :  Name or IP Address

Item	Description
<b>Enabled</b>	If this option is selected, the System Log feature will be enabled.
<b>Syslog Server</b>	The device provides external system log servers with log collection feature. System log is an industrial standard communications protocol. It is designed to dynamically capture related system message from the network. The system log provides the source and the destination IP addresses during the connection, service number, and type. To apply this feature, enter the system log server name or the IP address into the empty "system log server" field.

## Log Setting

### Log Setting

Alert Log		
<input type="checkbox"/> Syn Flooding	<input type="checkbox"/> IP Spoofing	<input type="checkbox"/> Win Nuke
<input type="checkbox"/> Ping Of Death	<input checked="" type="checkbox"/> Unauthorized Login Attempt	

General Log		
<input type="checkbox"/> Deny Policies	<input type="checkbox"/> Allow Policies	<input checked="" type="checkbox"/> Authorized Login

[View System Log](#)
[Outgoing Log Table](#)
[Incoming Log Table](#)
[Clear Log Now](#)

## Alert Log

The device provides the following warning message. Click to activate these features: Syn Flooding, IP Spoofing, Win Nuke, Ping of Death / Unauthorized Login Attempt.

Item	Description
<b>Syn Flooding</b>	Bulky syn packet transmission in a short time causes the overload of the system storage of record in connection information.
<b>IP Spoofing</b>	Through the packet sniffing, hackers intercept data transmitted on the network. After they access the information, the IP address from the sender is changed so that they can access the resource in the source system.
<b>Win Nuke</b>	Servers are attacked or trapped by the Trojan program.
<b>Ping of Death</b>	The system fails because the sent data exceeds the maximum packet that can be handled by the IP protocol.
<b>Unauthorized Login</b>	If intruders into the device are identified, the message will be sent to the system log.



## General Log

The device provides the following warning message. Click to activate the feature. System error message, blocked regulations, regulation of passage permission, system configuration change and registration verification.

Item	Description
<b>System Error Message</b>	Provides the system log with all kinds of error messages. For example, wrong settings, occurrence of abnormal functions, system reactivation, disconnection of PPPoE and so on.
<b>Deny Policies</b>	If remote users fail to enter the system because of the access rules; for instance, message will be recorded in the system log.
<b>Allow Policies</b>	If remote users enter the system because of compliance with access rules; for instance, message will be recorded in the system log.
<b>Configuration Change</b>	When the system settings are changed, this message will be sent back to the system log.
<b>Authorized Login</b>	Successful entry into the system includes login from the remote end or from the LAN into this device. These messages will be recorded in the system log.

The following is the description of the four buttons allowing online inquiry into the log.

## View System Log

This option allows users to view system log. The message content can be read online via the device. They include **All Log**, **System Log**, **Access Log**, **Firewall Log**, and **VPN log**, which is illustrated as below.

System Log		
Current Time:	Fri Mar 4 20:10:49 2011	All Log <input type="button" value="Refresh"/> <input type="button" value="Close"/>
Time ▲	Event-Type	Message
Mar 4 15:27:59 2011	System Log	4WAN_1LAN_IPSec_VPN_Router : System is up
Mar 4 15:28:22 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 16:16:34 2011	System Log	4WAN_1LAN_IPSec_VPN_Router : System is up
Mar 4 16:19:58 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 16:25:45 2011	System Log	4WAN_1LAN_IPSec_VPN_Router : System is up
Mar 4 16:26:04 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 16:56:05 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 16:56:37 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 17:38:47 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 17:43:38 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 18:12:54 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 19:02:23 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 20:02:12 2011	System Log	HTTP Basic authentication success for user: admin
Mar 4 20:10:40 2011	System Log	recvfrom: Network is down
Mar 4 20:10:40 2011	System Log	

## Outgoing Packet Log

View system packet log which is sent out from the internal PC to the Internet. This log includes LAN IP, destination IP, and service port that is applied. It is illustrated as below.

Time ▲	Event-Type	Message
Feb 6 03:46:03 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->77.239.233.64:20301 on ixp2
Feb 6 03:46:06 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->84.10.118.17:10682 on ixp7
Feb 6 06:27:54 2006	Connection Refused - Policy violation	TCP 192.168.1.1:80->192.168.1.100:1224 on ixp0
Feb 6 08:18:58 2006	Connection Refused - Policy violation	TCP 192.168.1.101:18195->163.253.104.148:1234 on ixp1
Feb 6 08:19:53 2006	Connection Refused - Policy violation	TCP 192.168.1.101:51671->3.139.58.12:1234 on ixp1

## Incoming Packet Log

View system packet log of those entering the firewall. The log includes information about the external source IP addresses, destination IP addresses, and service ports. It is illustrated as below.

### Incoming Log Table

Current Time: Fri Mar 4 20:14:20 2011

Time ▲	Event-Type	Message
Feb 6 02:34:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->255.255.255.255:68 on ixp2
Feb 6 02:57:54 2006	Connection Refused - Policy violation	UDP 192.168.1.100:137->192.168.1.255:137 on ixp0
Feb 6 03:06:39 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.102:68 on ixp2
Feb 6 03:15:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.100:68 on ixp4
Feb 6 03:45:58 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->75.128.47.253:27220 on ixp0
Feb 6 03:46:00 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->91.153.161.189:27310 on ixp0
Feb 6 03:46:02 2006	Connection Refused - Policy violation	UDP 192.168.1.100:7464->24.160.250.156:19343 on ixp0

### Clear Log Now

This feature clears all the current information on the log.

## 13.2 System Statistic

The device has the real-time surveillance management feature that provides system current operation information such as port location, device name, current WAN link status, IP address, MAC address, subnet mask, default gateway, DNS, number of received/ sent/ total packets , number of received/ sent/ total Bytes, Received and Sent Bytes/Sec., total number of error packets received, total number of the packets dropped, number of session, number of the new Session/Sec., and upstream as well as downstream broadband usage (%).

### System Statistic

[Next Page](#)

Interface :	WAN 1	WAN 2	WAN 3	WAN 4
Device Name :	eth1	eth2	eth3	eth4
Status :	Connect	Enabled	Enabled	Enabled
Device IP Address :	192.168.4.103	0.0.0.0	0.0.0.0	0.0.0.0
MAC Address :	50-56-4D-32-30-31	50-56-4D-32-30-32	50-56-4D-32-30-33	50-56-4D-32-30-34
Subnet Mask :	255.255.254.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway :	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS :	192.168.5.121	0.0.0.0	0.0.0.0	0.0.0.0
Network Service Detection :	Test Succeeded	Test Failed	Test Failed	Test Failed
Received Packets :	3266	0	0	0
Transmitted Packets :	122	0	0	0
Total Packets :	3388	0	0	0
Received Packets Byte :	332884	0	0	0
Transmitted Packets Byte :	19797	0	0	0
Total Packets Byte :	352681	0	0	0
Received Byte/Sec :	293	0	0	0
Transmitted Byte/Sec :	0	0	0	0
Error Packets :	0	0	0	0
Dropped Packets :	0	0	0	0
Sessions :	0	0	0	0
New Sessions/Sec :	0	0	0	0
Upstream Bandwidth Usage :	0	0	0	0
Downstream Bandwidth Usage :	0	0	0	0

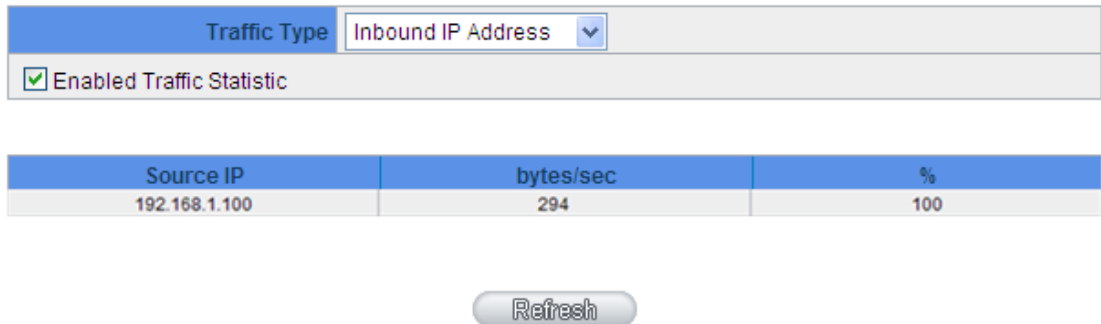
Refresh

### 13.3 Traffic Statistic

Six messages will be displayed on the **Traffic Statistic** page to provide better traffic management and control.

#### Traffic Statistic

---

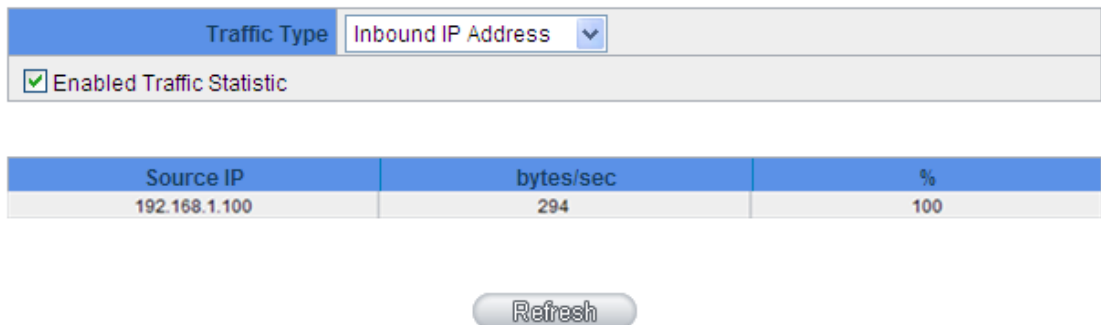


#### By Inbound IP Address

The figure displays the source IP address, bytes per second, and percentage.

#### Traffic Statistic

---

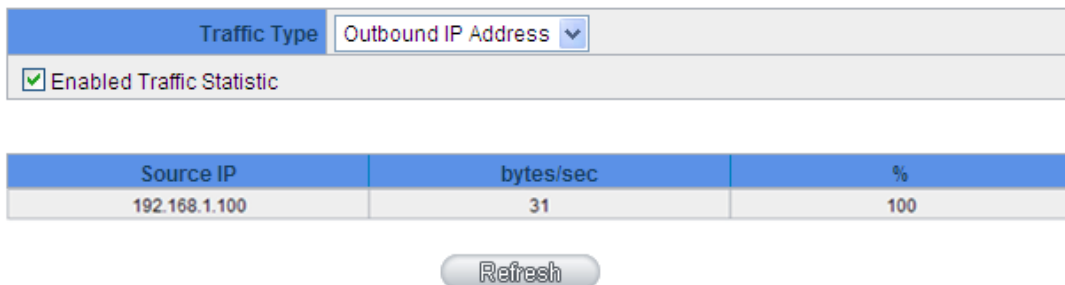


#### By outbound IP Address

The figure displays the source IP address, bytes per second, and percentage.

#### Traffic Statistic

---



#### By Outbound Port

The figure displays the network protocol type, destination IP address, bytes per second, and percentage.

### Traffic Statistic

Traffic Type    
 Enabled Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	http(80)	32	56
TCP	1144	17	30
TCP	1863	3	6
UDP	137	2	4
TCP	netbios(139)	1	2

### By Inbound Port

The figure displays the network protocol type, destination IP address, bytes per second, and percentage.

### Traffic Statistic

Traffic Type    
 Enabled Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	1863	37	65
TCP	1144	11	20
TCP	http(80)	8	14

### By Outbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

### By Inbound Session

The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

### Traffic Statistic

Traffic Type    
 Enabled Traffic Statistic

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2940	192.168.5.126	1144	9	100

### 13.4 IP/ Port Statistic

The device allows administrators to inquire a specific IP (or from a specific port) about the addresses that this IP had visited, or the users (source IP) who used this service port. This facilitates the identification of websites that needs authentication but allows a single WAN port rather than Multi-WANs. Administrators may find out the destination IP for protocol binding to solve this login problem. For example, when certain port software is denied, inquiring about the IP address of this specific software server port may apply this feature. Moreover, to find out BT or P2P software, users may select this feature to inquire users from the port.

#### IP/Port Statistic

Enabled IP/Port Statistic IP Address

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
-----------	----------	-------------	-----------------	----------	------------	----------------------	--------------------

Specific IP Status :

Enter the IP address that users want to inquire, and then the entire destination IP connected to remote devices as well as the number of ports will be displayed.

#### IP/Port Statistic

Enabled IP/Port Statistic IP Address

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2959	WAN1	74.120.121.3	80	8	32
192.168.1.100	TCP	2940	WAN1	192.168.5.126	1144	11	20
192.168.1.100	TCP	3036	WAN1	192.168.5.27	445	1	1
192.168.1.100	TCP	2958	WAN1	65.54.189.156	1863	0	0
192.168.1.100	TCP	2942	WAN1	192.168.5.121	49156	0	0
192.168.1.100	TCP	3128	WAN1	118.160.195.248	1894	0	0
192.168.1.100	TCP	2947	WAN1	192.168.5.120	49157	0	0

## Specific Port Status

Enter the service port number in the field and IP that are currently used by this port will be displayed.

### IP/Port Statistic

Enabled IP/Port Statistic Port Port: 0 Search

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2959	WAN1	74.120.121.3	80	8	33
192.168.1.100	TCP	3576	WAN1	203.69.113.18	80	0	0

Refresh



## Appendix A : Configure the 3G USB Interface

Before configure the 3G USB interface, please prepare those device as below:

- USB 3G (WCDMA) Device
- NK Series Router
- 3G SIM & Configuration

For Example: AT&T 3G connection, the parameter as below:

- APN: wap.cingular
- Dialup Number : \*99#
- Username: WAP@CINGULARGPRS.COM (all-uppercase)
- Password: CINGULAR1 (all-uppercase)

**Please follow the configure step as below:**

- Step 1: USB/3G Connection Setting**
- Step 2: Check IP Address for USB/3G Connection**
- Step 3: Check 3G Info from Service Provider**
- Step 4: Configure Advance Setting**
- Step 5: Send System log via SMS Message**

## Step 1: USB/3G Connection Setting

[Sidebar Menu] Network > Network Connection



### [WAN Setting]

Select USB port for 3G/4G connection, and enter detail setting after click hyper-link "Edit" at USB port column.

#### WAN Setting

Please choose how many WAN ports you prefer to use :  (Default: 4)

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	<a href="#">Edit</a>
WAN 2	Obtain an IP automatically	<a href="#">Edit</a>
WAN 3	Obtain an IP automatically	<a href="#">Edit</a>
WAN 4	Obtain an IP automatically	<a href="#">Edit</a>
USB	3G / 3.5G	<a href="#">Edit</a>

Interface:

Connection Type: 3G / 3.5G

PIN CODE:

Reconfirm PIN CODE:

USB Connection Status: 3G modem is not available

APN:

Dial Number:

UserName:


Password:

Use the Following DNS Server Addresses

DNS Server(Required):  .  .  .

DNS Server(Optional):  .  .  .

MTU:  Auto  Manual  bytes

Item	Description
<p><b>PIN CODE</b></p>	<p>Entry PIN code when the PIN protection is enabled at your 3G SIM, but it is not necessary when the function was disabled.</p> <p>PIN CODE: <input type="text"/></p> <p>Reconfirm PIN CODE: <input type="text"/></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> <b>Attention</b> The SIM card will be locked and displays “[PUK] PIN Unlocked Key” when entering incorrect PIN code more than 3 times.</p> </div>
<p><b>USB Connect Status</b></p>	<p>The status filed will display specific description:</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>USB Connection Status : 3G modem is not available</p> </div> <ul style="list-style-type: none"> <li>● 3G modem is connected and works normally.</li> <li>● 3G modem is connected, but it requires the PIN code to enable the 3G service.</li> <li>● 3G modem is connected, but there is no SIM card available. Please insert the SIM card for 3G service.</li> <li>● 3G modem is connected, but the SIM card is locked. Please enter the</li> </ul>

	<p><b>PUK code to unlock.</b></p> <ul style="list-style-type: none"> <li>● <b>3G modem is not available.</b></li> </ul>
<p><b>DNS Server:</b></p>	<p>Router is forced to use assigned DNS Server manually, which is not from ISP settings.</p> <p><input type="checkbox"/> Use the Following DNS Server Addresses</p> <p>DNS Server(Required): <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></p> <p>DNS Server(Optional): <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/></p>
<p><b>3G Setting :</b></p>	<p><b>APN</b>(Access Point Network): most carriers use "Internet " as default value. Need to check with carrier provider for the correct value.</p> <p><b>Dial Number:</b> Default value is *99# for WCDMA-UMTS system.</p> <p><b>User name &amp; Password:</b> Enter suitable authenticated contents if need.</p> <p><b>APN:</b> <input type="text"/></p> <p><b>Dial Number:</b> <input type="text" value="*99#"/></p> <p><b>Username :</b> <input type="text"/></p> <p><b>Password:</b> <input type="text"/></p> <p>※<b>Tip :</b> For Example: AT&amp;T 3G connection</p> <p><b>APN:</b> wap.cingular</p> <p><b>Dialup Number:</b> *99#</p> <p><b>Username:</b> WAP@CINGULARGPRS.COM (all-uppercase)</p> <p><b>Password:</b> CINGULAR1 (all-uppercase)</p>

**Step 2: Check IP Address for USB/3G Connection.****[Sidebar Menu] Home****[WAN Status]****WAN Status**

Interface	WAN 1	WAN 2	WAN 3	WAN 4	USB
WAN IP Address	192.168.4.141	0.0.0.0	0.0.0.0	0.0.0.0	---
Default Gateway	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0	---
DNS	192.168.5.121	0.0.0.0	0.0.0.0	0.0.0.0	---
Downstream Bandwidth Usage	0	0	0	0	---
Upstream Bandwidth Usage	0	0	0	0	---
DDNS Setup	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled	Dyndns Disabled 3322 Disabled
Quality of Service	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connect	Release Renew	Release Renew	Release Renew	Release Renew	

Item	Description
<b>WAN IP Address</b>	Indicates the current IP configuration for USB port.
<b>Default Gateway</b>	Indicates gateway IP address from ISP.
<b>Domain Name Server</b>	Indicates the current DNS IP configuration.
<b>Downstream Bandwidth Rate</b>	Indicates the current downstream bandwidth usage(%) for USB port.
<b>Upstream Bandwidth Rate</b>	Indicates the current upstream bandwidth usage(%) for USB Port.
<b>DDNS Setup</b>	Indicates if Dynamic Domain Name is activated. The default configuration is "Disabled".
<b>QoS</b>	Indicate how many QoS rules are set.
<b>Manual Connect</b>	Disconnect: Stop current connection status. Connect: Change the disconnection to connection.

### [Physical Port Status]

Status cell indicated current connection status for USB Port

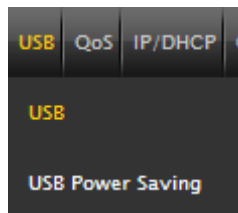
Item	Description
Connected	This 3G/4G device just still connected via USB Port
Enabled	This 3G/4G deice still available & wait to connect

#### Physical Port Status

Port ID	1				
Interface	LAN				
Status	<a href="#">Connect</a>				
Port ID	Internet	Internet	Internet	Internet	USB
Interface	WAN 1	WAN 2	WAN 3	WAN 4	USB
Status	<a href="#">Connect</a>	<a href="#">Enabled</a>	<a href="#">Enabled</a>	<a href="#">Enabled</a>	<a href="#">Enabled</a>

### Step 3: Check 3G Info from Service Provider

#### [Sidebar Menu] USB Setting



Interface : USB  
 Connection Type : 3G Modem

System Provider :

Signal Quality :  Refresh

Charge count :  Disabled  By traffic(KBytes)  By time(Minutes)

Restart the count on  th day every month

Item	Description
Interface	Indicated Current USB Port
Connection Type	Specify Connection Type. Default value is " 3G Modem "
System Provider	Indicated current Service Provider name
Signal Quality	Indicated current Signal Strength

	Push <input type="button" value="Refresh"/> button to get the updated status.
<b>Charge count</b>	Default value is disabled.

### 3G service charge by traffic usage

Charge count :  Disabled  By traffic(KBytes)  By time(Minutes)

Premium :  KBytes  Dollars

Extra Charge :  Dollars / KBytes

Stop connection when total traffic reaches  KBytes

Previous Total Traffic (KBytes) : --

Current total Traffic (KBytes) : --

Charge : --

Restart the count on  th day every month

Item	Description
<b>Premium</b>	The basic service fee for 3G traffic usage
<b>Extra charge</b>	The additional fee after exceeding the premium.
<b>Auto Disconnect</b>	Auto isconnection function when user defines max accumulated traffic to avoid paying unplanned 3G service fee.
<b>Previous Total Traffic</b>	Previous traffic usage record after clean button is pushed.
<b>Current Total Traffic</b>	Current Accumulated traffic usage
<b>Charge</b>	Calculated fee based on current total traffic usage
<b>Restart the count</b>	Auto-flush on the specific date every month
<input type="button" value="Clean"/>	Flush accumulated record manually

### 3G service charge by time usage

Charge count:  Disabled  By traffic(KBytes)  By time(Minutes)

Premium:  Minutes  Dollars

Extra Charge:  Dollars / Minutes

Stop connection when it's over  minutes

Previous Cumulative Time : --

Current Cumulative Time : --

Charge : --

Restart the count on  th day every month

Item	Description
Premium	The basic service fee for 3G time usage
Extra Charge	Billing Rate by Over-basic connected time
Auto-disconnect	Auto isconnection function when user defines max accumulated time to avoid paying unplanned 3G service fee.
Previous Cumulative Time	Previous accumulated time record after clean button is pushed.
Current Cumulative Time	Current Accumulated time
Charge	Calculated fee based on current total time
Restart the count	Auto-flush on the specific date every month
<input type="button" value="Clean"/>	Flush accumulated record manually



## Step 4: Configure Advance Setting

The VPN Security Router supports four USB 3G/4G connection modes.

- **Performance Mode:** 3G service is always connected.
- **Backup mode:** supports WAN failover.
- **Smart mode:** detect the WAN connection status to decide which mode 3G dongle should be in, including active mode, power saving mode, and power off mode.
- **Scheduling mode:** 3G services can be automatically connected following the pre-set time.

### Mode Selection

Disabled  
 Performance Mode (Always connected)  
 Backup Mode  
 Smart Mode  
 Scheduling Mode

Idle time  Minutes

### Performance mode

The performance mode will keep 3G/4G service connected. The power consumption is higher than other modes.

### Backup Mode

The 3G dongle keeps on power-saving mode if all the WAN connections work normally. However, when all the wired WAN connections fail or are disconnected, the 3G services will be connected automatically until any wired WAN connection recovers.

## Trigger Condition

Interface : USB

### Mode Selection

Disabled  
 Performance Mode (Always connected)  
 Backup Mode  
 Smart Mode  
 Scheduling Mode

Idle time  Minutes

### Trigger Condition

	NSD-Start Failover	Threshold-Start Load Balance	
WAN 1:	<input checked="" type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="0"/> kbits	<input type="checkbox"/> Under <input type="text" value="0"/> %
WAN 2:	<input checked="" type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="0"/> kbits	<input type="checkbox"/> Under <input type="text" value="0"/> %
WAN 3:	<input type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="10000"/> kbits	<input checked="" type="checkbox"/> Under <input type="text" value="10"/> %
WAN 4:	<input type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="10000"/> kbits	<input checked="" type="checkbox"/> Under <input type="text" value="10"/> %

Auto Self-test at  :  everyday

Add log for auto self test

## NSD- Start Failover

### 1. The selected wired WAN port is detected failing the connection.

Administrator has to select at least one wired WAN port here. If several wired WAN ports are selected, the 3G dongle will be connected automatically when the selected wired WAN ports all fail the connections.

### 2. Failover

When the router detects the selected wired WAN ports are all connected, the router will return the 3G dongle back to power saving mode.

## Auto self test

Item	Description
Interface : USB	Display USB interface
<input type="checkbox"/> Auto Self-test at <input type="text" value="00"/> : <input type="text" value="00"/> everyday	USB 3G/4G dongle will be activated and run the connection test on a daily basis.
Add log for auto self test	Checkbox for added record to system log for auto self test

## Smart Mode

The router will keep the 3G dongle on power-saving mode based on the idle time set. If all the wired WAN connections work normally, the router will stop providing power for the 3G dongle after the pre-set idle time. However, if all the wired WAN connections fail or are disconnected, the 3G services will return connected automatically until any wired WAN connection recovers.

### Mode Selection

- Disabled  
 Performance Mode (Always connected)  
 Backup Mode  
 Smart Mode  Idle time  Minutes  
 Scheduling Mode


### Trigger Condition

	NSD-Start Failover	Threshold-Start Load Balance	
WAN 1:	<input checked="" type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="10000"/> kbits	<input checked="" type="checkbox"/> Under <input type="text" value="10"/> %
WAN 2:	<input checked="" type="checkbox"/> Enable Failover	<input type="checkbox"/> Over <input type="text" value="0"/> kbits	<input type="checkbox"/> Under <input type="text" value="0"/> %
WAN 3:	<input type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="0"/> kbits	<input checked="" type="checkbox"/> Under <input type="text" value="0"/> %
WAN 4:	<input type="checkbox"/> Enable Failover	<input checked="" type="checkbox"/> Over <input type="text" value="0"/> kbits	<input checked="" type="checkbox"/> Under <input type="text" value="0"/> %

### Threshold- Start Load Balance

After administrator chooses which WAN ports are required for 3G service backup, the administrators can set up bandwidth setting in the threshold- Start Load Balance columns.

In addition to backup WAN port failures, administrators can decide when the traffic is over the bandwidth setting, 3G dongle can be connected for load balance.

 <b>Note</b>	Administrators must click NSD- Start Failover checkbox before configuring the Threshold- Start Load Balance settings.
--	---

#### 1. Configure Threshold- Start Load Balance:

Take the above GUI screenshot for example, when the router detects that WAN1 traffic is over 10000Kbits, 3G services will be connected for load balance.

#### 2. Return to power Saving mode:

During 3G dongle is connected for load balance, the router will keep detecting WAN1 traffic usage. If the WAN1 traffic is lower than 90000Kbits (10% of 10000Kbits), the router will return the 3G dongle back to power saving mode.

### Scheduling Mode

In Schedule mode, administrator can set up time table for USB 3G/4G device connection.

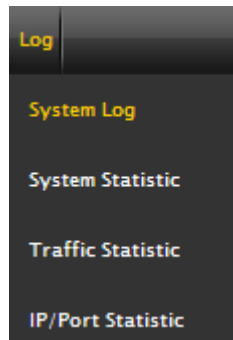
Scheduling Mode

	00:00 to 02:59	03:00 to 05:59	06:00 to 08:59	09:00 to 11:59	12:00 to 14:59	15:00 to 17:59	18:00 to 20:59	21:00 to 23:59
Sun.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mon.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Tue.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wed.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Thu.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fri.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sat.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

USB Active state                       Power saving state

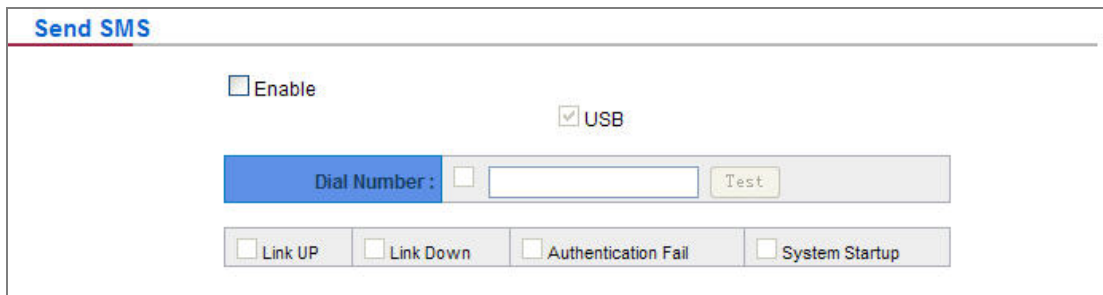
## Step 5: Send System log Via SMS Message

[Sidebar Menu] Log > System Log



### [Send SMS]

Router can send system log to mobile phones via SMS when events are triggered.

A screenshot of the 'Send SMS' configuration page. The page has a title bar with 'Send SMS' in blue. Below the title bar, there is a checkbox for 'Enable' which is unchecked. To the right of 'Enable' is a checkbox for 'USB' which is checked. Below these is a 'Dial Number:' label followed by a text input field and a 'Test' button. At the bottom, there are four checkboxes: 'Link UP', 'Link Down', 'Authentication Fail', and 'System Startup', all of which are unchecked.