User’s Manual

SG-4800

Gigabit SSL VPN Security Router

Security Router

Copyright

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 A 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 SSL 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 SSL 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 SSL VPN Security Router

Model: SG-4800

Rev: 1.0 (June, 2012)

Table of Contents

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 SSL VPN Security Router, SG-4800, 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 SSL VPN Security Router provides a complete security solution in a box. The policy-based firewall, content filtering function and VPN connectivity provides SSL, IPSec, and PPTP VPN. The SSL VPN function supports up to 60 SSL VPN connection tunnels. The IPSec VPN feature provides 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.

This product is built-in bandwidth management function which 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 SG-4800 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 SG-4800 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, IPSec and the SSL VPN. The SSL VPN function supports up to 60 SSL VPN connection tunnels. The 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

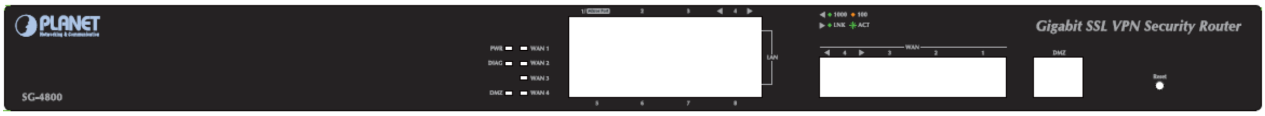
The following items should be included:

- SG-4800 x 1
- Power Cord x 1
- Quick Installation Guide x 1
- User's Manual CD x 1
- Cat5 Cable x 1
- Screw Packer x1
- Rack-mount ear x 2

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

1.3 Physical Specification

Front Panel



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.

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 SSL VPN Security Router
Model		SG-4800
Hardware		
Ethernet	LAN	8x 10/100/1000 Mbps RJ-45
	WAN	4 x 10/100/1000 Mbps RJ-45
	DMZ	1 x 10/100/1000 Mbps RJ-45
Button	Reset	1 x Reset button for reset to factory default setting
	Power	1 x Power on/off Switch
Software		
Multi-WAN Function		● Inbound / Outbound Load Balance: by session and by IP ● Protocol Binding ● Network Service Detection
Routing		● Dynamic Route RIP v1/v2 ● Static Route ● Strategy Routing
System Performance		● Concurrent session :50000 ● Firewall performance :1Gbps ● Corporation Size: SMB(clients 200~250) ● 3DES performance:270Mbps
Bandwidth Management		● Guaranteed Bandwidth ● Max Bandwidth ● Session Limit ● Port-based QoS
Firewall Security		● NAT ● One-to-One NAT ● Multiple-to-One NAT ● Stateful Packet Inspection(SPI) Firewall ● Denial of Service (DoS) prevention ● IP & Port filtering ● Block Website by Keyword, Content Filter ● Firewall detection: Ping of Death, SYN Flooding, Land attack, IP Spoofing ● Email Alert for Hacker Attack ● IP&MAC Binding ● Support DMZ to protect your network: DMZ Host ● Prevent ARP Attack on LAN
Networking		● Configurable DMZ ● DHCP Server (support class C), client, dynamic IP, static IP,IP Grouping support ● Multiple DHCP Server (support 4 sets of Class C) ● PPPoE / Static IP/ DHCP Client ● Multiple Subnet ● Protocol: TCP /IP, ARP, ICMP, FTP/TFTP, IPv4 ● NAT with port forwarding(Virtual Server) ● DNS Relay ● DDNS: Support DynDNS,3322 ● Password protected configuration or management sessions for web access ● Port Management – Speed/Duplex/Auto Negotiation/VLAN ● Transparent Bridge ● Support IPv4/IPv6
Network Management		● Comprehensive web based management and policy setting ● SNMP v1/v2c ● Monitoring, Logging, and Alarms of system activities

		● Firmware upgrade through Web browser
VPN Support	PPTP VPN	● 60 PPTP VPN Tunnels
	IPSec VPN	● 200 IPSec VPN Tunnels ● IPSec H/W acceleration ● Friendly VPN Tunnel Management ● IKE: Pre-Shared keys ● IPSec Encryption DES/3DES/AES128/AES192/AES256 ● IPSec Authentication MD5/SHA1 ● Support PMTU ● NAT Traversal ● Connect on Demand ● DPD detection ● VPN Hub ● IP by DNS Resolved ● View Log
	SSL VPN	● 10 full set SSL VPN tunnel / 50 Virtual Passage SSL VPN Client ● SSL H/W acceleration ● Remote Desktop Access ● HTTP and HTTPs Proxy ● FTP and Windows Network File Sharing ● Terminal Access: Telnet, SSH ● Authentication: Radius, LDAP, Microsoft Active Directory and NT Domain Name ● Platform support Windows / Linux / MAC ● SSL Encryptions: 128bit SHA1 (DES-CBC-SHA) ● Encrypted cookies ● Web cache cleaner ● Certificate Server: RSA, PKI, Digital Certificate ● Host Check: Virus Scan, Personal Firewalls, OS Patch ● Role based management ● Access Policy Management ● Logging and monitoring: Syslog logging of SSL VPN events by user, service and type of event ● Customized User Portal: Allows Portal Layout, Available Services to be customized ● Single sign-on: Allows Single Sign-On for accessing multiple private network resources ● Group and Global Bookmark Support: Enables users to access resources without needing to remember hostnames or IP addresses ● Tunnel quantity upgrade mechanism
	VPN Pass through	● IPSec, PPTP ,L2TP Pass through

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 efficiency, 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 simplize 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.

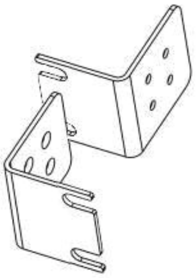
Chapter 3: Hardware Installation

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

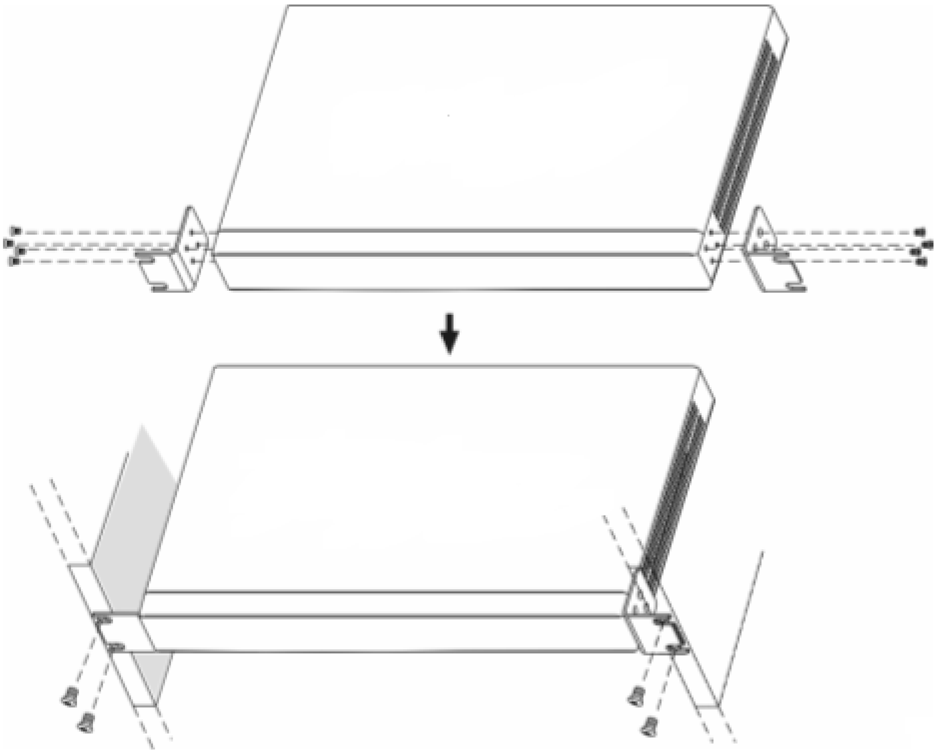
3.1 Installing the Device on a Standard 19" Rack

We suggest to either place the device on a desk or install it in a rack with attached brackets. Do not place other heavy objects together with the device on a rack. Overloading may cause the rack to fail, thus causing damage or danger.

Each device comes with a set of rack installation accessories, including 2 L brackets and 8 screws. Users can rack- mount the device onto the chassis.



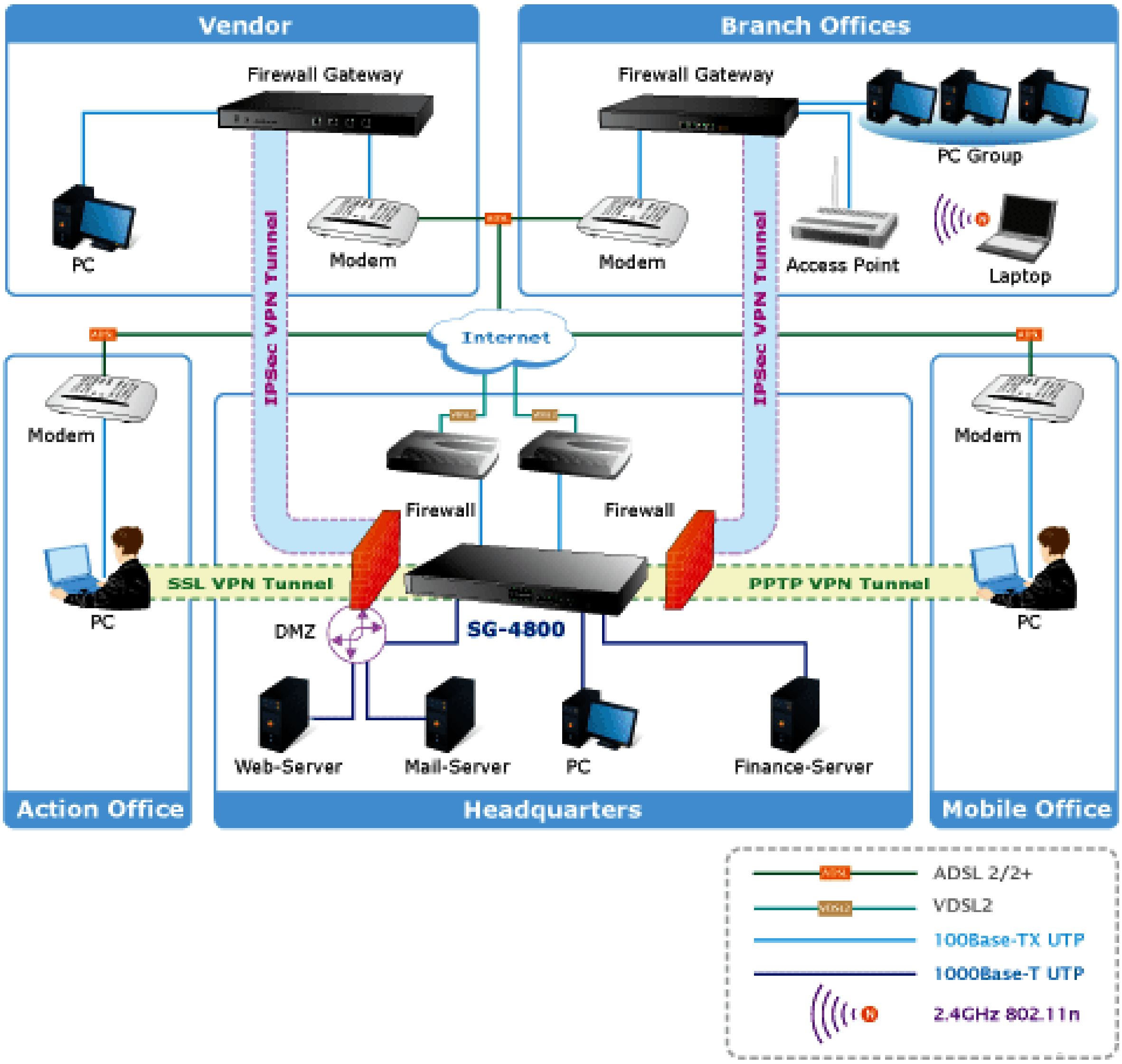
Refer to the figure below for the device installation onto a 19" rack:



✍ **Attention**	In order for the device to run smoothly, wherever users install it, be sure not to obstruct the vent on each side of the device. Keep at least 10cm space in front of both the vents for air convection.

3.2 VPN Router Network Connection

The device has 4 WAN ports and a hardware DMZ port, therefore, users can connect the device to the Internet, and configure a connection to a Public IP server at the same time.



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. The device has 4 WAN ports. If some of the ports are not in use, WAN3 and WAN4 can be set up, through software, as LAN ports. **If only some of the WAN ports are to be used, it is suggested to select WAN1 and WAN2 as the default choices for Internet connection.**

LAN Connection:

The LAN port can be connected to a Switching Hub or directly to a PC.

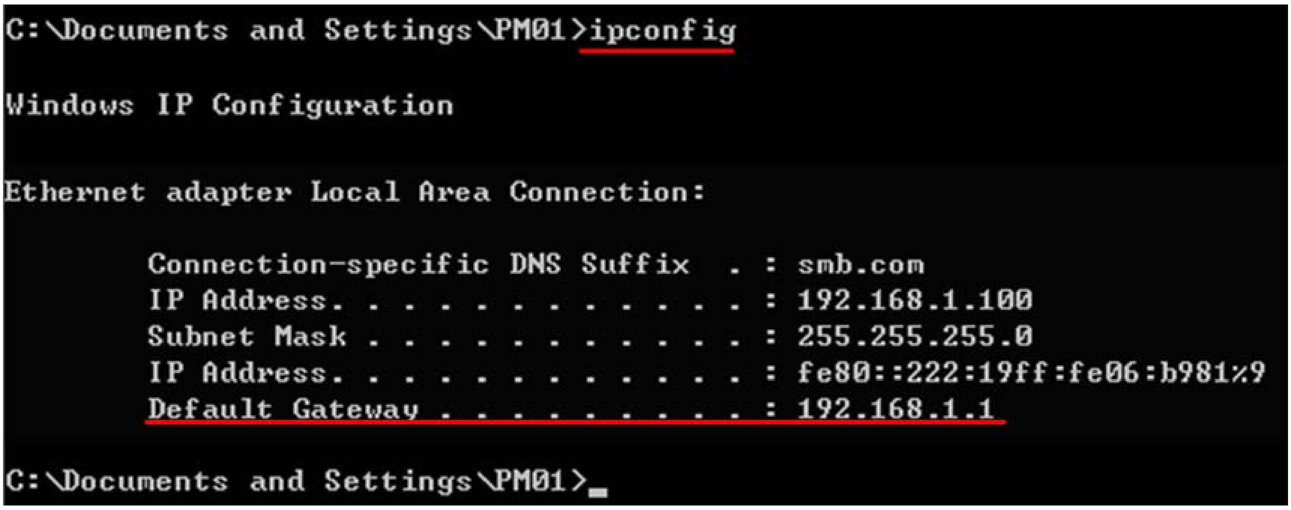
DMZ port:

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.

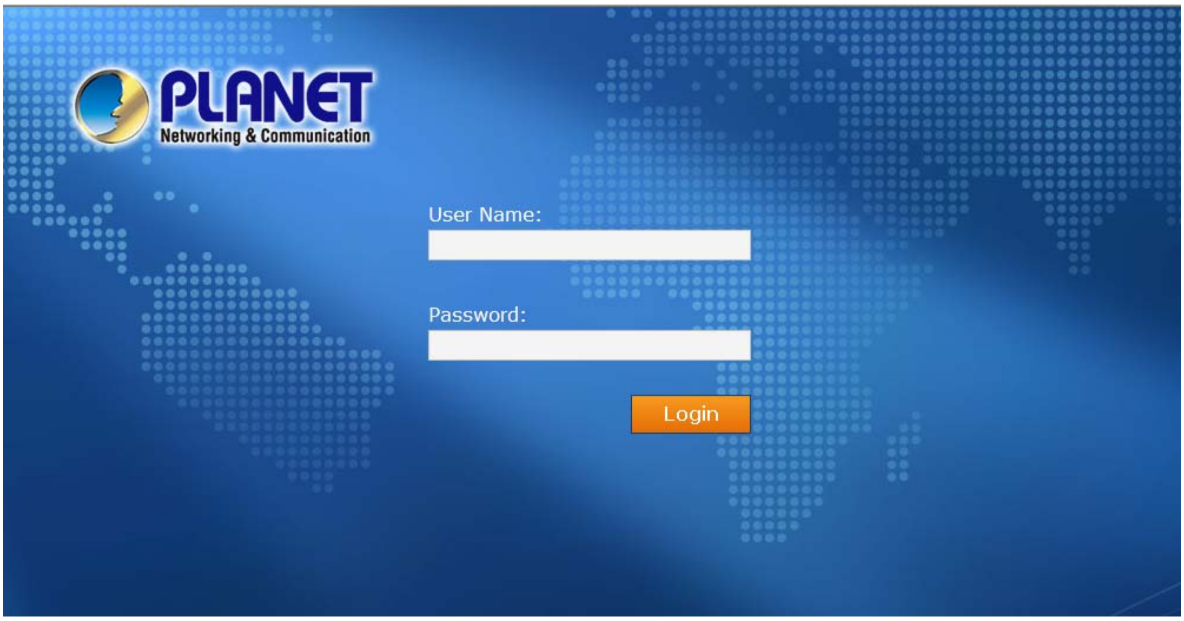
First, check up VPN Router IP address by connecting to DOS through the LAN PC under VPN Security Router. Go to Start → Run, enter cmd to commend DOS, and enter ipconfig for getting Default Gateway address, as the graphic below, 192.168.1.1. Make sure Default Gateway is also the default IP address of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

✍ **Attention**	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.

✍ **Attention**	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.

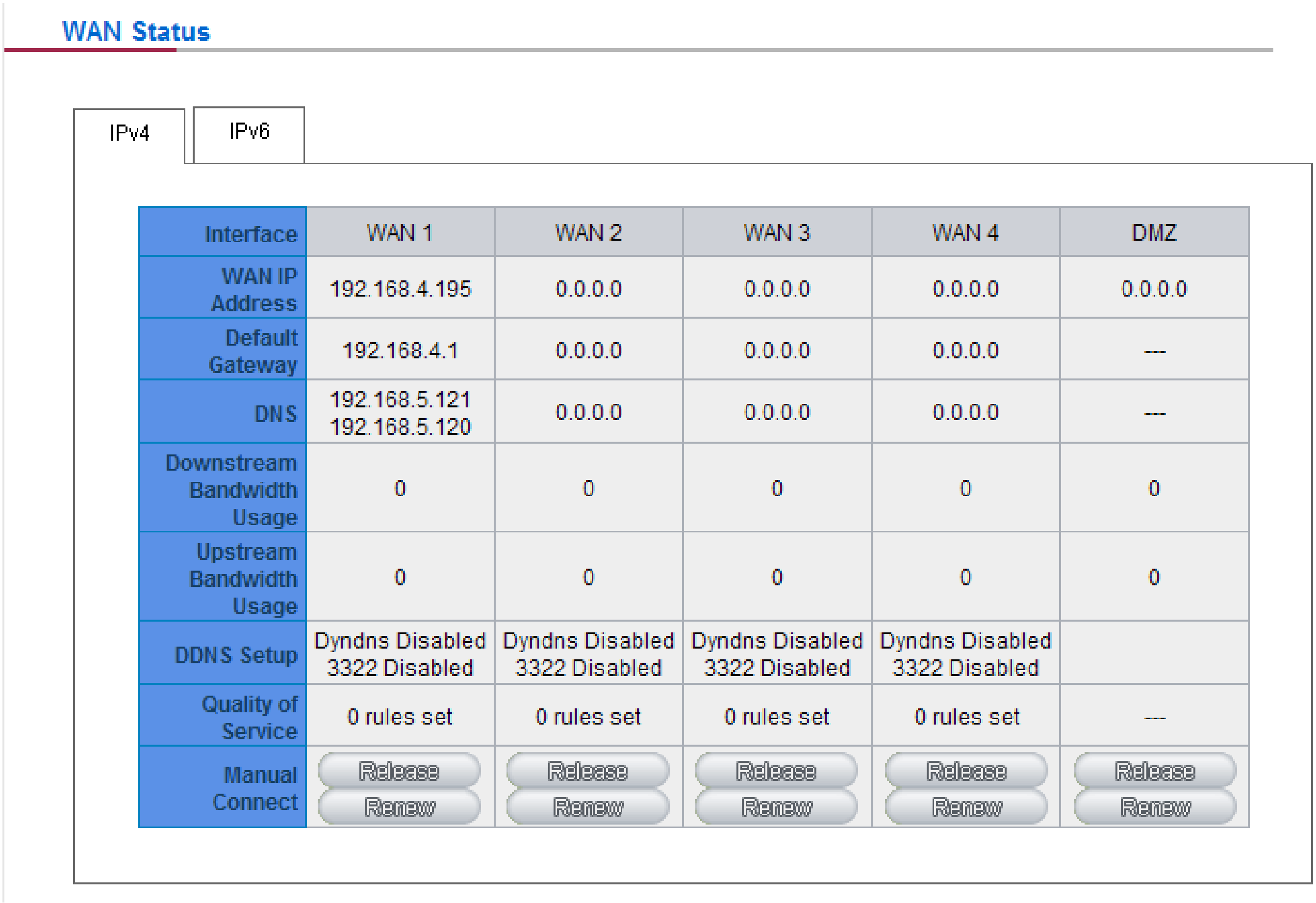
Chapter 5: System Status

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



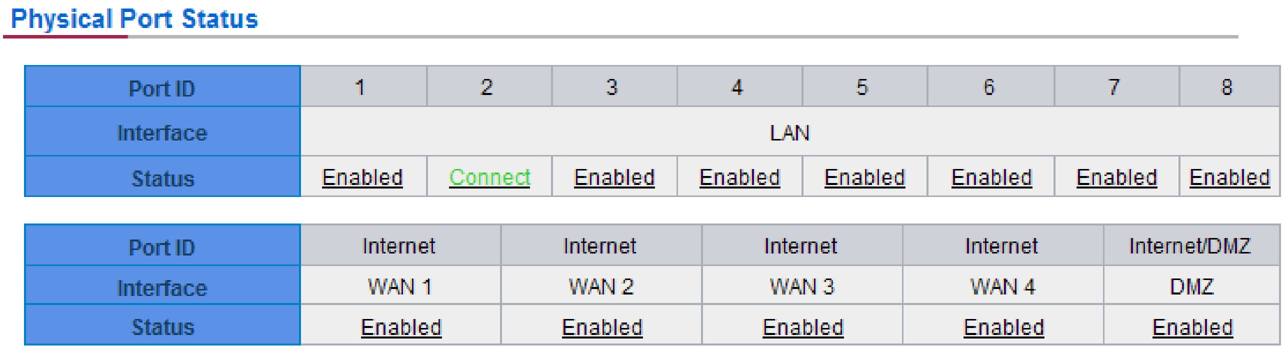
WAN Status

Interface	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
WAN IP Address	192.168.4.195	0.0.0.0	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	192.168.5.121 192.168.5.120	0.0.0.0	0.0.0.0	0.0.0.0	---
Downstream Bandwidth Usage	0	0	0	0	0
Upstream Bandwidth Usage	0	0	0	0	0
DDNS Setup	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	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.
DMZ IP Address	Indicates the current DMZ IP address.

5.1.2 Physical Port Status

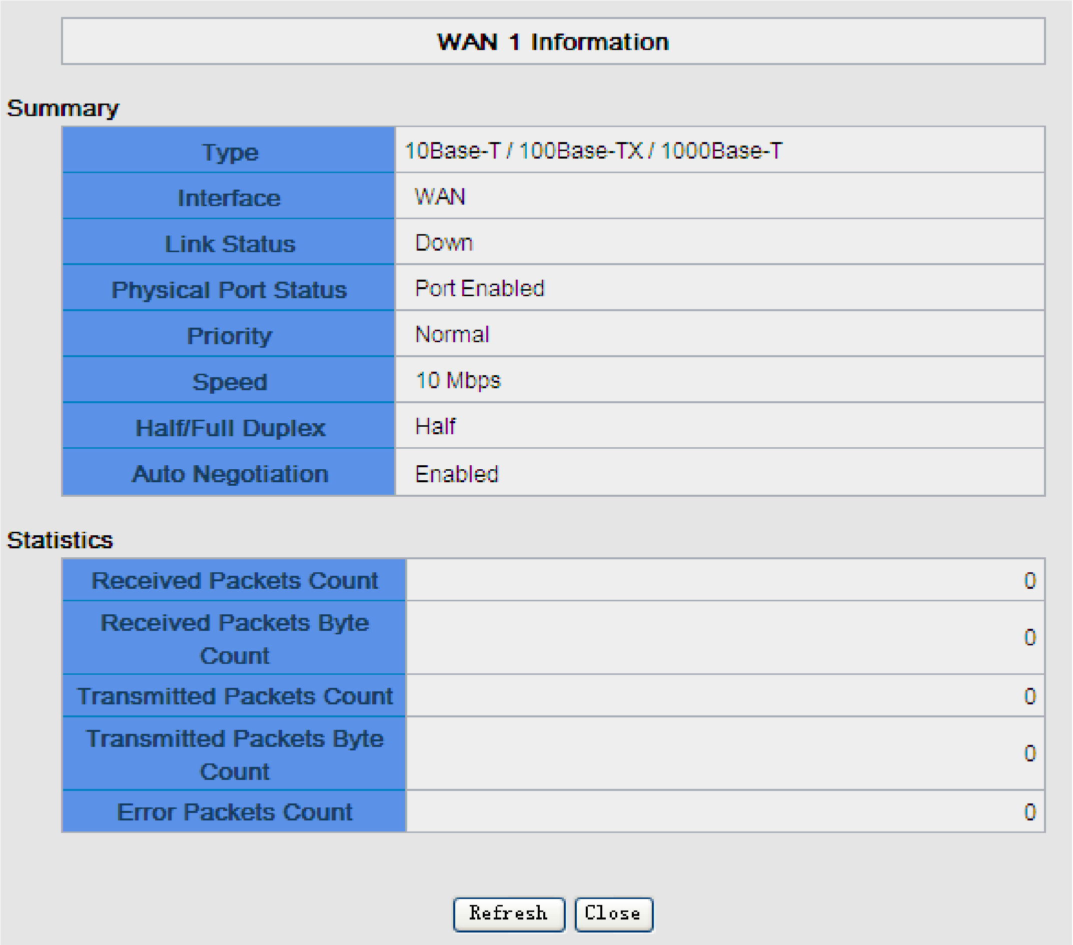


Physical Port Status

Port ID	1	2	3	4	5	6	7	8
Interface	LAN							
Status	Enabled	Connect	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Port ID	Internet	Internet	Internet	Internet	Internet/DMZ
Interface	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
Status	Enabled	Enabled	Enabled	Enabled	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 appeare to show detailed data (including setting status summary and statisitcs) of the selected port.



WAN 1 Information

Summary

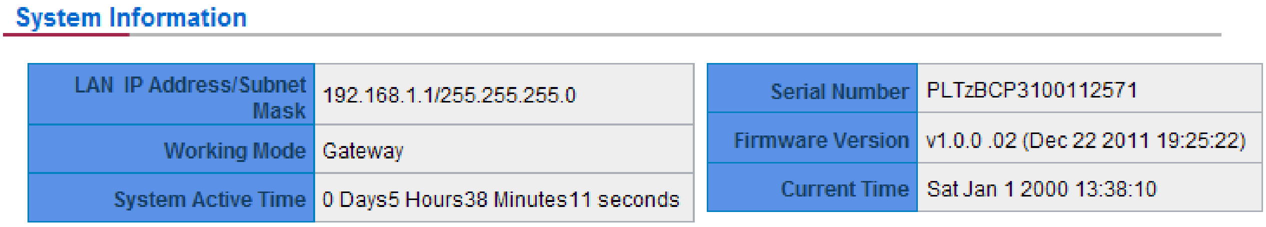
Type	10Base-T / 100Base-TX / 1000Base-T
Interface	WAN
Link Status	Down
Physical Port Status	Port Enabled
Priority	Normal
Speed	10 Mbps
Half/Full Duplex	Half
Auto Negotiation	Enabled

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), iniferface (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 tabble also shows statistics of Receive/ Transmit Packets, Receive/Transmit Packets Byte Count as well as Error Packets Count.

5.1.3 System Information



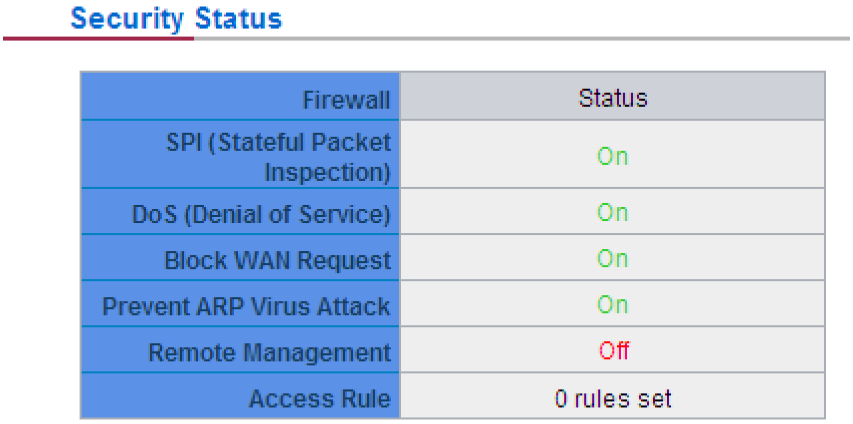
System Information

LAN IP Address/Subnet Mask	192.168.1.1/255.255.255.0
Working Mode	Gateway
System Active Time	0 Days5 Hours38 Minutes11 seconds

Serial Number	PLTzBCP3100112571
Firmware Version	v1.0.0 .02 (Dec 22 2011 19:25:22)
Current Time	Sat Jan 1 2000 13:38:10

Item	Description
LAN IP Address/ Subnet Mask	Identifies the current device IP address and subnet mask. The default is 192.168.1.1 and 255.255.255.0
Working Mode	Indicates the current working mode. Can be Gateway or Router mode. The default is "Gateway" mode
System active time:	Indicates how long the device has been running.
Serial Number:	This number is the device serial number.
Firmware Version	Information about the device present software version.
Current Time	Indicates the device present time. **Note** To have the correct time, users must synchronize the device with the remote NTP server first.

5.1.4 Firewall Status



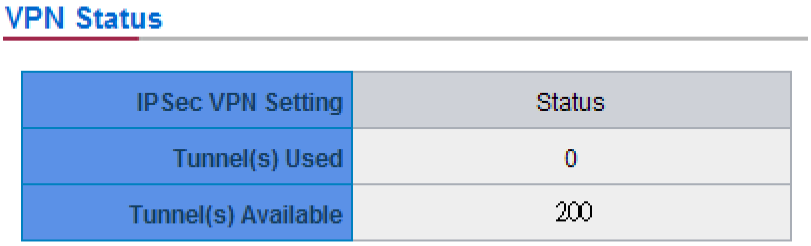
Security Status

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
SPI (Stateful Packet Inspection)	Indicates whether SPI (Stateful Packet Inspection) is on or off. The default configuration is "On".
DoS (Denial of Service)	Indicates if DoS attack prevention is activated.The default configuration is "On".
Block WAN Request	Indicates that denying the connection from Internet is activated. The default

	configuration is "On".
Prevent ARP Virus Attack	Indicates that preventing Arp virus attack is acitvated. The default configuration is "Off".
Remote Management	Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is "Off".
Access Rule	Indicates the number of access rule applied in VPN Security Router.

5.1.5 VPN Status

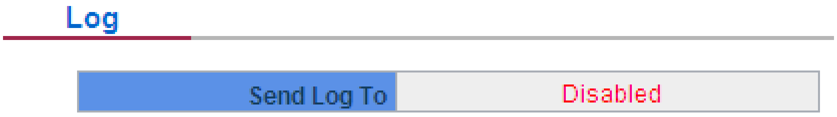


VPN Status

IPSec VPN Setting	Status
Tunnel(s) Used	0
Tunnel(s) Available	200

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

5.1.6 Log Setting Status



Log

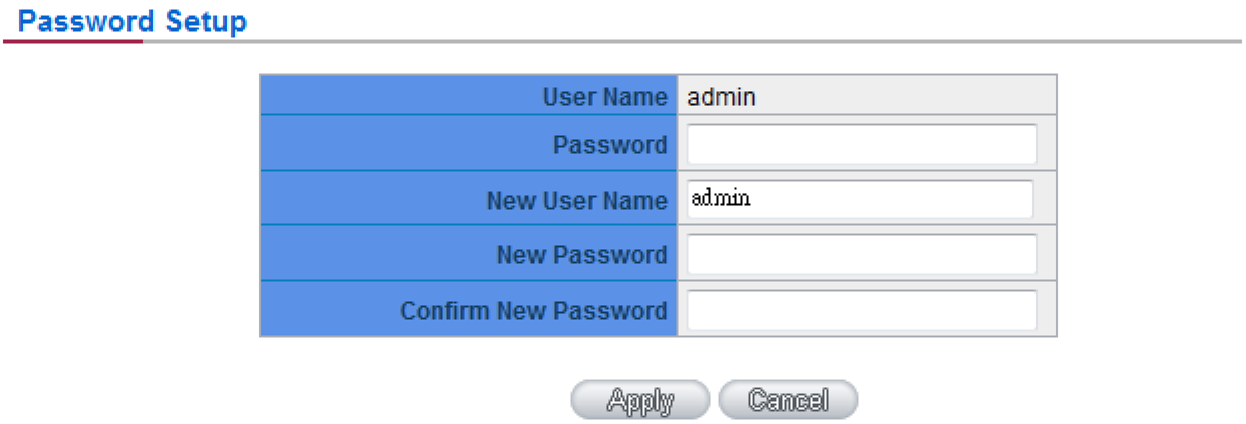
Send Log To	Disabled

Item	**Description**
Sent Log To	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	
New User Name	admin
New Password	
Confirm New Password	

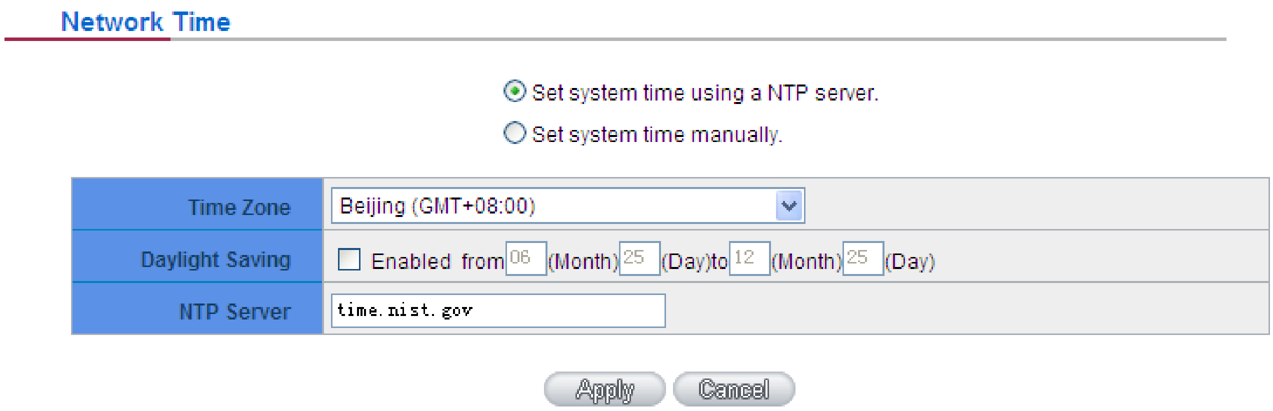
Item	Description
User Name	The default is "**admin**".
Password	Input the original password.（The default is "**admin**".）
New User Name	Input the new user name. e.x. Planet
New Password	Input the new password.
Confirm New Password	Input the new password again for verification.
Apply	Click **"Apply"** 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 Network 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

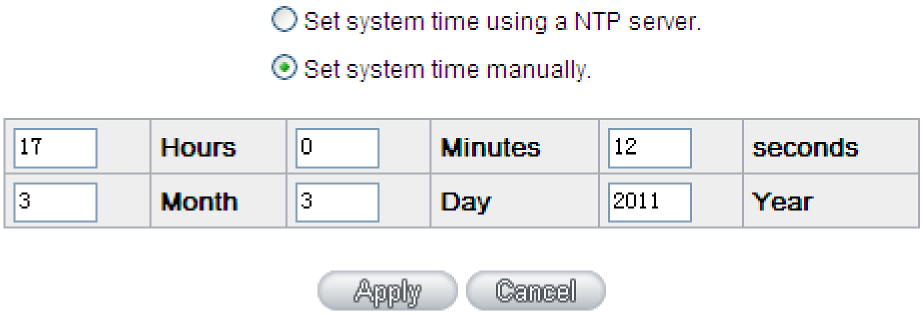
● Set system time using a NTP server.

○ Set system time manually.

Time Zone	Beijing (GMT+08:00)
Daylight Saving	□ Enabled from 06 (Month) 25 (Day)to 12 (Month) 25 (Day)
NTP Server	time.nist.gov

Item	**Description**
Time Zone	Select your location from the pull-down time zone list to show correct local time.
Daylight Saving	If there is **Daylight Saving Time** in your area, input the date range. The device will adjust the time for the Daylight Saving period automatically.
NTP Server	If you have your own preferred time server, input the server IP address.
Apply	After the changes are completed, 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.

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	Hours	0	Minutes	12	seconds
3	Month	3	Day	2011	Year

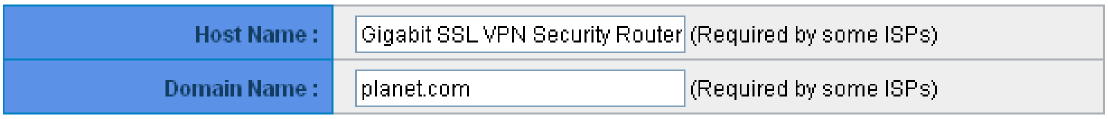
After the changes are completed, click **"Apply"** to save the configuration. Click **"Cancel"** to leave without making any change. This action will be effective before "Apply" to save the configuration.

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

6.1.1 Host Name and Domain Name

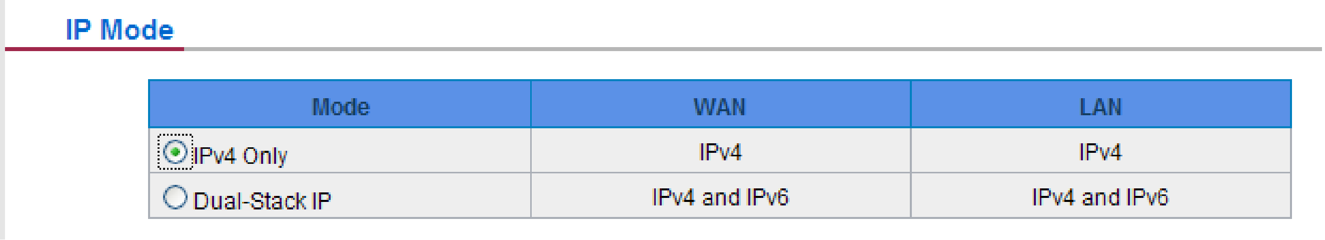


Host Name :	Gigabit SSL VPN Security Router (Required by some ISPs)
Domain Name :	planet.com (Required by some ISPs)

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 IP Mode

Choose the type of addressing to use on your network:



IP Mode

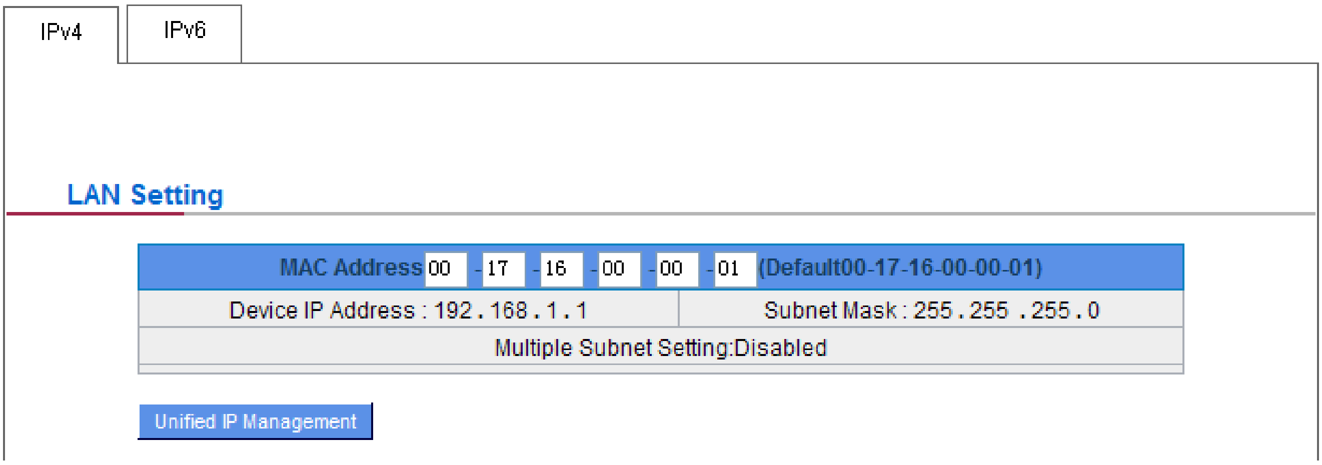
Mode	WAN	LAN
● IPv4 Only	IPv4	IPv4
○ Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4 Only: Use only IPv4 addressing.

Dual-Stack IP: Use IPv4 and IPv6 addressing. So that you can configure both IPv4 and IPv6 addresses for LAN, WAN, and DMZ settings on this page.

6.1.3 LAN Setting

6.1.3.1 IPv4 Only



LAN Setting

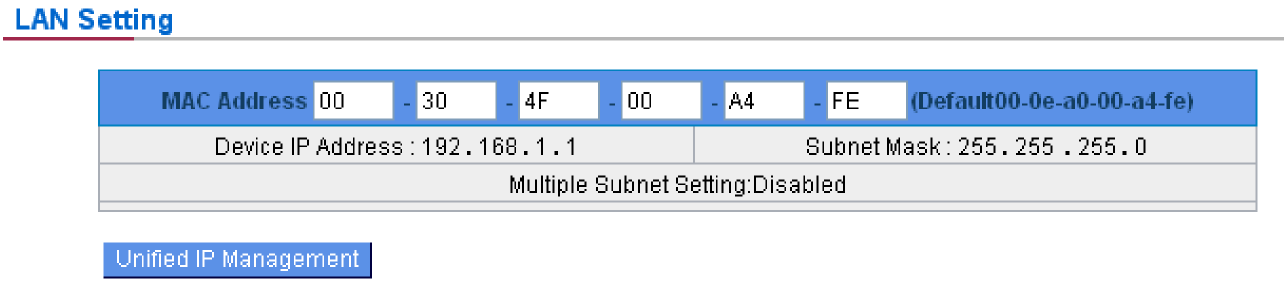
MAC Address 00 - 17 - 16 - 00 - 00 - 01 (Default00-17-16-00-00-01)

Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0
Multiple Subnet Setting:Disabled	

This is configuration information for SG-4800 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： (IPv4 Only)

Click "Unified IP Management" to enter the configuration page, as shown in the following figure. Input the respective IP addresses and subnet masks.

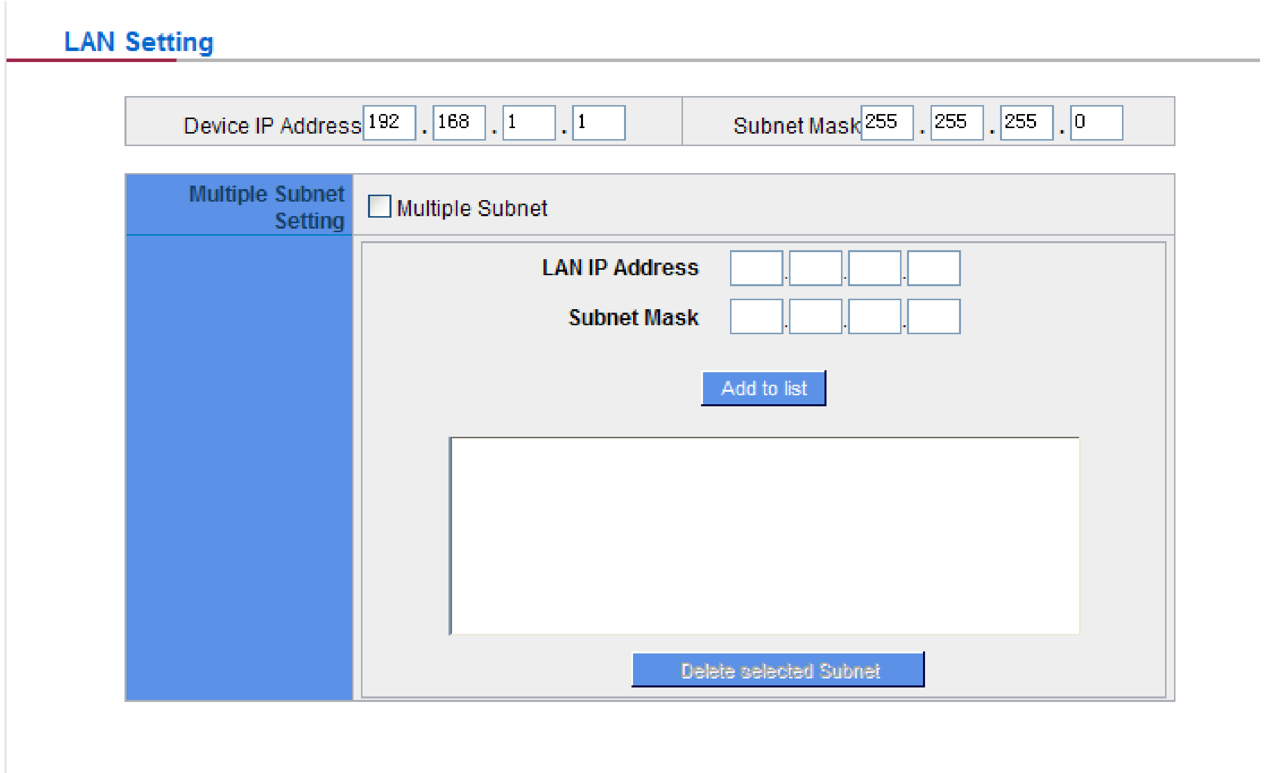


LAN Setting

MAC Address 00 - 30 - 4F - 00 - A4 - FE (Default00-0e-a0-00-a4-fe)

Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0
Multiple Subnet Setting:Disabled	

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.



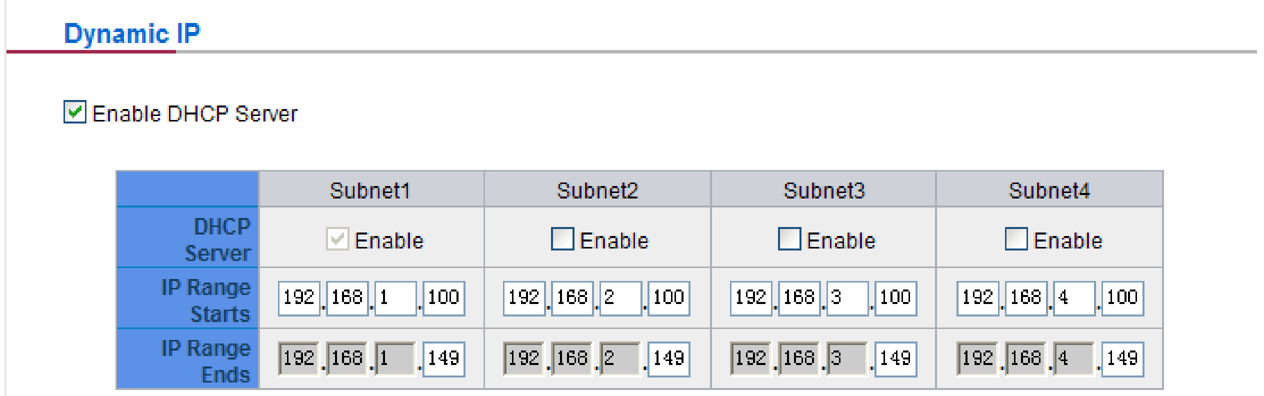
LAN Setting

Device IP Address 192 . 168 . 1 . 1 Subnet Mask 255 . 255 . 255 . 0

Multiple Subnet Setting: □ Multiple Subnet

LAN IP Address

Subnet Mask



Dynamic IP

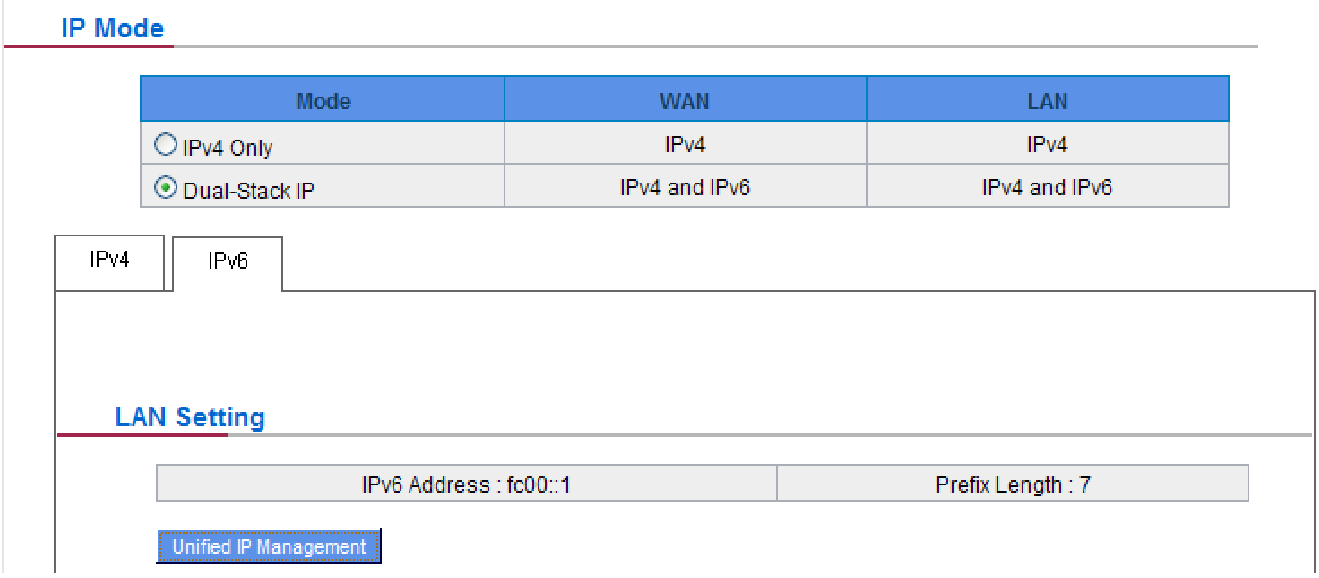
☑ Enable DHCP Server

	Subnet1	Subnet2	Subnet3	Subnet4
DHCP Server	☑ Enable	□ Enable	□ Enable	□ 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

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.

6.1.3.2 Dual-Stack IP (IPv4 and IPv6)

Users have to enable **Dual-Stack IP** in the IP mode section in advance to configure IPv6. Then click the **IPv6** tab, and then enter the IPv6 Address and the Prefix Length. The default IP address is **fc00::1**, and the default prefix length is **7**. It can be changed according to the actual network structure.



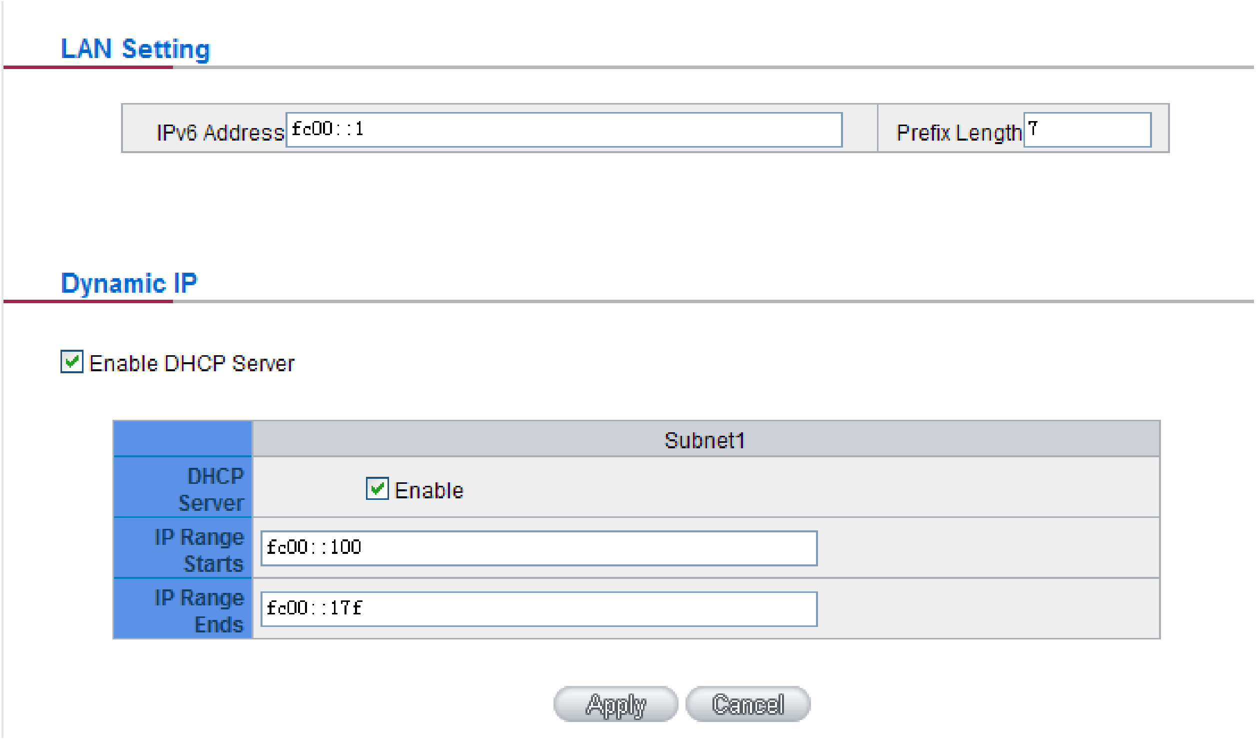
IP Mode

Mode	WAN	LAN
○ IPv4 Only	IPv4	IPv4
● Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

LAN Setting

IPv6 Address : fc00::1	Prefix Length : 7

Click "Unified IP Management" to enter the configuration page, as shown in the following figure. Input the respective IP addresses and subnet masks.



LAN Setting

IPv6 Address fc00::1 Prefix Length 7

Dynamic IP

☑ Enable DHCP Server

	Subnet1
DHCP Server	☑ Enable
IP Range Starts	fc00::100
IP Range Ends	fc00::17f

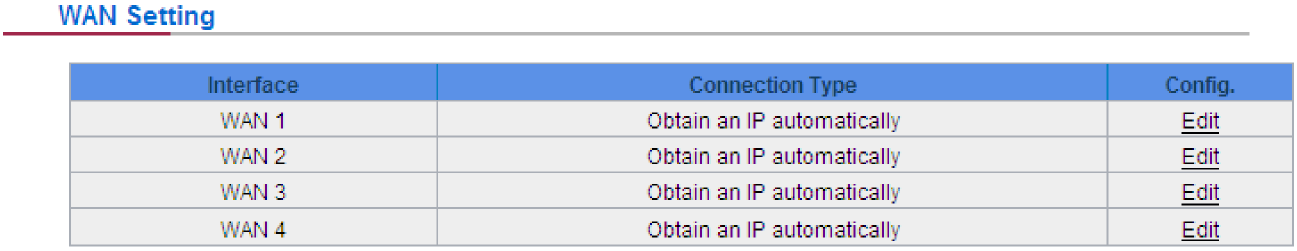
✍ Note	To configure global IPv6 prefixes for your LAN devices, go to the WAN Setting, click the **IPv6** tab, and click **Edit** for the WAN interface. Then enter the LAN IPv6 Address.

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

6.1.4 WAN & DMZ Settings

6.1.4.1 IPv4 Only

WAN Setting



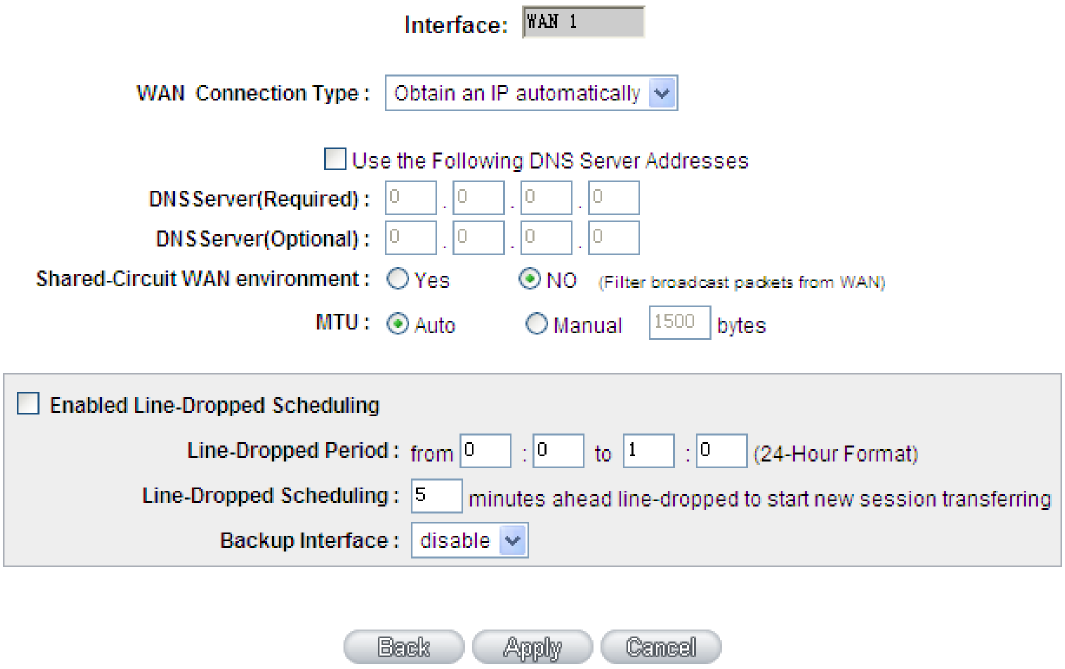
WAN Setting

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	Edit
WAN 2	Obtain an IP automatically	Edit
WAN 3	Obtain an IP automatically	Edit
WAN 4	Obtain an IP automatically	Edit

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 1

WAN Connection Type : Obtain an IP automatically

□ Use the Following DNS Server Addresses

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

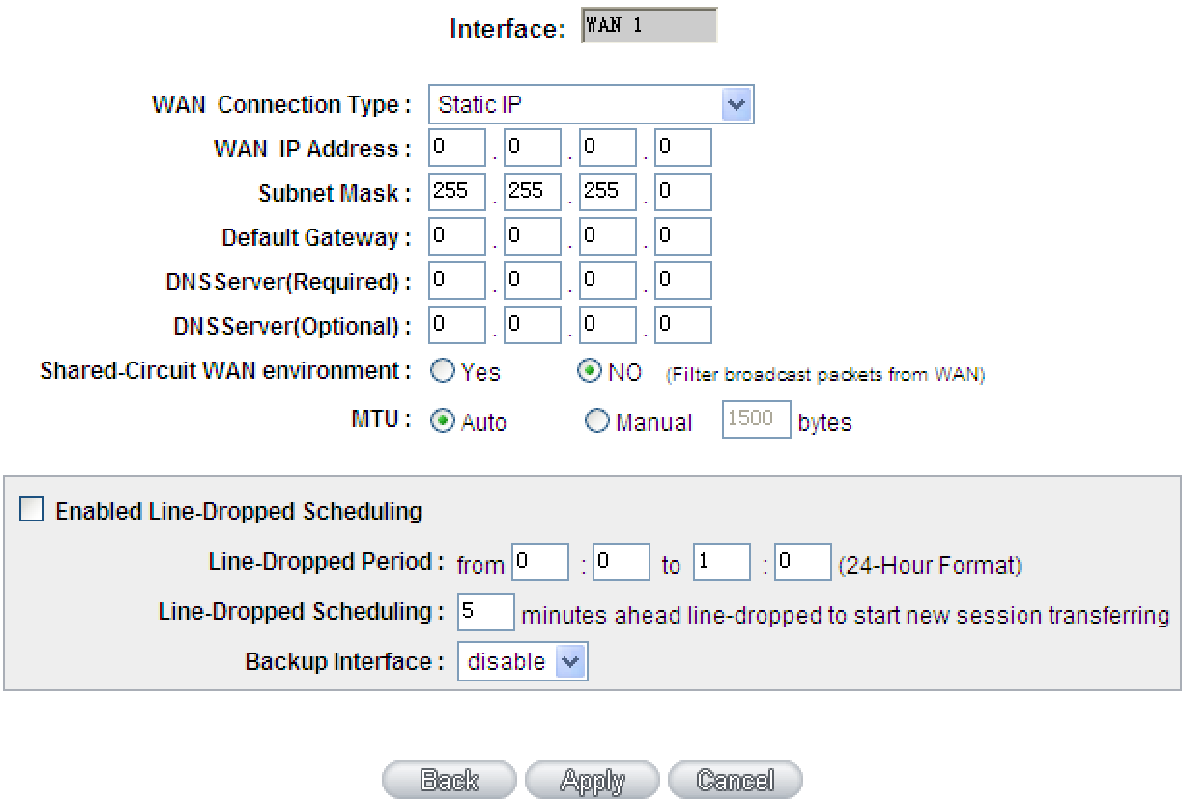
Backup Interface : disable

Item	Description
Use the following DNS Server Addresses:	Select a user-defined DNS server IP address.
DNS Server:	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable groups is two IP groups.
Enable Line-Dropped Scheduling:	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.
Line-Dropped Period	Input the time rule for disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU:	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

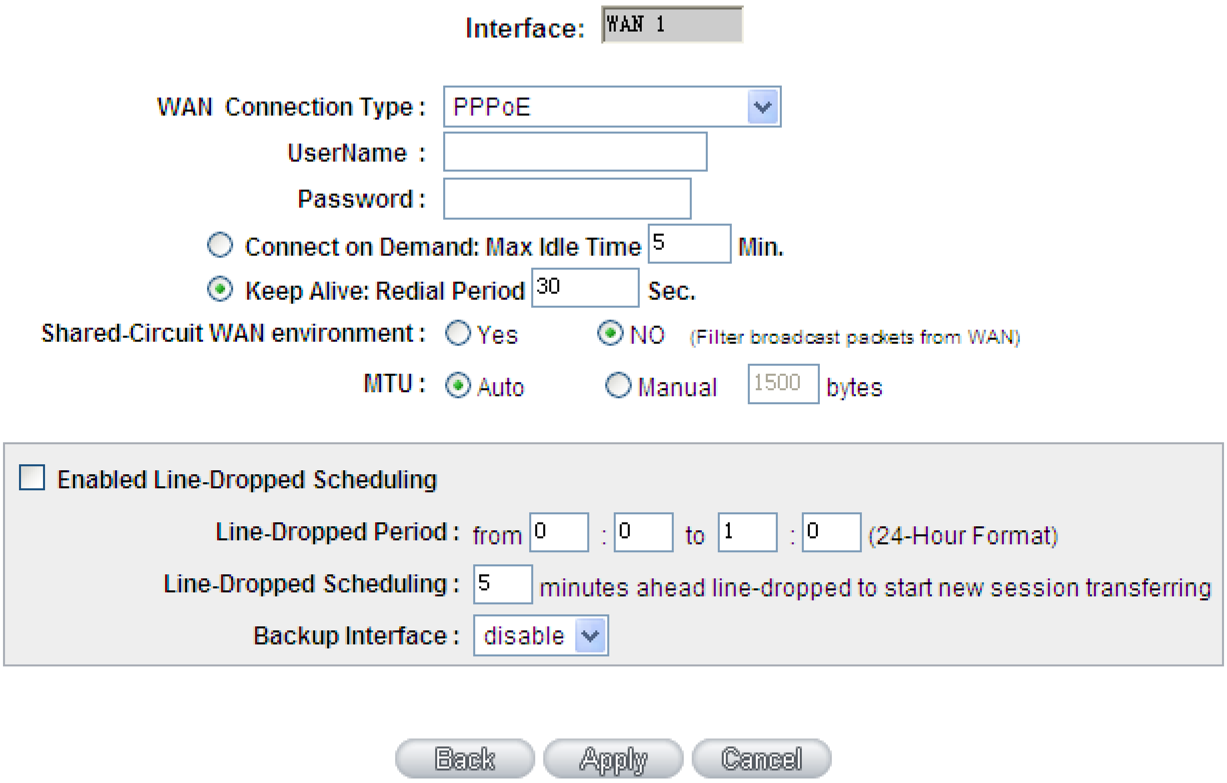
Item	Description
WAN IP address	Input the available static IP address issued by ISP.
Subnet Mask	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway	Input the default gateway 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.
DNS Server	Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
Enable Line-Dropped Scheduling	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.

Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	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 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

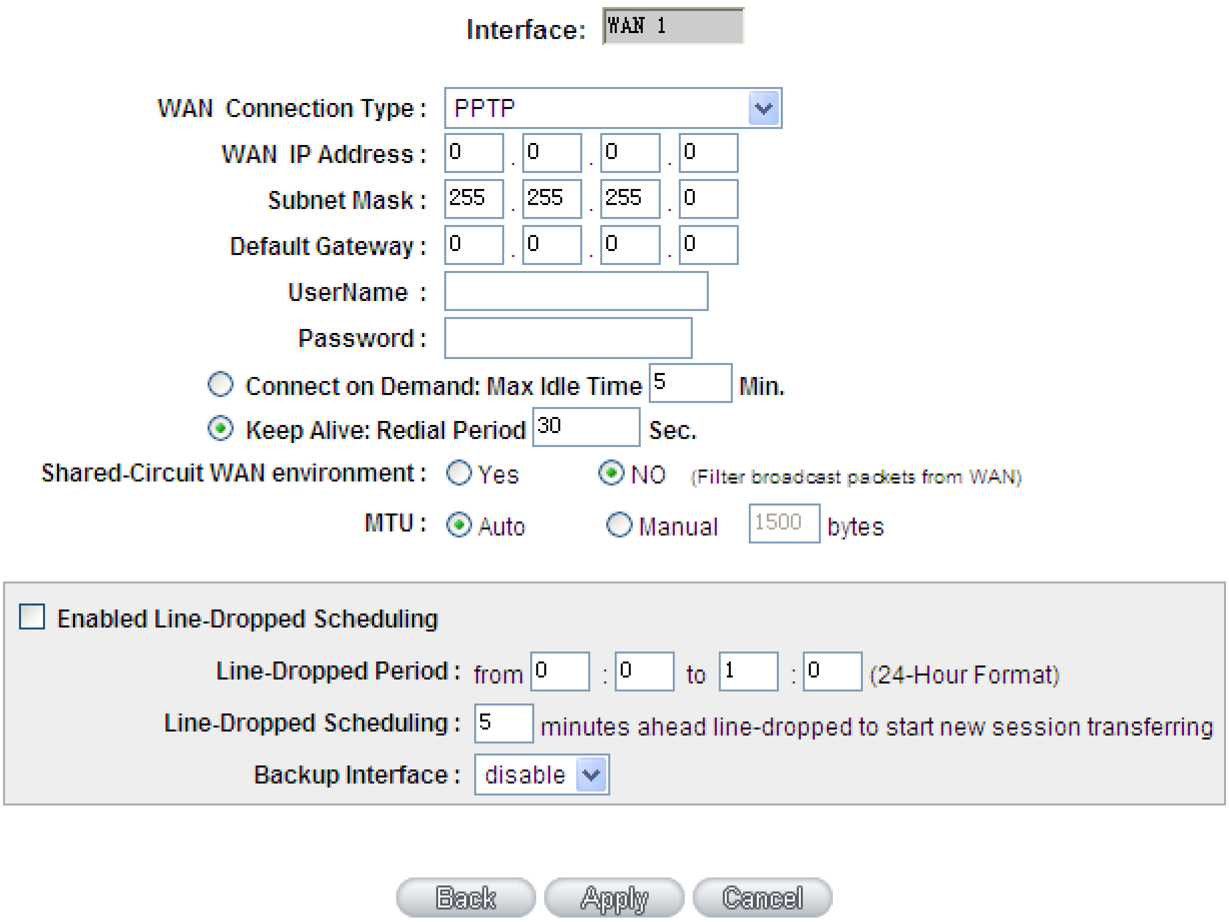
Backup Interface : disable

Item	Description
User Name	Input the user name issued by ISP.
Password	Input the password issued by ISP.
Connect on Demand	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).
Keep Alive	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.
Enable Line-Dropped Scheduling	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.
Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	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
WAN IP Address	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).
Subnet Mask	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
Default Gateway Address	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
User Name	Input the user name issued by ISP.

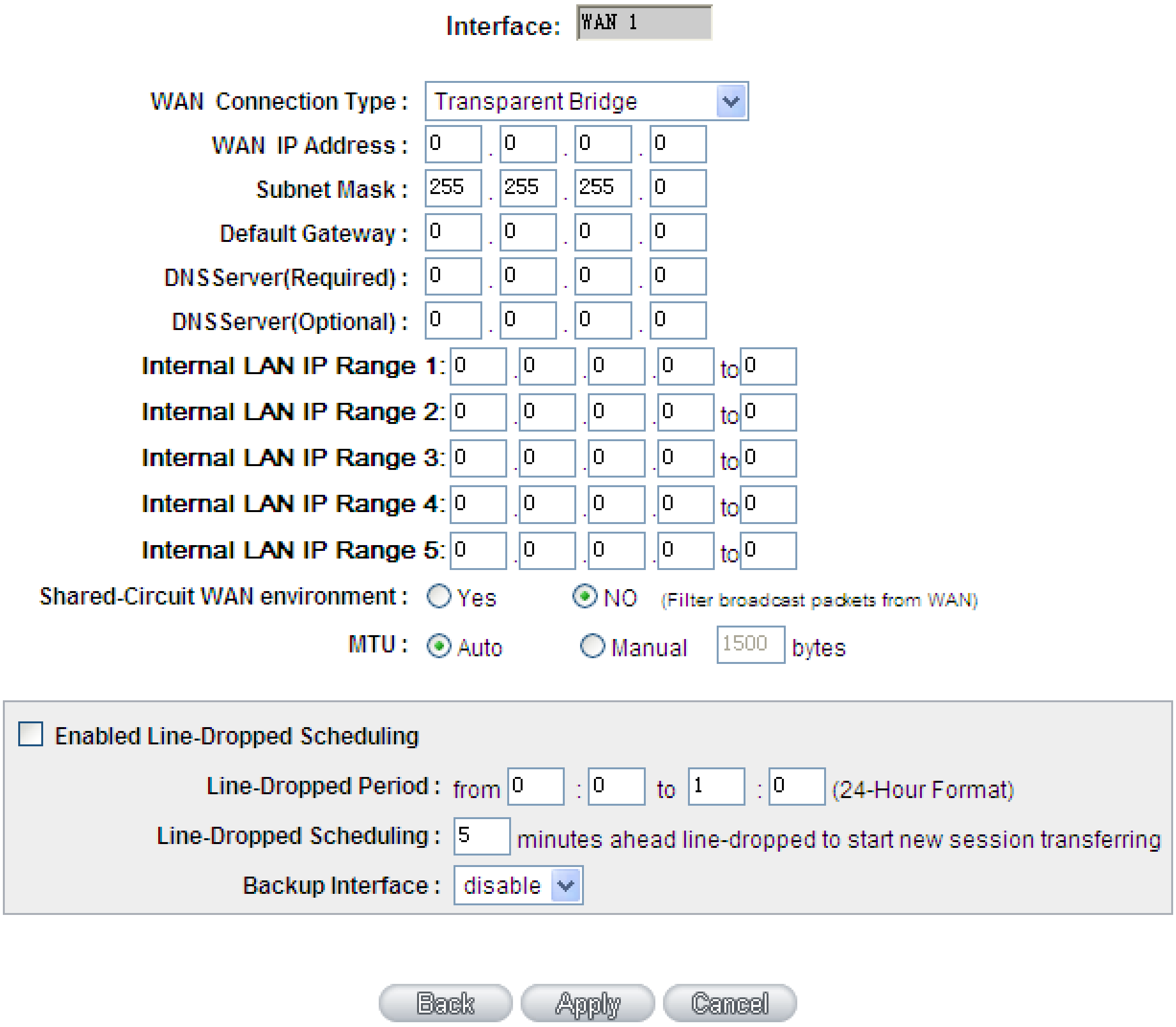
Password	Input the password issued by ISP.
Connect on Demand	This function enables the auto-dialing function to be used for a PPTP dial connection. When the client port attempts to connect with the Internet, the device will automatically connect with the default ISP auto dial connection; when the network 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).
Keep Alive	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.
Enable Line-Dropped Scheduling	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.
Line-Dropped Period	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	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

Item	Description
WAN IP Address	Input one of the static IP addresses issued by ISP.
Subnet Mask	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
Default Gateway Address	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.

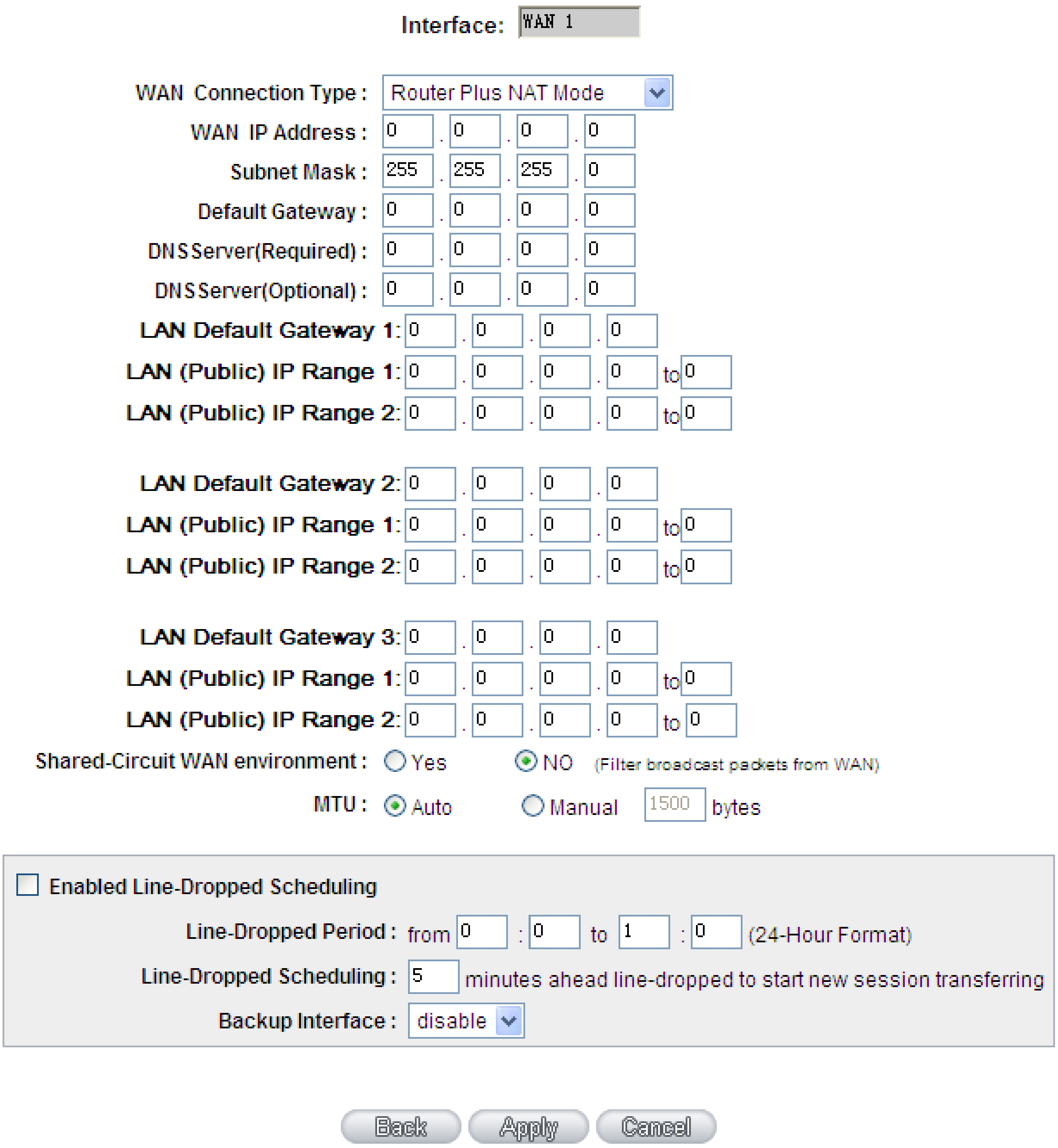
DNS Server	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
Internal LAN IP Range	Input the available IP range issued by ISP. If ISP issued two discontinuous IP address ranges, users can input them into Internal LAN IP Range 1 and Internal LAN IP Range 2 respectively.
Enable Line-Dropped Scheduling	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.
Line-Dropped Period:	Input the time rule for the disconnection of this WAN service.
Line-Dropped Scheduling:	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	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 : 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

LAN Default Gateway 1: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 0 . 0 . 0 . 0 to 0

LAN Default Gateway 2: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 0 . 0 . 0 . 0 to 0

LAN Default Gateway 3: 0 . 0 . 0 . 0

LAN (Public) IP Range 1: 0 . 0 . 0 . 0 to 0

LAN (Public) IP Range 2: 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

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

WAN default gateway	Enter the WAN default gateway, which provided by your ISP.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
Intranet routing default gateway	Enter one of IP addresses that provide by the ISP as your default gateway.
Intranet IP addresses range	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.
Enable Line-Dropped Scheduling	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.
Line-Dropped Period	Input the time rule for disconnection of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be disconnected before the newly added connections should go through another WAN to connect with the Internet.
Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Link Backup Interface	Select another WAN port as link backup when port binding is configured. Users should select the port that employs the same ISP.
Shared- Circuit WAN environment:	If your WAN connects to a Switch, select "Enabled" to filter broadcast packets. The default is "Disabled".
MTU	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".

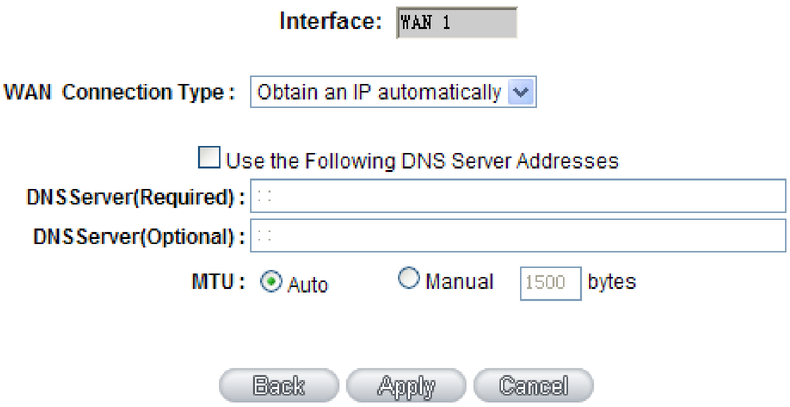
Click **"Apply"** to save the configuration, or click **"Cancel"** to leave without making any changes.

6.1.4.2 Dual-Stack IP (IPv4 and IPv6)

Users have to enable **Dual-Stack IP** in the IP mode section in advance to configure the WAN with IPv6 addressing.

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 1

WAN Connection Type : Obtain an IP automatically

□ Use the Following DNS Server Addresses

DNS Server(Required) : : :

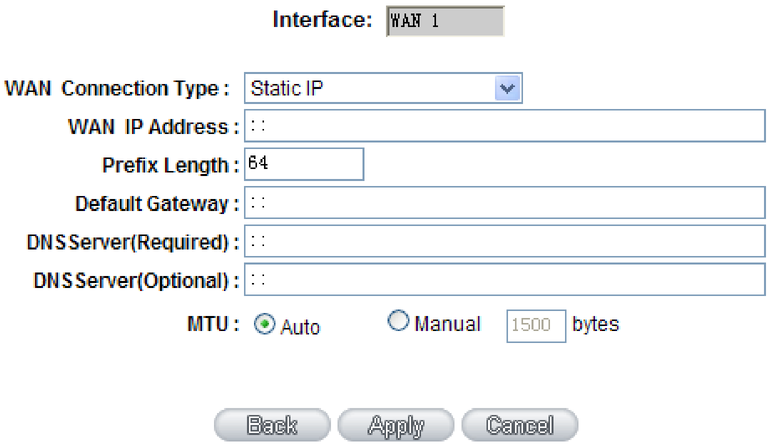
DNS Server(Optional) : : :

MTU : ● Auto ○ Manual 1500 bytes

Item	Description
Use the Following DNS Server Addresses	Select an user-defined DNS server IP address.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
MTU	"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".
Use the Following DNS Server Addresses	Select an user-defined DNS server IP address.

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 : ::

Prefix Length : 64

Default Gateway : ::

DNSServer(Required) : ::

DNSServer(Optional) : ::

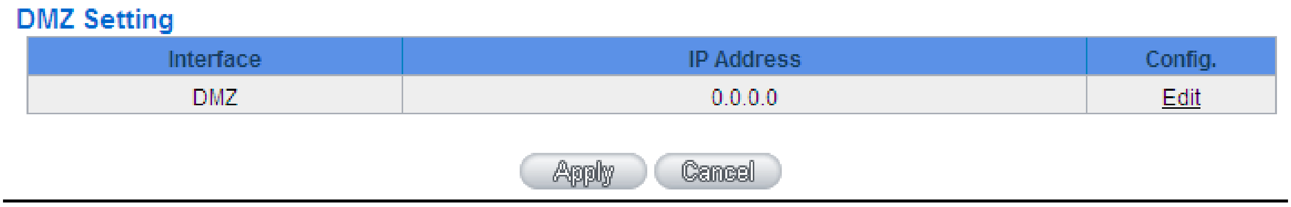
MTU : ● Auto ○ Manual 1500 bytes

Item	Description
WAN IP Address	Input the available static IP address issued by ISP.
Prefix Length	The prefix length specified by your ISP.
Default Gateway	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.
DNS Servers	Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
MTU	"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

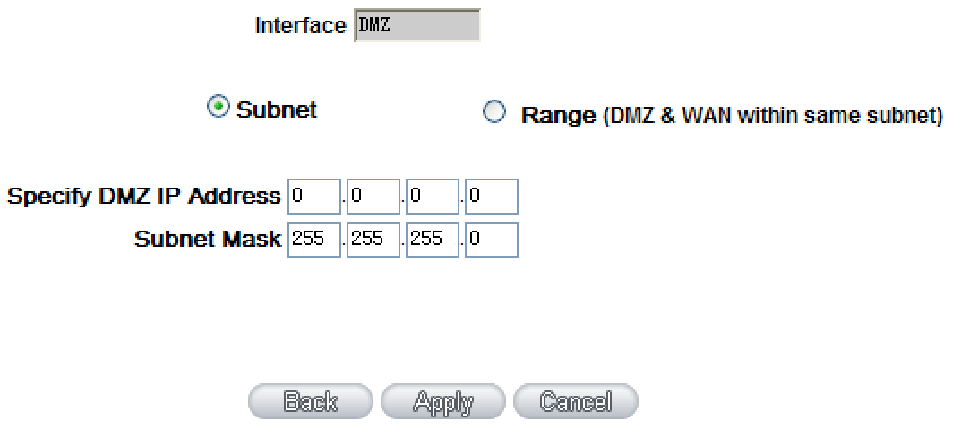
Interface	IP Address	Config.
DMZ	0.0.0.0	Edit

Item	Description
IP address	Indicates the current default static IP address.
Config.	Indicates an advanced configuration modification: Click **Edit** 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 DMZ

● Subnet ○ Range (DMZ & WAN within same subnet)

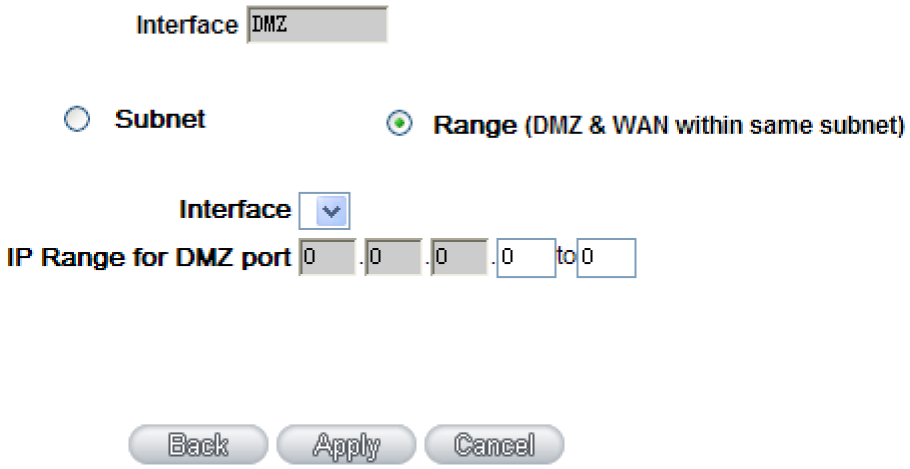
Specify DMZ IP Address 0 . 0 . 0 . 0

Subnet Mask 255 . 255 . 255 . 0

Item	Description
Specify DMZ IP Address	Enter the DMZ Port IP Address
Subnet Mask	Enter the DMZ Port Subnet Mask

Range

DMZ and WAN are within same Subnet



Interface DMZ

○ Subnet ● Range (DMZ & WAN within same subnet)

Interface

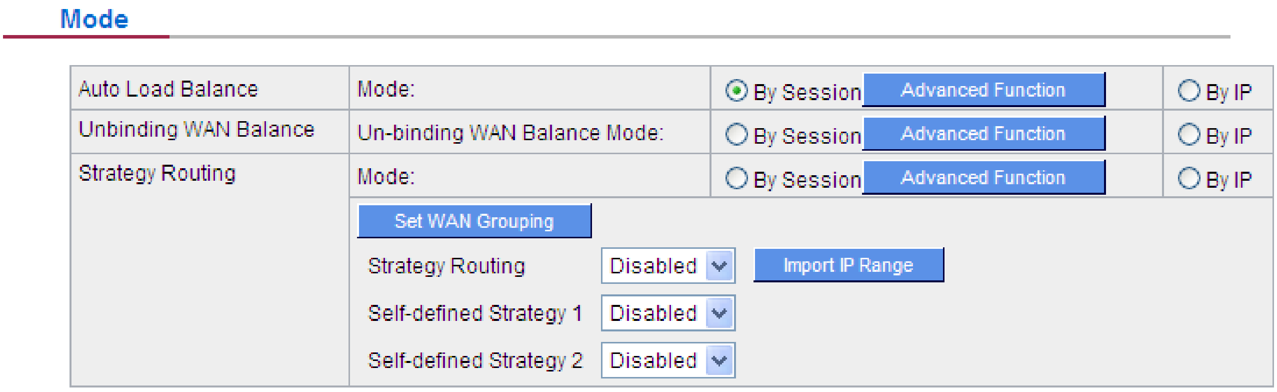
IP Range for DMZ port 0 . 0 . 0 . 0 to 0

Item	Description
Interface	Select a WAN Port witch is the same subnet with DMZ
IP Range for DMZ port	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.

6.2 Multi- WAN Setting

6.2.1 Load Balance Mode



Mode

Auto Load Balance	Mode:	● By Session Advanced Function	○ By IP
Unbinding WAN Balance	Un-binding WAN Balance Mode:	○ By Session Advanced Function	○ By IP
Strategy Routing	Mode:	○ By Session Advanced Function	○ By IP

Set WAN Grouping

Strategy Routing: Disabled — Import IP Range

Self-defined Strategy 1: Disabled

Self-defined Strategy 2: 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
Session Balance	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
IP Session Balance	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**
Session Balance:	If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.
IP Balance:	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.

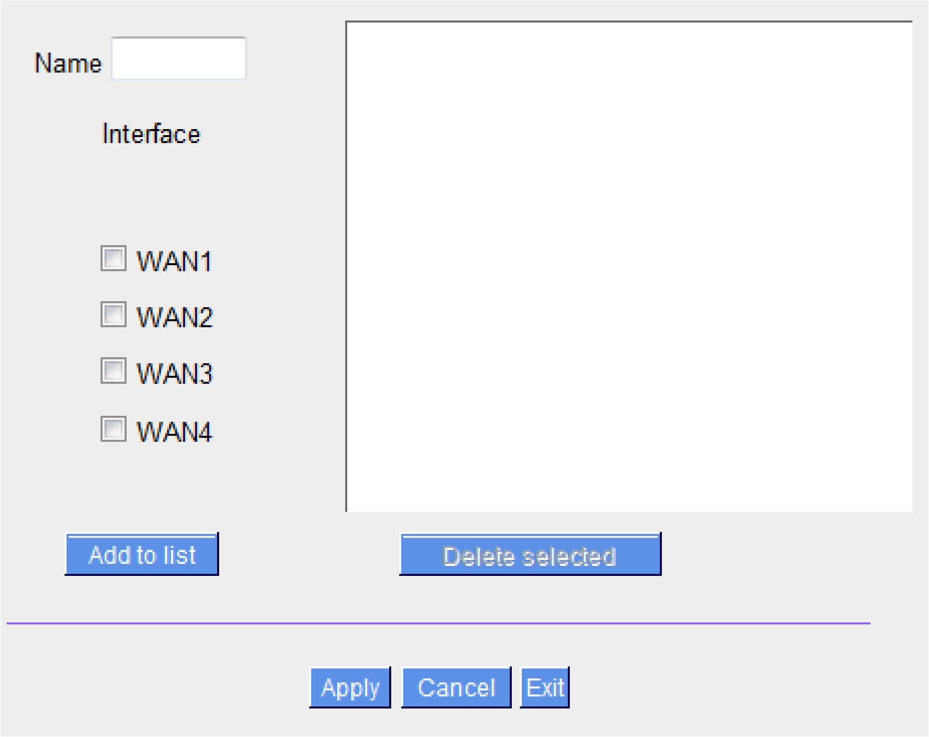
✍ **Attention**	When assigning mode is selected, as in the above example, the IP(s) or service provider(s) configured in the connection rule will follow the rule for external connections, but those which are not configured in the rule will still follow the device Load Balance system to go through other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



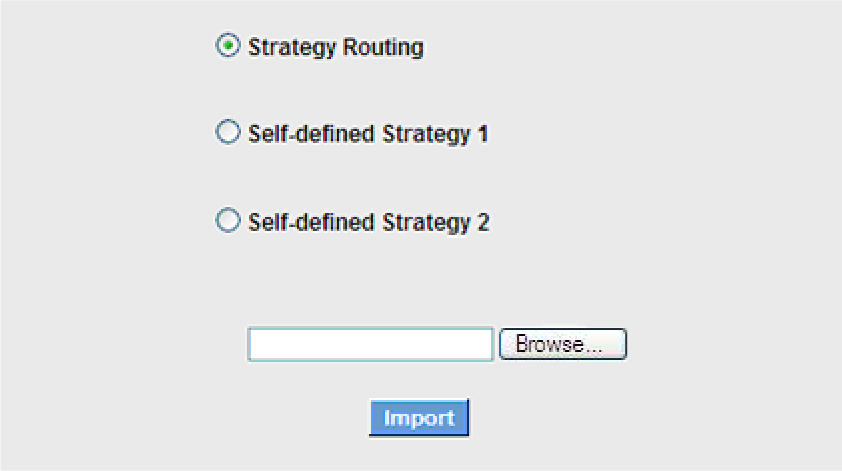
Item	Description
Name	To define a name for the WAN grouping in the box, such as "Education" etc. The name is for recognizing different WAN groups.
Interface	Check the boxes for the WANs to be added into this combination.
Add To List	To add a WAN group to the grouping list.
Delete selected Item	To remove selected WANs from the WAN grouping.
Apply	Click "Apply" to save the modification.
Close	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.



● Strategy Routing

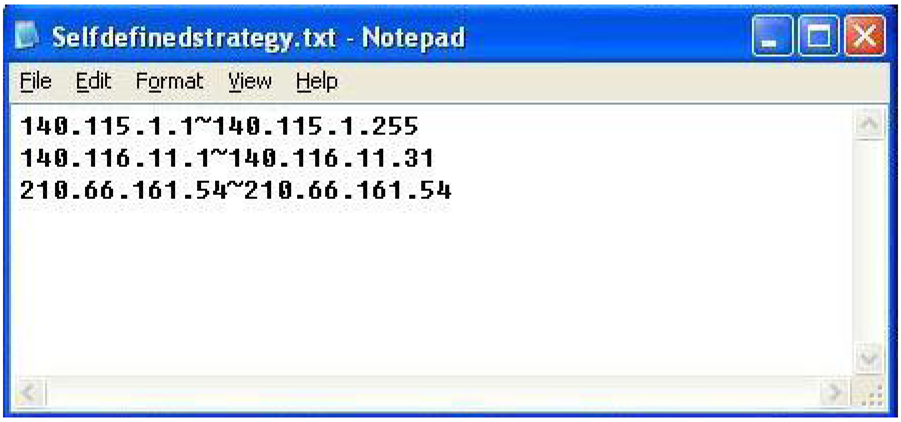
○ Self-defined Strategy 1

○ Self-defined Strategy 2

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.



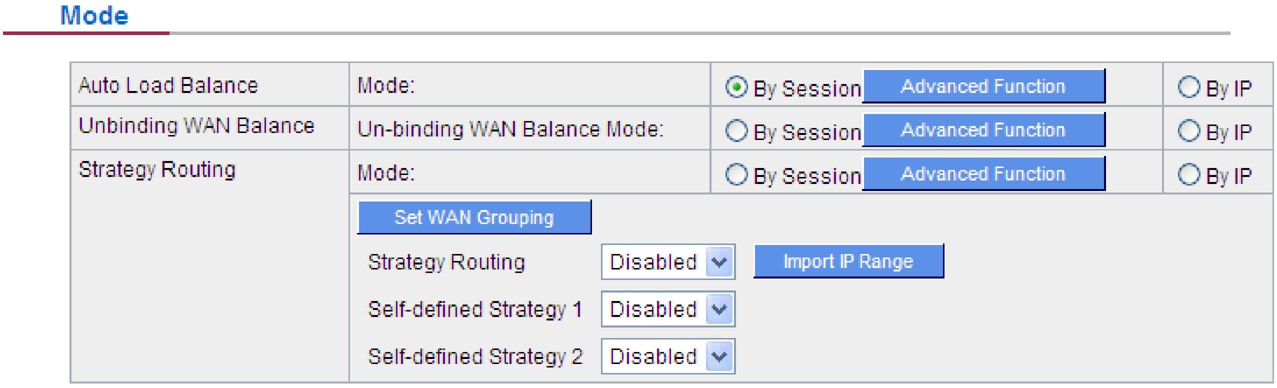
```
140.115.1.1~140.115.1.255
140.116.11.1~140.116.11.31
210.66.161.54~210.66.161.54
```

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.

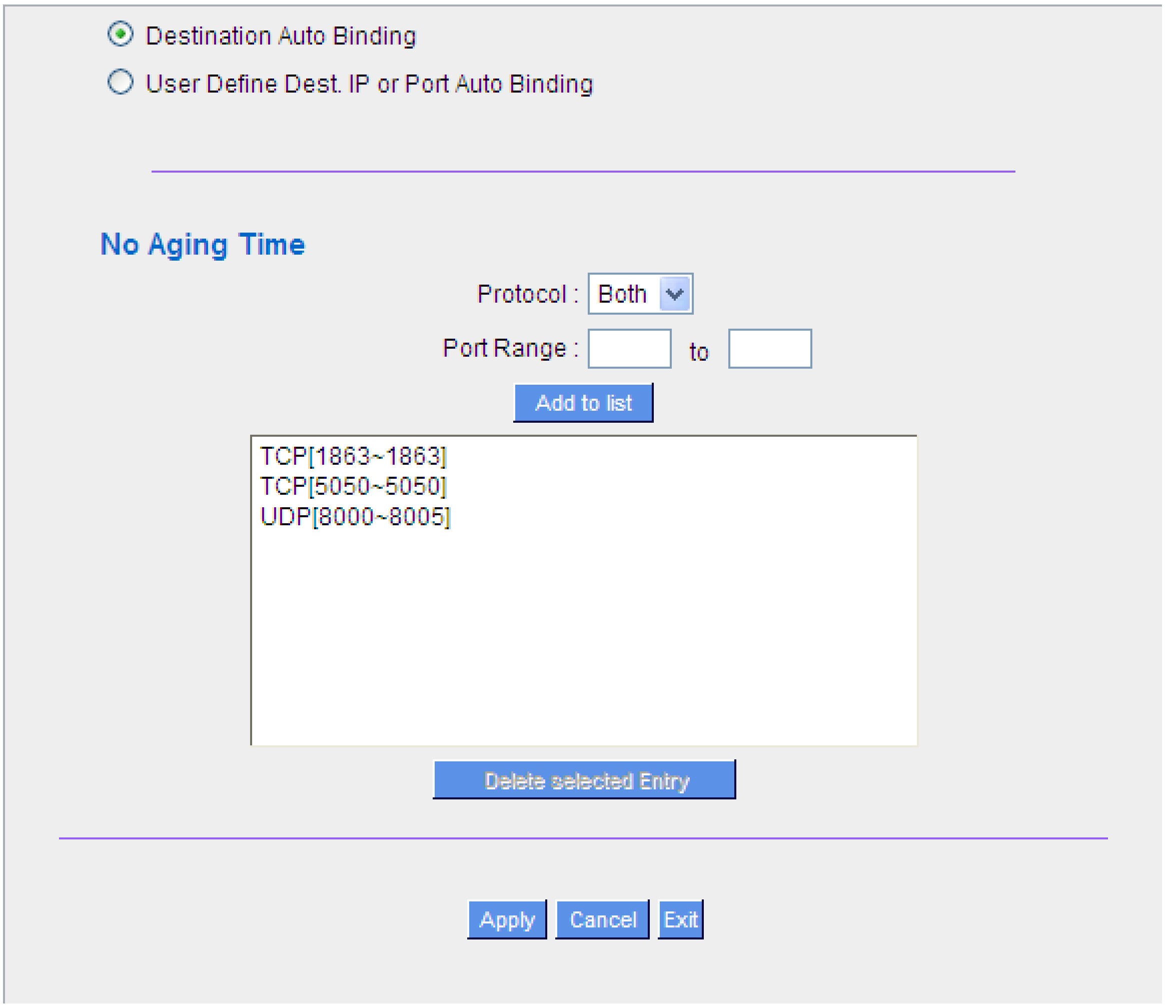
Session balance advanced function can set the same intranet IP keeps having sessions from the same WAN IP for some specific service protocols. Other service protocols can still adopt the original balance mechanism to distribute the sessions equally and randomly. With the original session balance efficiency,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



Mode

Auto Load Balance	Mode:	● By Session Advanced Function	○ By IP
Unbinding WAN Balance	Un-binding WAN Balance Mode:	○ By Session Advanced Function	○ By IP
Strategy Routing	Mode:	○ By Session Advanced Function	○ By IP
	Set WAN Grouping		
	Strategy Routing	Disabled	Import IP Range
	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 : Both

Port Range : to

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

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

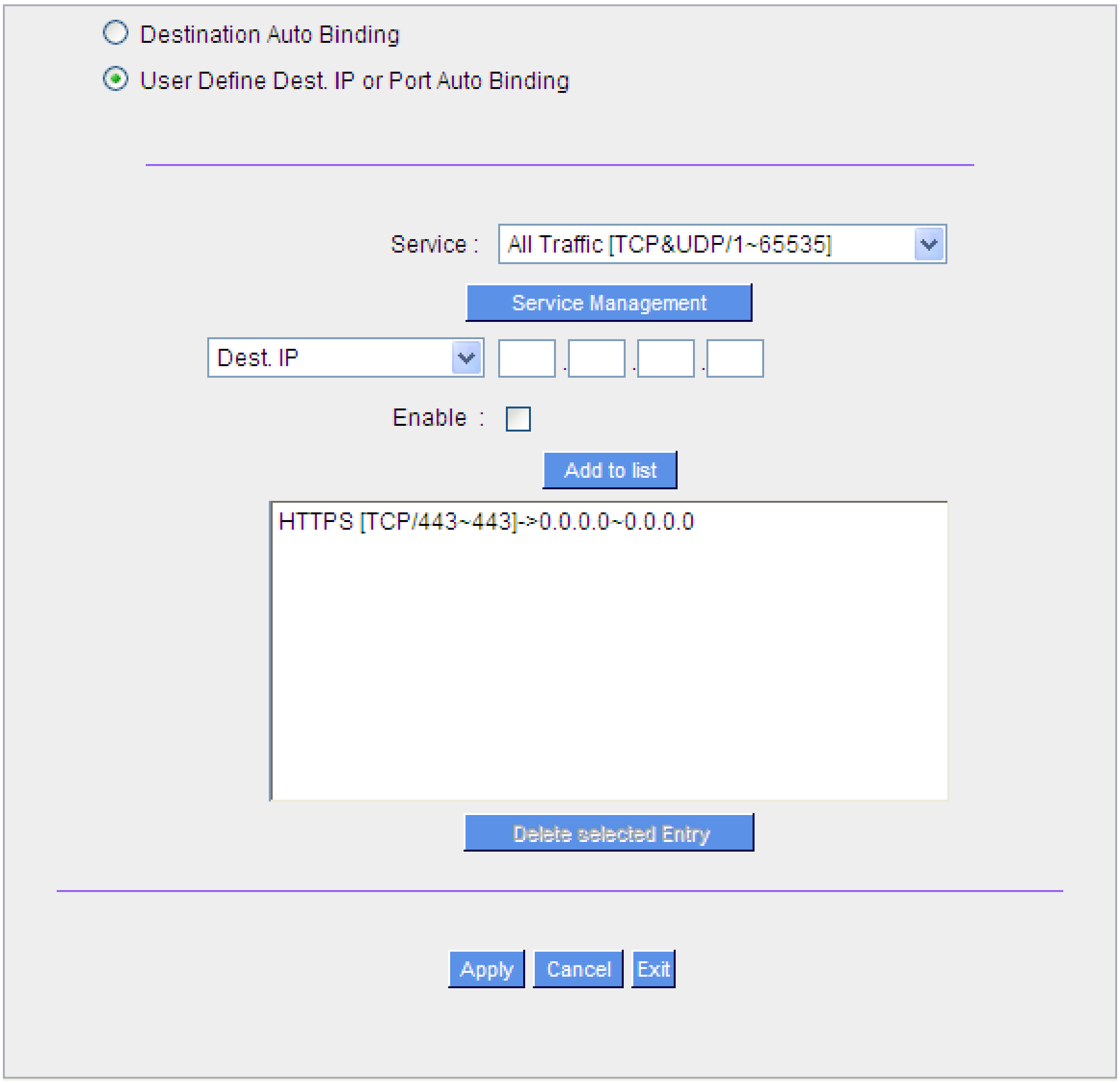
For example, there are WAN1-1 200.10.10.1 and WAN2- 200.10.10.2, and two intranet IP addresses. When 192.168.1.100 visits Internet 61.222.81.100 for the first time, the connection is through WAN1- 200.10.10.1. If the next destination is to 61.222.81.101 (in the same Class B range), the connection will 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.

✍ Note	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.

Item	Description
User Define Dis. Or Port Auto Binding	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.) ✍ Note: You can only choose either **Destination Auto Binding or User Define Dis.** Or **Port Auto Binding**.

Take default rules for example:



○ Destination Auto Binding

● User Define Dest. IP or Port Auto Binding

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

Dest. IP . . .

Enable : □

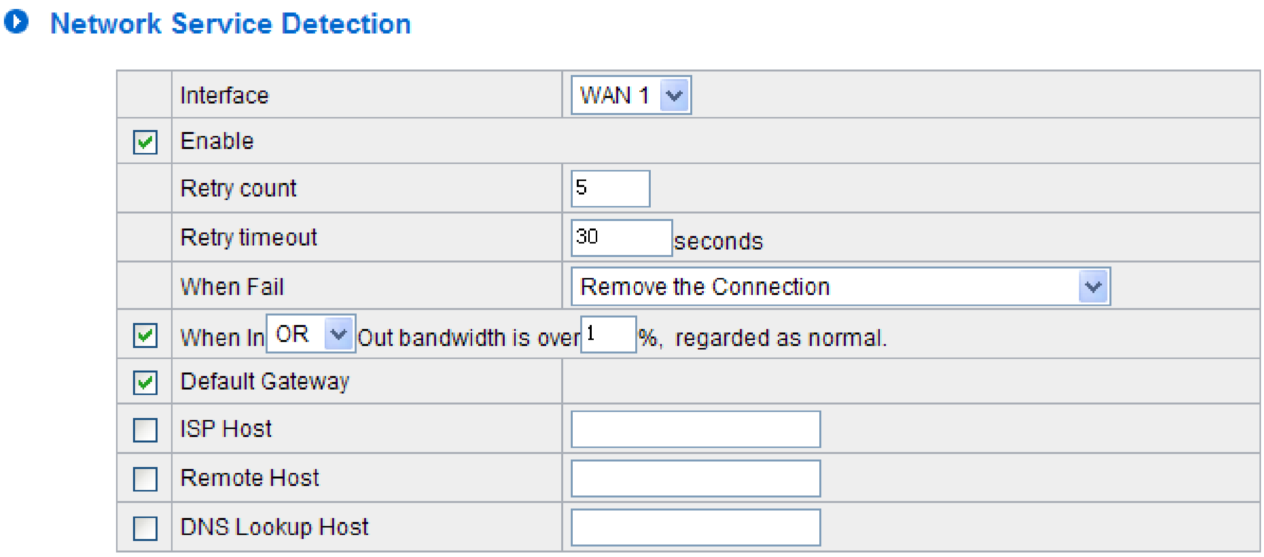
HTTPS [TCP/443~443]->0.0.0.0~0.0.0.0

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
☑	Enable	
	Retry count	5
	Retry timeout	30 seconds
	When Fail	Remove the Connection
☑	When In OR Out bandwidth is over 1 %, regarded as normal.	
☑	Default Gateway	
□	ISP Host	
□	Remote Host	
□	DNS Lookup Host	

Item	Description
Interface	Select the WAN Port that enables Network Service Detection.
Retry	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".
Retry Timeout	Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.
When Fail	**(1) Generate the Error Condition in the System Log:** 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.

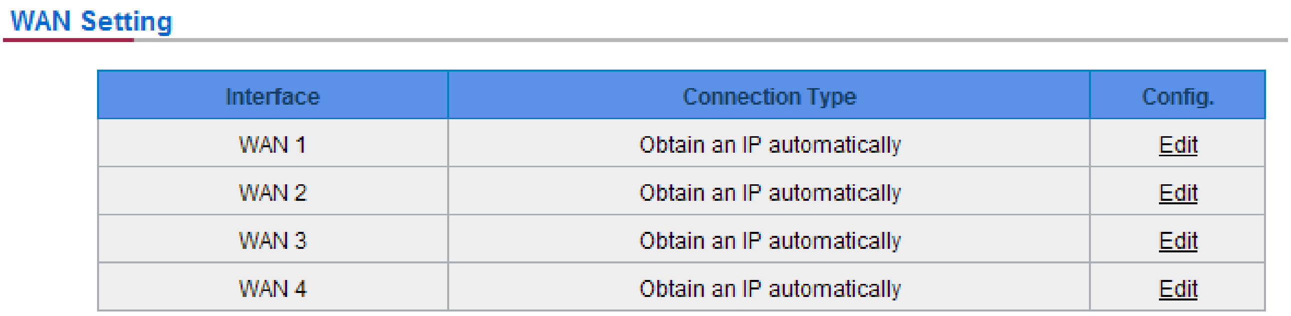
	This option is suitable under the condition that one of the WAN connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination. For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 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. **(2) Keep System Log and Remove the Connection:** 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. 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.
Default Gateway	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.
ISP Host	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)
Remote Host	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).
DNS Lookup	This is the detect location for DNS. (Only a web address such as
Host	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.

✍ **Note**	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

WAN Setting

The VPN Router allows maximum four WAN interface, the bandwidth and real connection of every WAN will impact the load balance mechanism; therefore you need to set the Bandwidth and the Network service detection by each WAN Port correctly. In **"Interface Configuration"**, click **"Edit"** to enter the WAN port configuration.

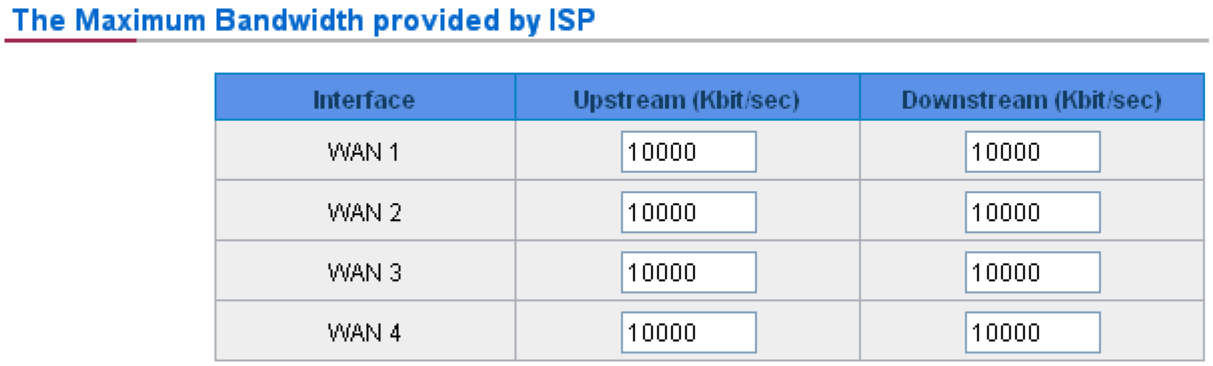


WAN Setting

Interface	Connection Type	Config.
WAN 1	Obtain an IP automatically	Edit
WAN 2	Obtain an IP automatically	Edit
WAN 3	Obtain an IP automatically	Edit
WAN 4	Obtain an IP automatically	Edit

Bandwidth Management

When Auto Load Balance mode is selected, the WAN bandwidth will automatically allocate connections through sessions or IP 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.



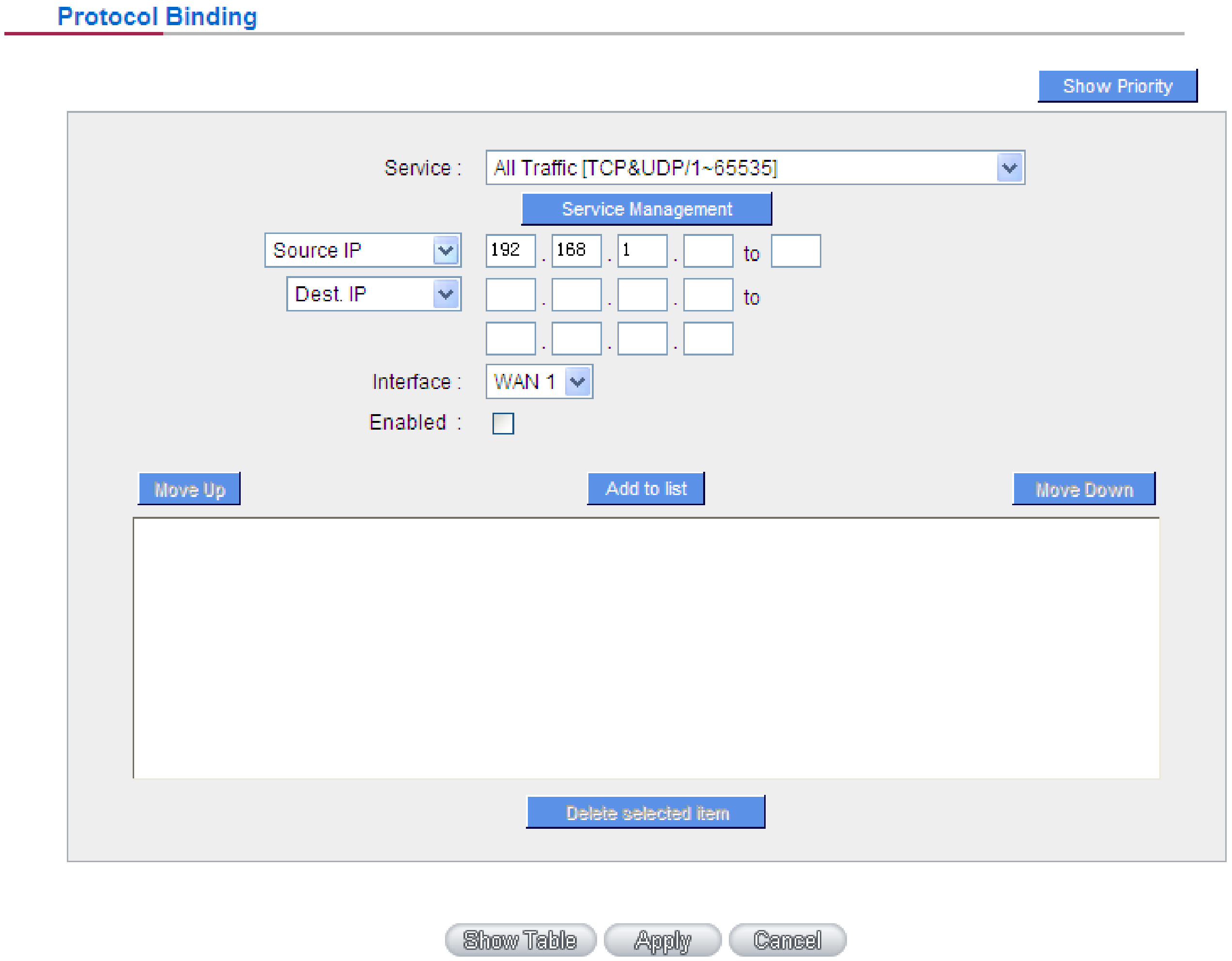
The Maximum Bandwidth provided by ISP

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

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.

Note	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.



Protocol Binding

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

Source IP: 192 . 168 . 1 . to

Dest. IP: . . . to

. . .

Interface : WAN 1

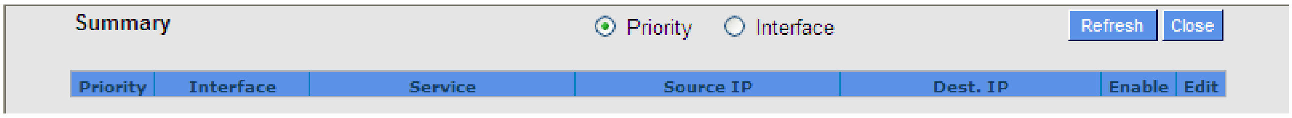
Enabled : □

Item	Description
Service	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.
Source IP	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.
Destination IP	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.
Interface	Select the WAN for which users want to set up the binding rule.
Enable	To activate the rule.
Add To List	To add this rule to the list.
Delete selected application	To remove the rules selected from the Service List.
Moving Up & Down	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.

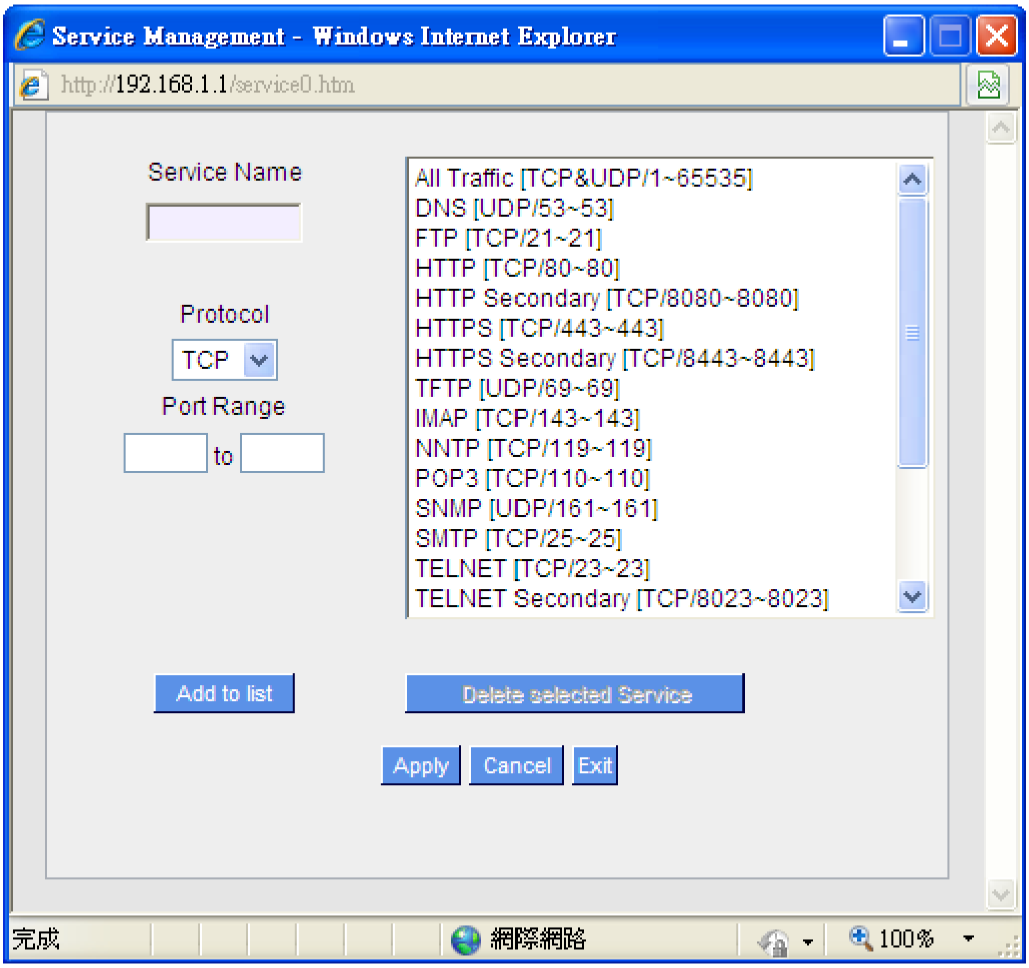


Summary ● Priority ○ Interface

Priority	Interface	Service	Source IP	Dest. IP	Enable	Edit

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:



Service Management - Windows Internet Explorer
http://192.168.1.1/service0.htm

Service Name

Protocol: TCP

Port Range ___ to ___

All Traffic [TCP&UDP/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]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]

Add to list
Delete selected Service
Apply
Cancel
Exit
完成
網際網路
100%

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

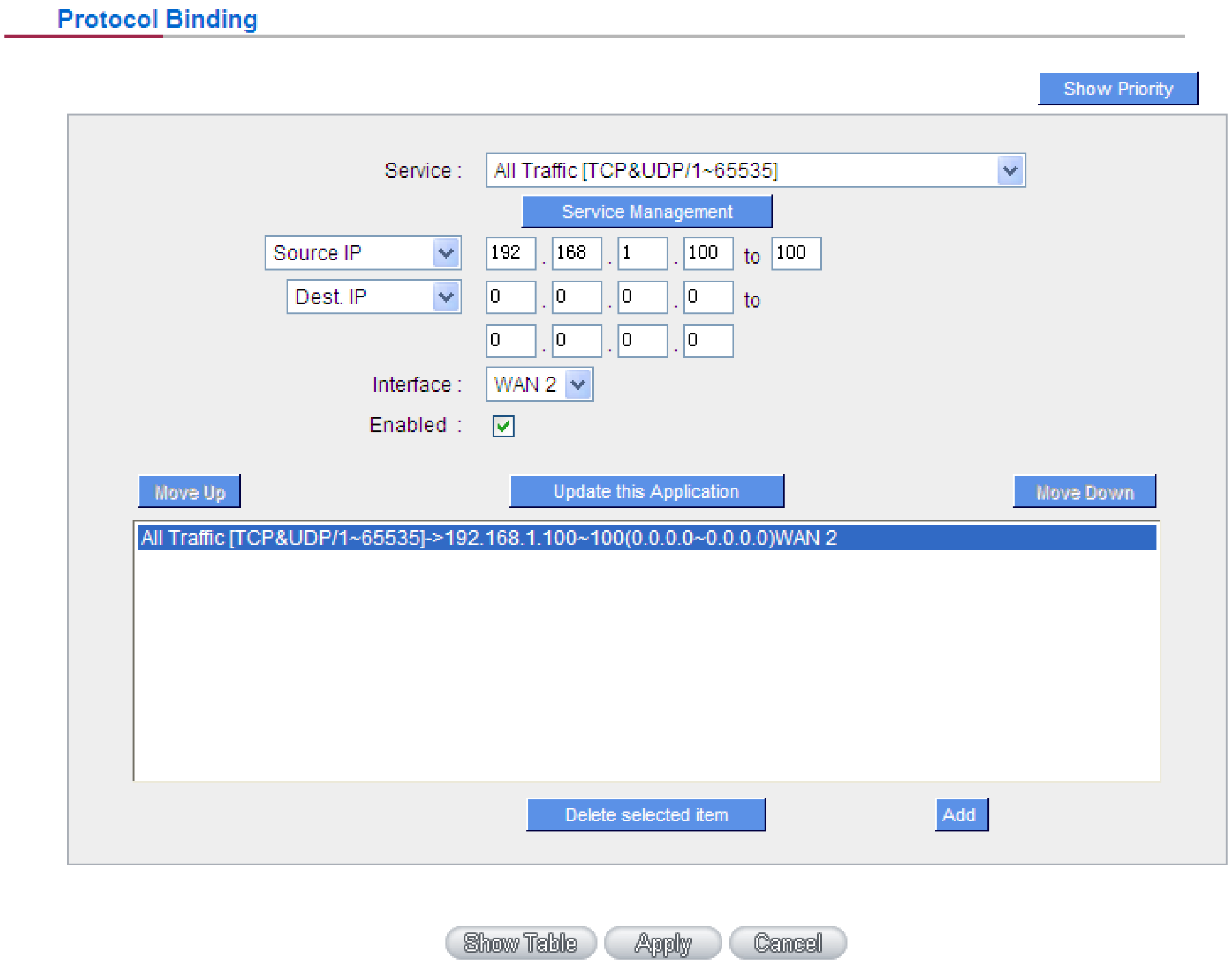
	up to 100 services into the list.
Delete selected service	To remove the selected activated Services.
Apply	Click the "**Apply**" button to save the modification.
Cancel	Click the **"Cancel"** button to cancel the modification. This only works before **"Apply"** is clicked.

Auto Load Balance 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 the 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.



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

Source IP 192 . 168 . 1 . 100 to 100

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

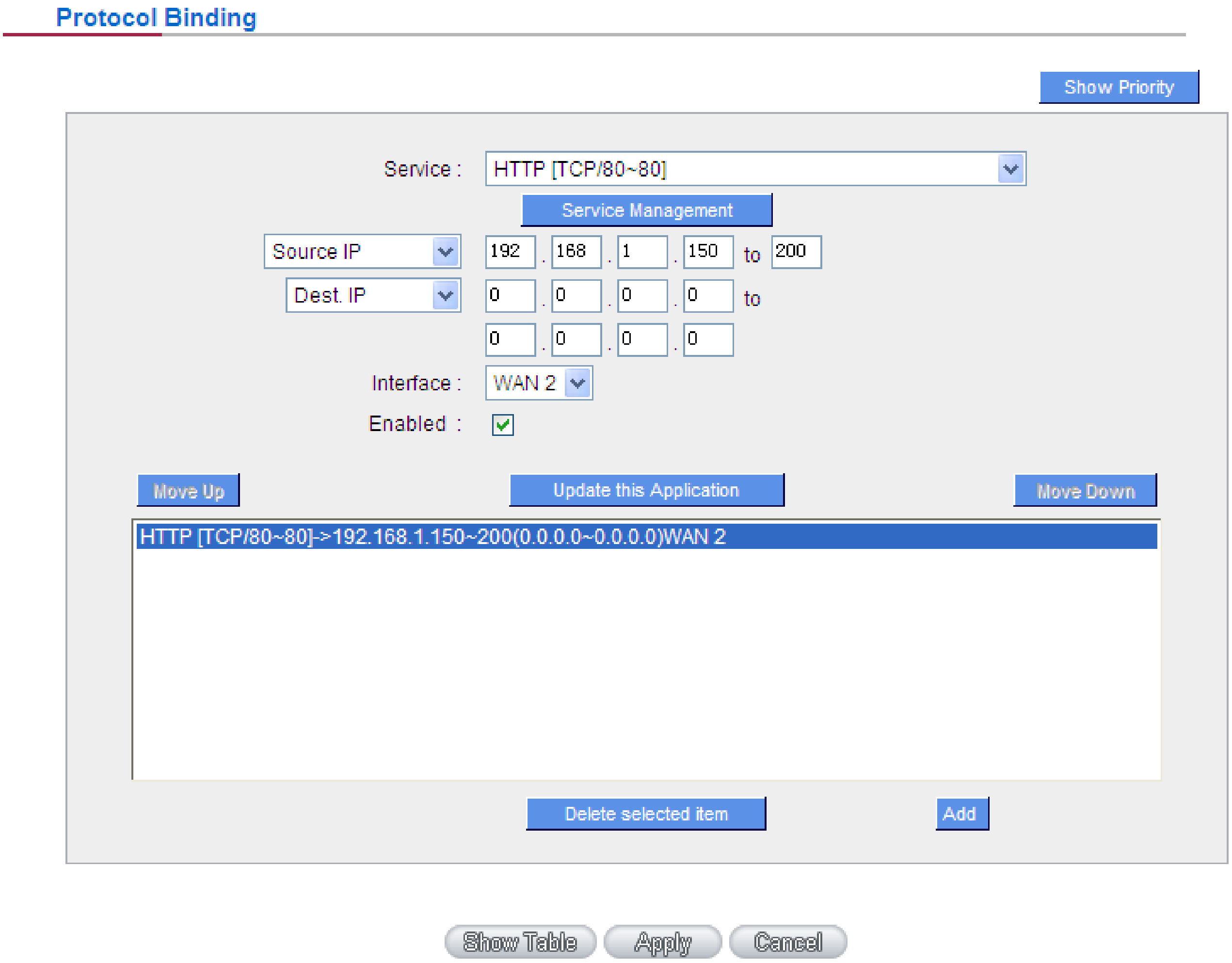
Interface : WAN 2

Enabled : ☑

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

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]

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

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

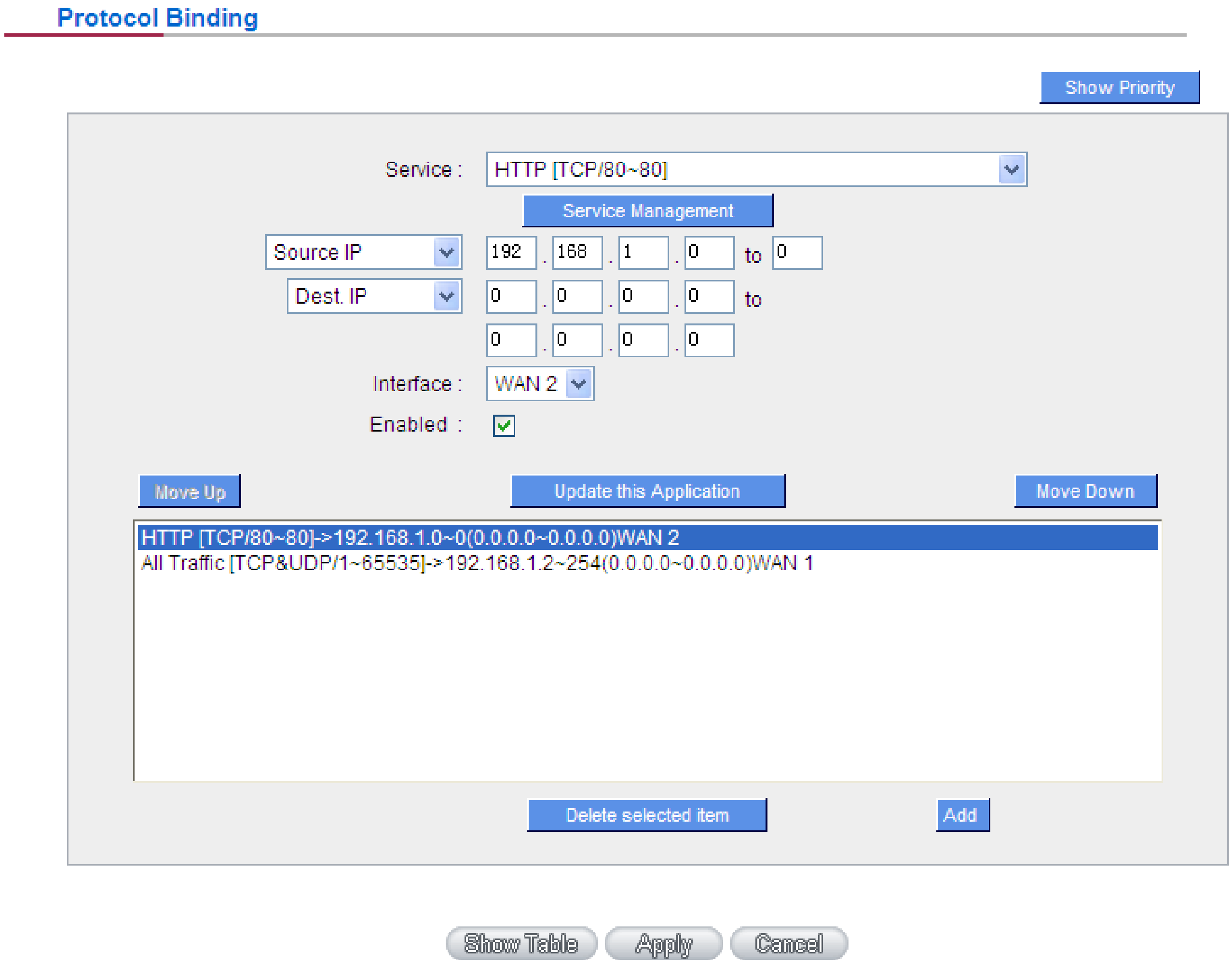
Interface : WAN 2

Enabled : ☑

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

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

Service : HTTP [TCP/80~80]

Source IP 192 . 168 . 1 . 0 to 0

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

Interface : WAN 2

Enabled : ☑

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

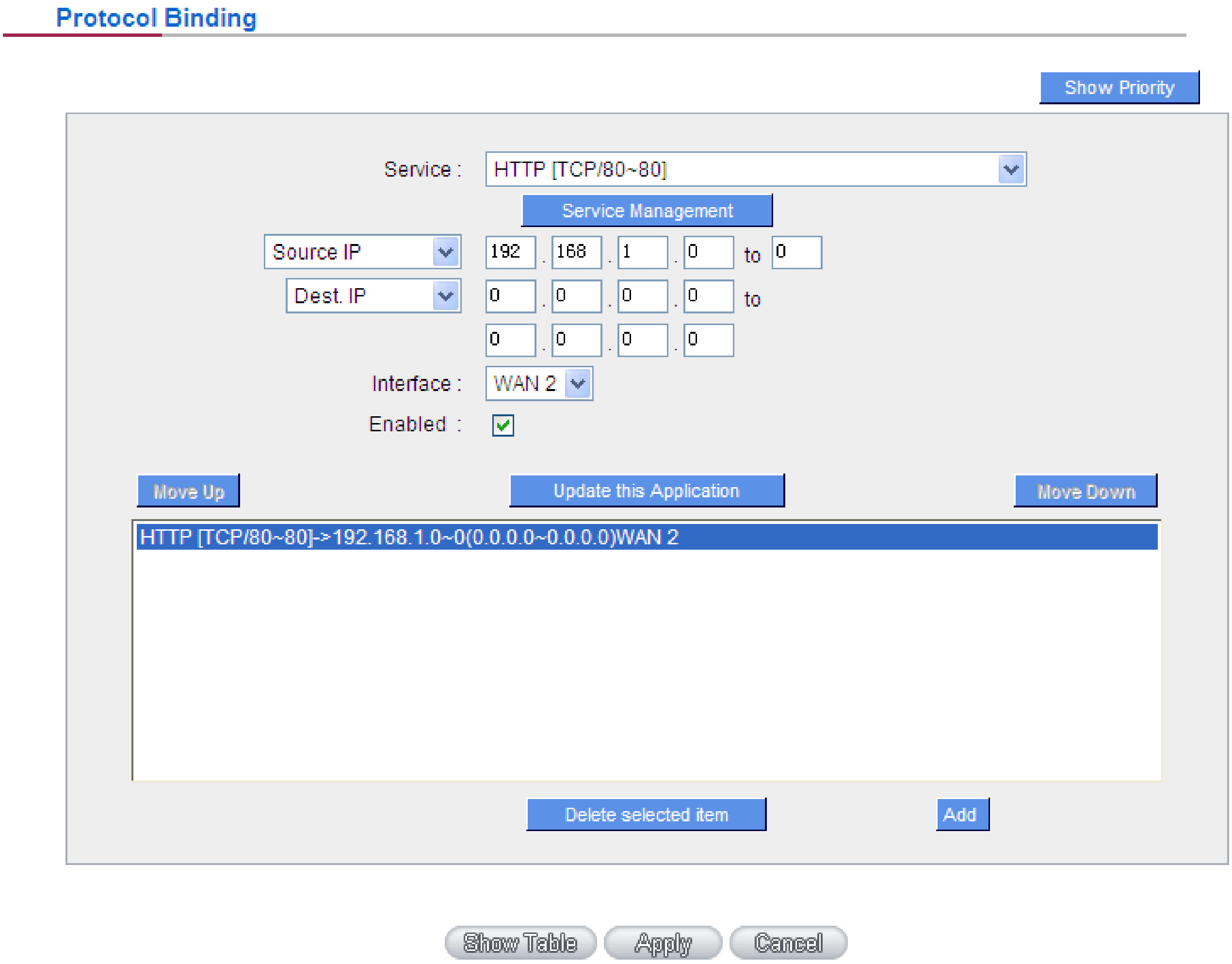
Configuring "Assigned Routing Mode" for load Balance

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.



Service : HTTP [TCP/80~80]

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

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

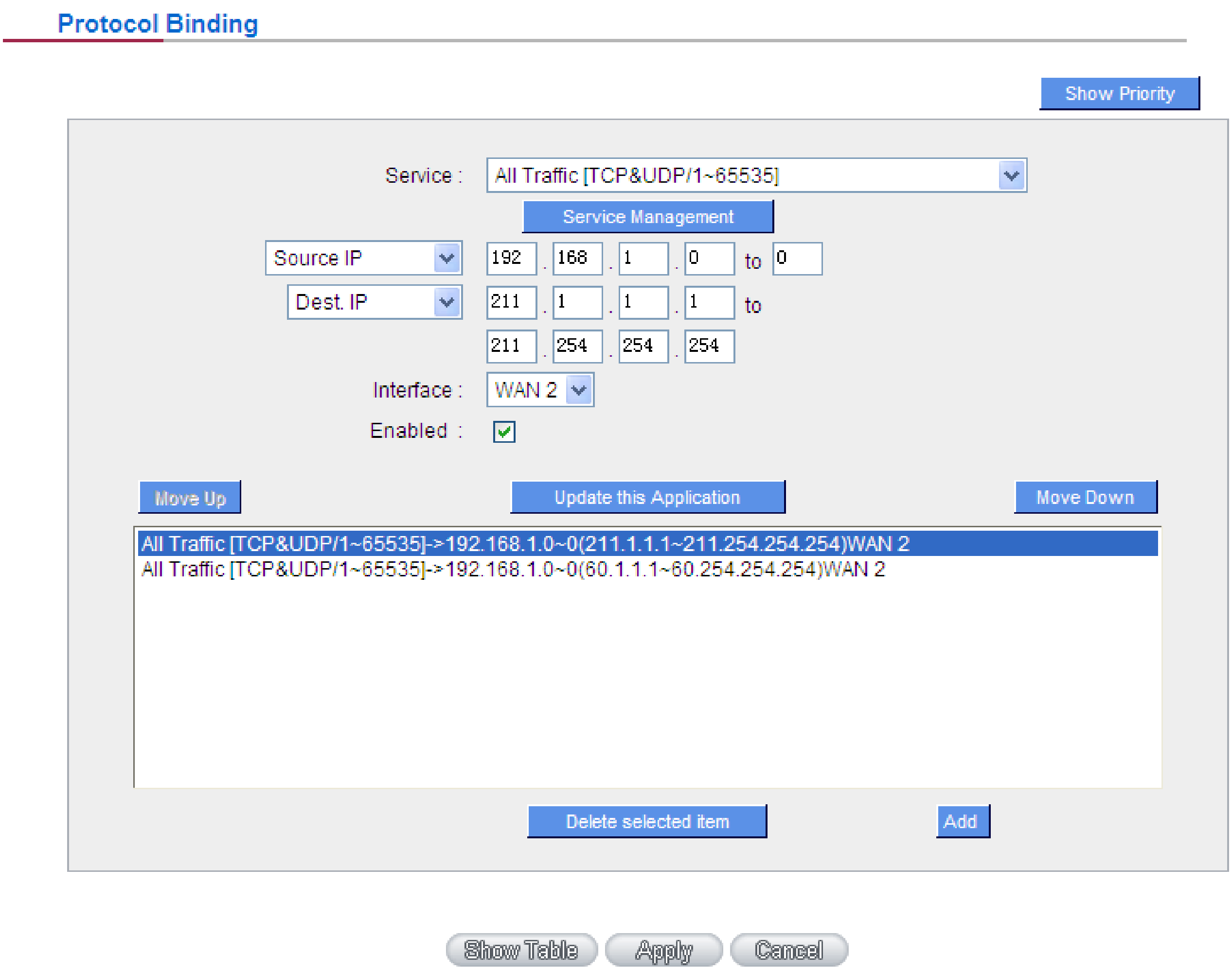
Interface : WAN 2

Enabled : ☑

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

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.



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

Source IP 192 . 168 . 1 . 0 to 0

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

Interface : WAN 2

Enabled : ☑

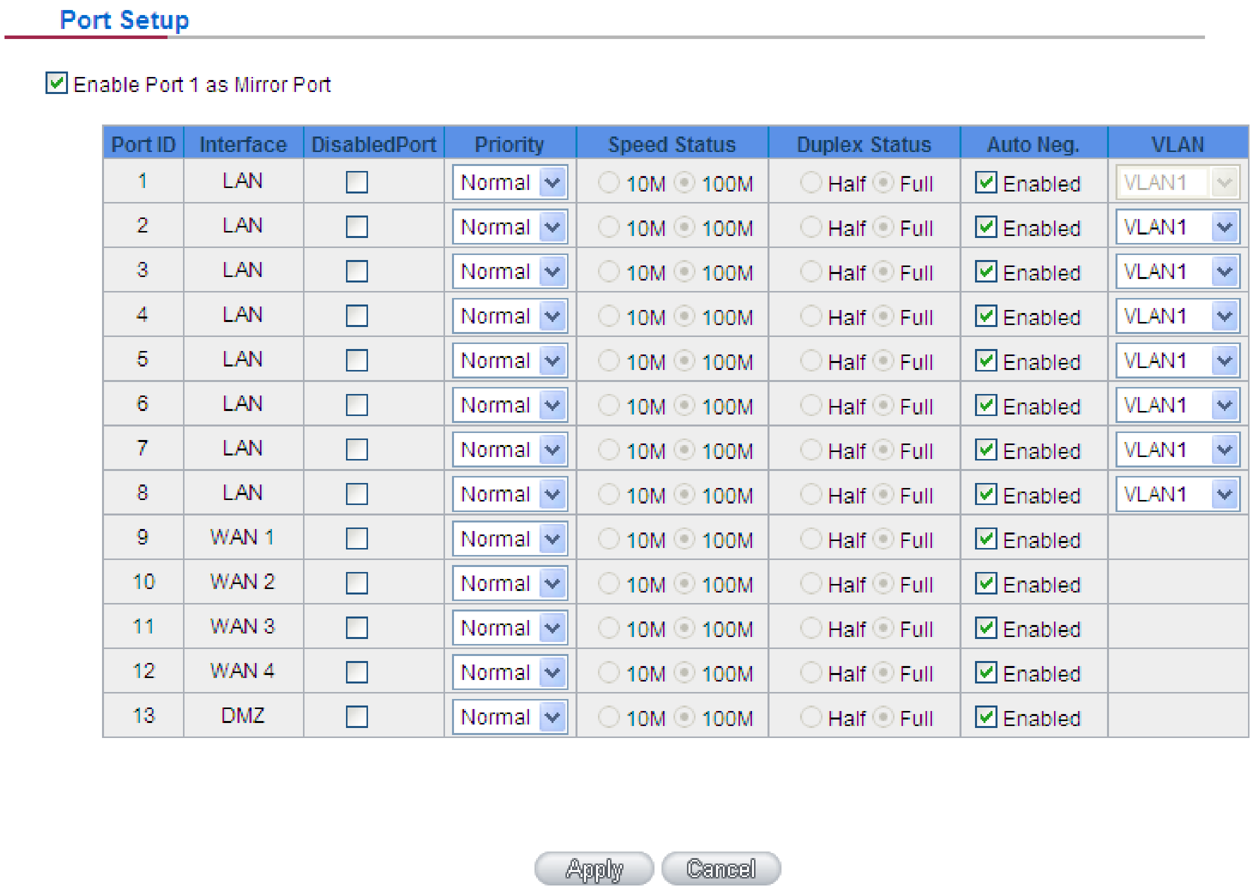
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(211.1.1.1~211.254.254.254)WAN 2
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0(60.1.1.1~60.254.254.254)WAN 2

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

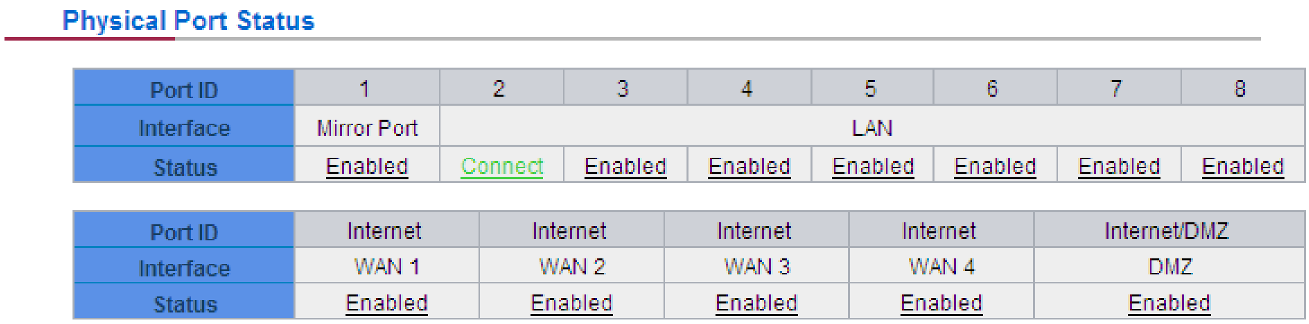
☑ Enable Port 1 as Mirror Port

Port ID	Interface	DisabledPort	Priority	Speed Status	Duplex Status	Auto Neg.	VLAN
1	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
2	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
3	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
4	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
5	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
6	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
7	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
8	LAN	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	VLAN1
9	WAN 1	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	
10	WAN 2	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	
11	WAN 3	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	
12	WAN 4	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	
13	DMZ	□	Normal	○ 10M ● 100M	○ Half ● Full	☑ Enabled	

Item	Description
Disabled	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".
Priority	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".
Speed	This feature allows users to select the network hardware connection speed for the Ethernet port. The options are 10Mbps and 100Mbps.
Duplex Status	This feature allows users to select the network hardware connection speed working mode for the Ethernet. The options are full duplex and half duplex.
Auto Neg.	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.
VLAN	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. 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.
VLAN All	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. 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.

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.

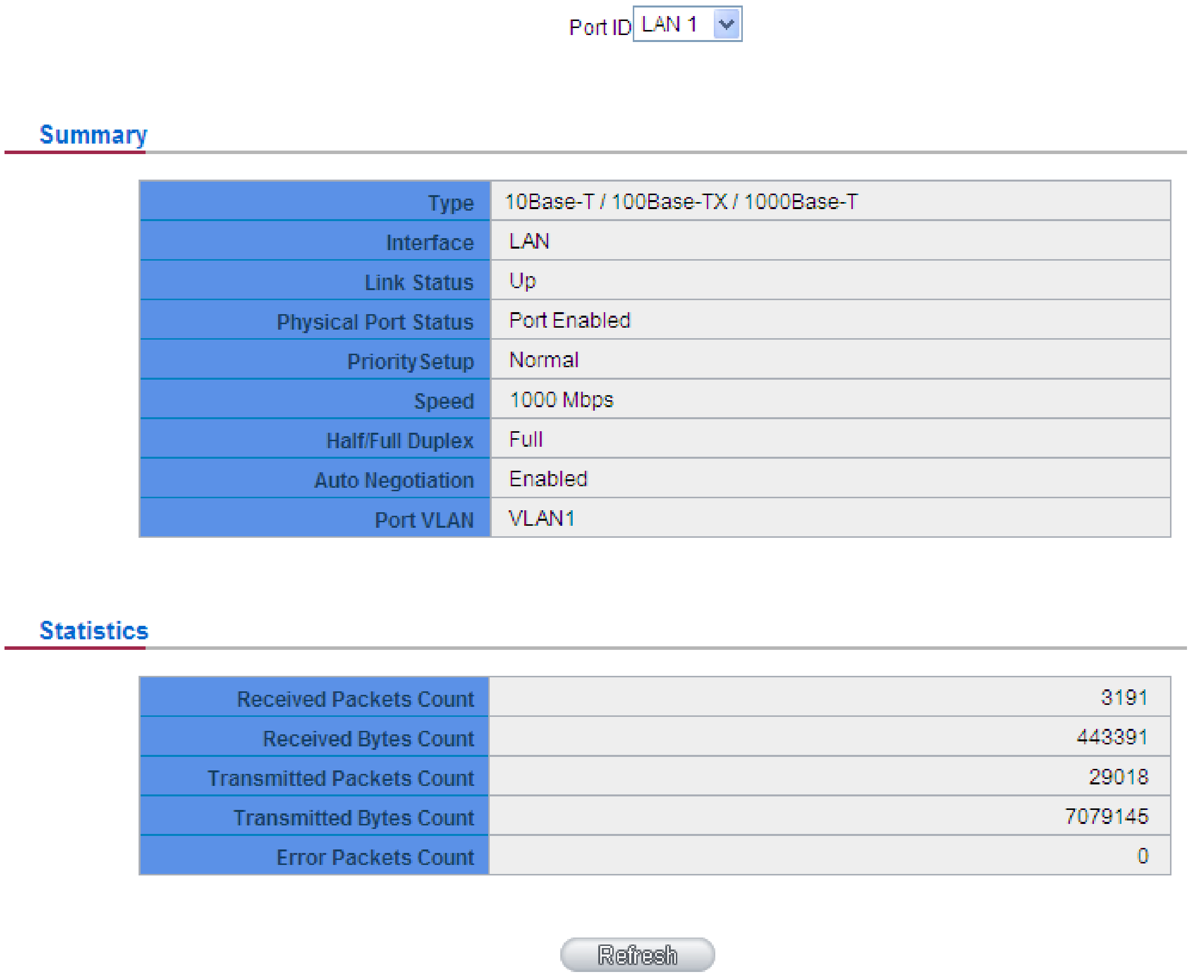


Physical Port Status

Port ID	1	2	3	4	5	6	7	8
Interface	Mirror Port	LAN						
Status	Enabled	Connect	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

Port ID	Internet	Internet	Internet	Internet	Internet/DMZ
Interface	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
Status	Enabled	Enabled	Enabled	Enabled	Enabled

7.2 Port Status



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

Summary

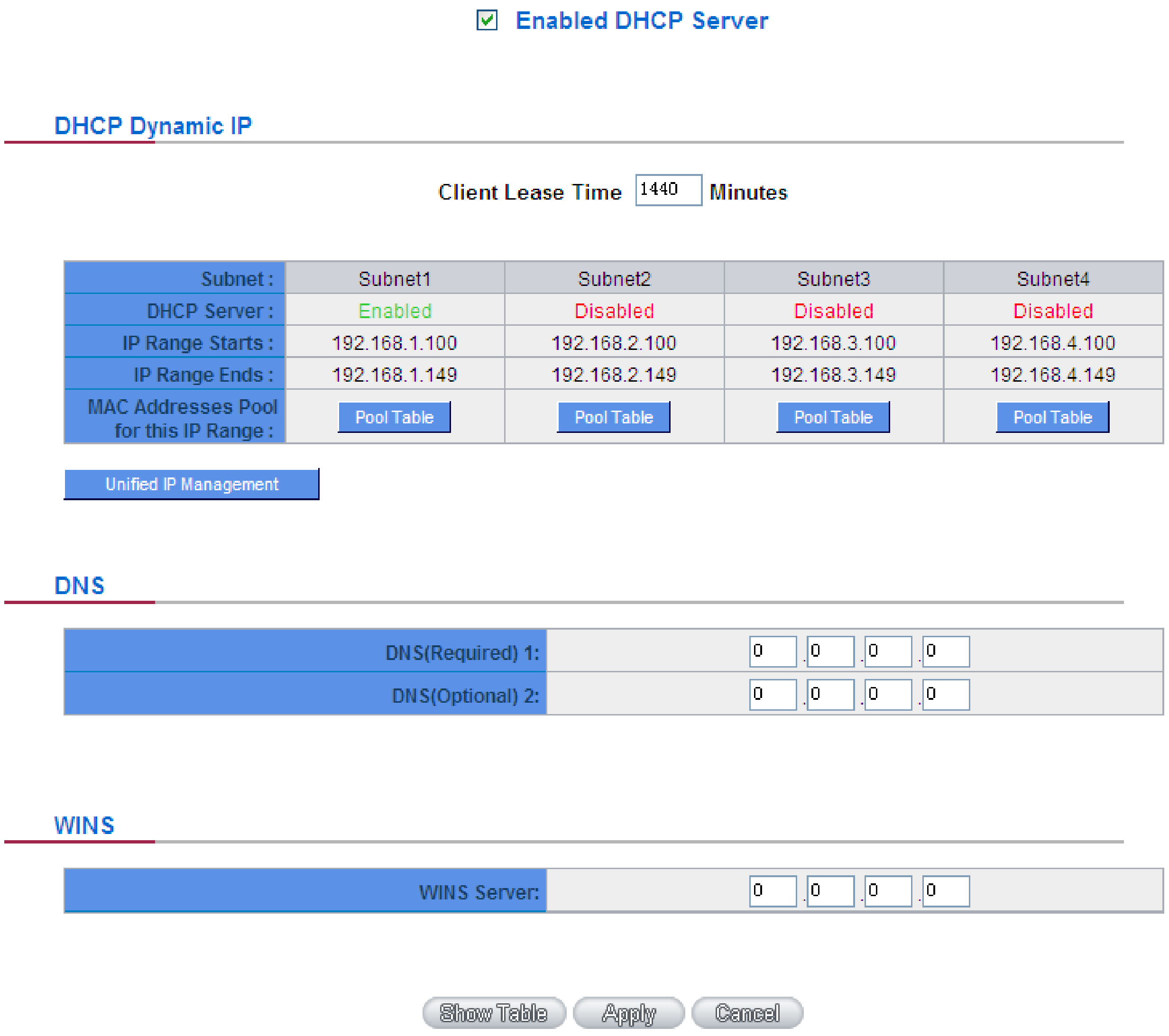
There are Network Connection Type, Interface, Link Status (Up/Down), Port Activity (Port Enabled), Priority Setting (High or Normal), Speed Status (10Mbps, 100Mbps or 1000Mbps), Duplex Status (half duplex or full duplex), Auto Neg. (Enabled/Disabled), and VLAN.

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 assignation 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 1440 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 :	Pool Table	Pool Table	Pool Table	Pool Table

Unified IP Management

DNS

DNS(Required) 1:	0 . 0 . 0 . 0
DNS(Optional) 2:	0 . 0 . 0 . 0

WINS

WINS Server:	0 . 0 . 0 . 0

DHCP Dynamic IP

Item	Description
Enable DHCP Server	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.
Client lease Time	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.
Range Start	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.
Range End	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
DNS (Required) 1	Input the IP address of the DNS server.
DNS (Optional) 2	Input the IP address of the DNS server.

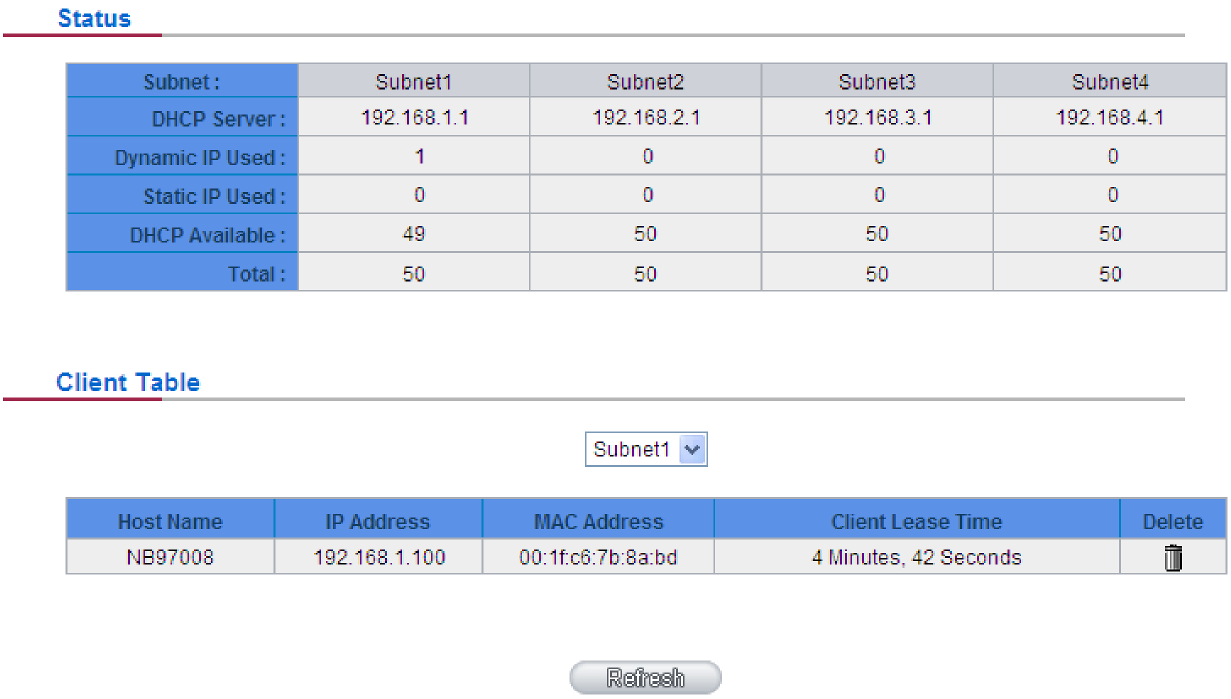
WINS:

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

Item	Description
WINS Server	Input the IP address of WINS.
Apply	Click **"Apply"** to save the network configuration modification.
Cancel	Click **"Cancel"** 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

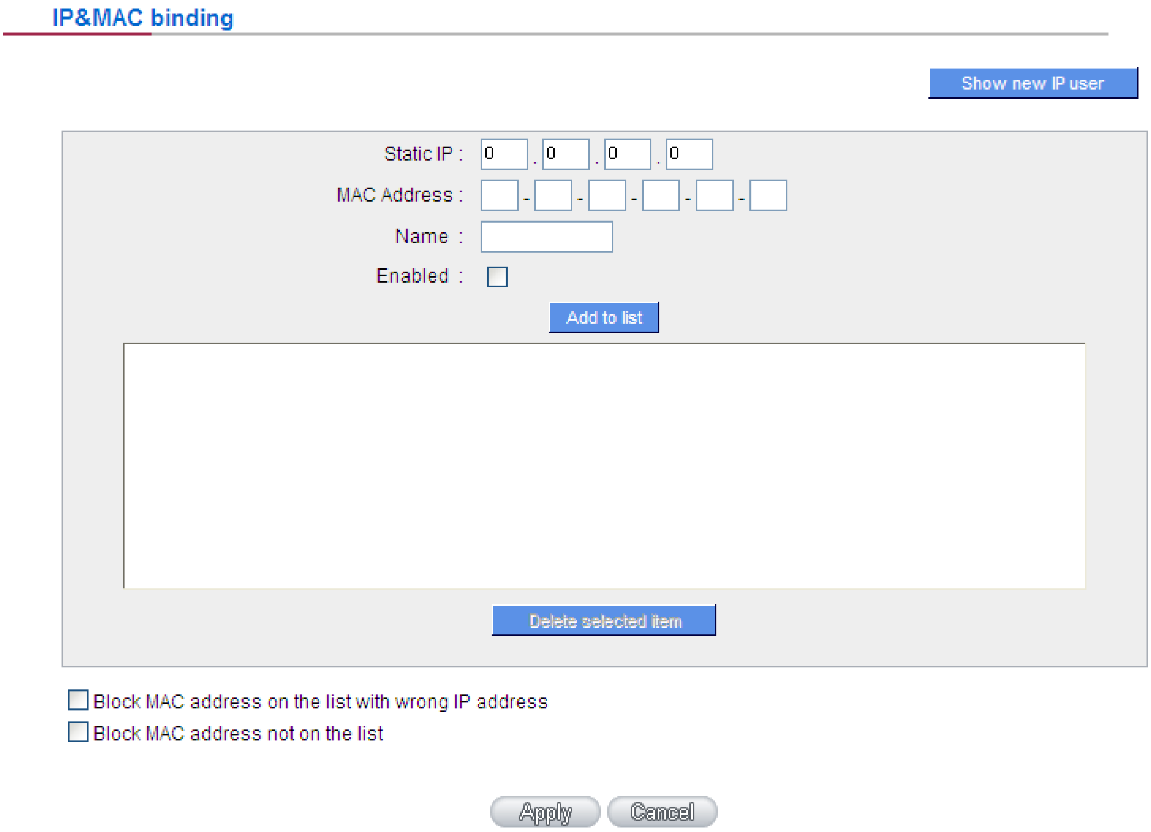
Subnet1

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	🗑

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.



Static IP : 0 . 0 . 0 . 0

MAC Address : - - - - -

Name :

Enabled : □

□ Block MAC address on the list with wrong IP address

□ Block MAC address not on the list

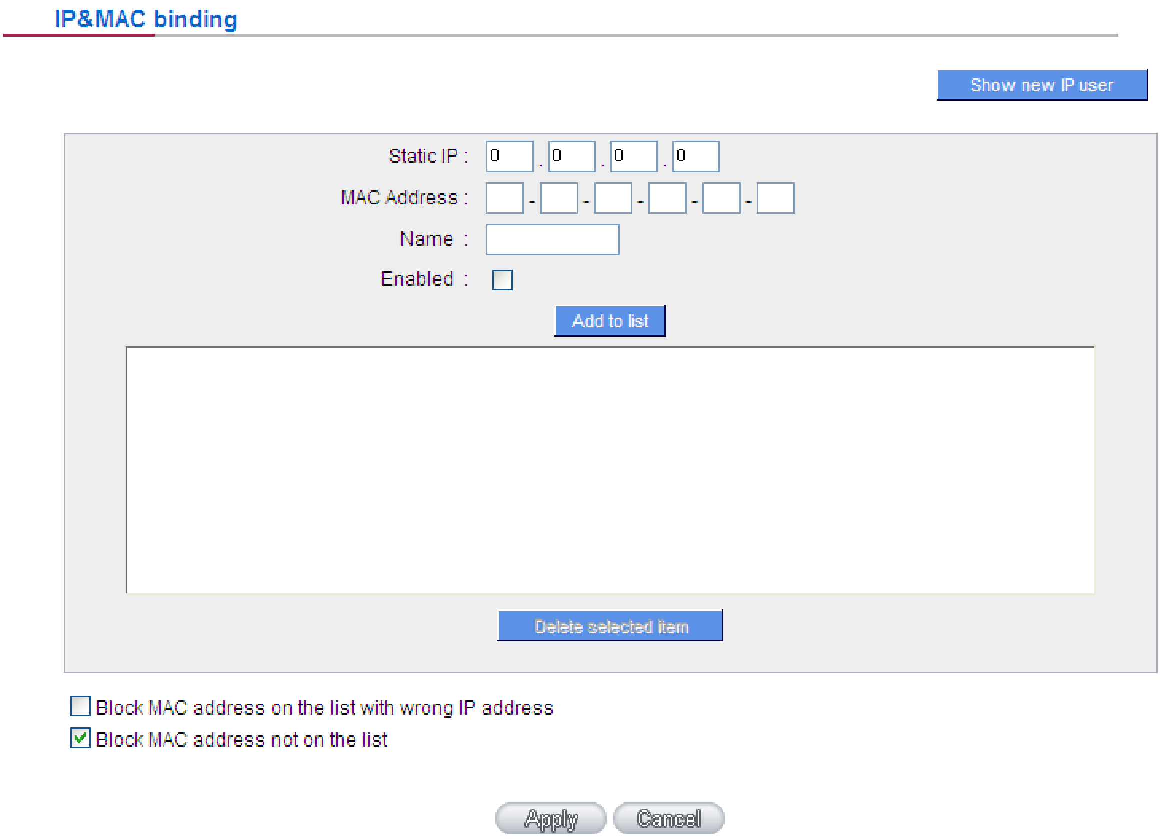
There are two methods for setting up this function:

Block MAC address on the list with wrong IP address:

This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access.

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:



Static IP : 0 . 0 . 0 . 0

MAC Address : - - - - -

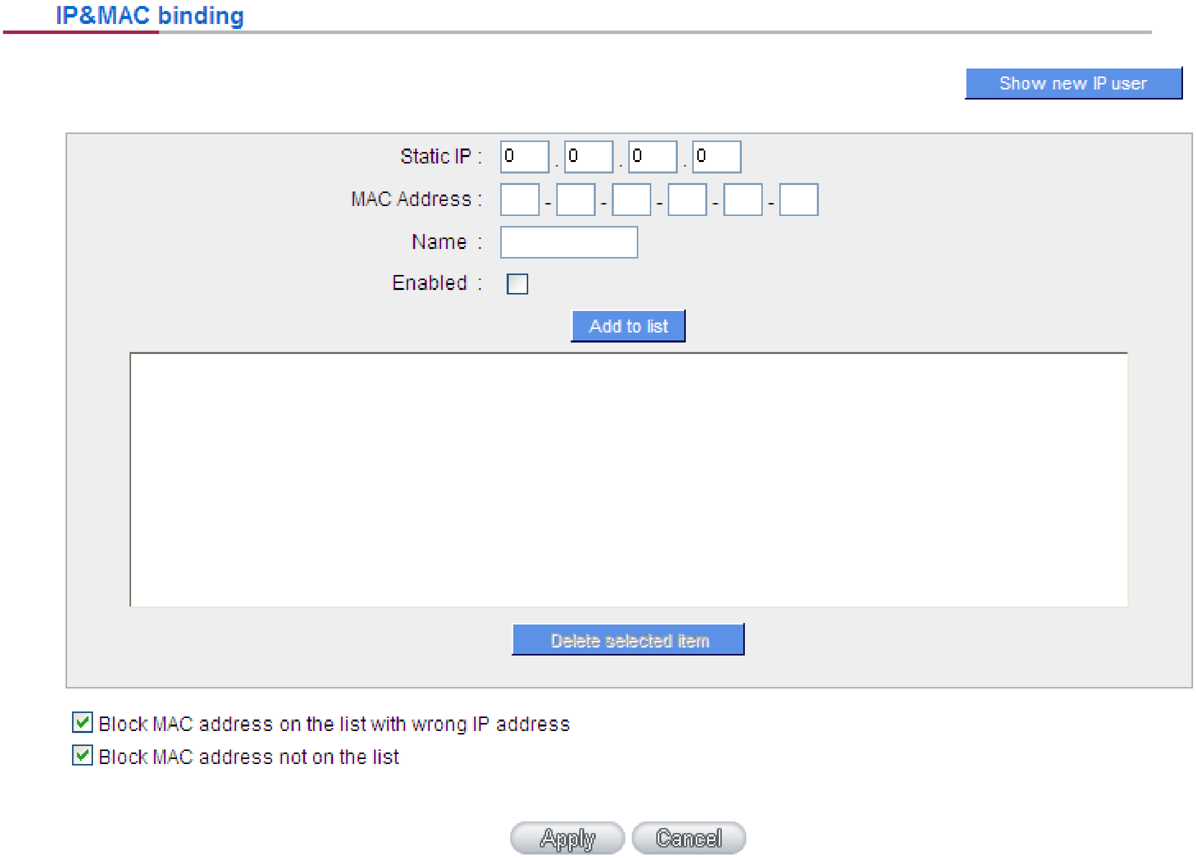
Name :

Enabled : □

□ Block MAC address on the list with wrong IP address

☑ Block MAC address not on the list

IP & MAC Binding



Static IP : 0 . 0 . 0 . 0

MAC Address : - - - - -

Name :

Enabled : □

☑ Block MAC address on the list with wrong IP address

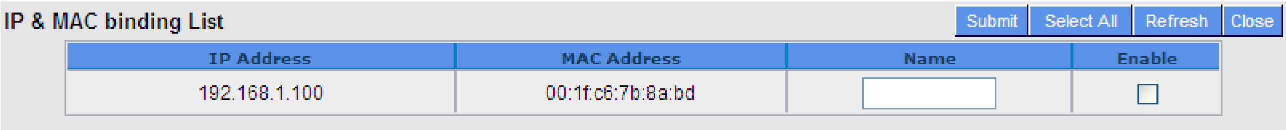
☑ Block MAC address not on the list

Item	Description
Static IP:	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.
MAC Address:	Input the static real MAC (the address on the network card) for the server or PC which is to be bound.
Name:	For distinguishing clients, input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
Enabled:	Activate this configuration.
Add to list:	Add the configuration or modification to the list.
Delete selected item:	Remove the selected binding from the list.
Add:	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

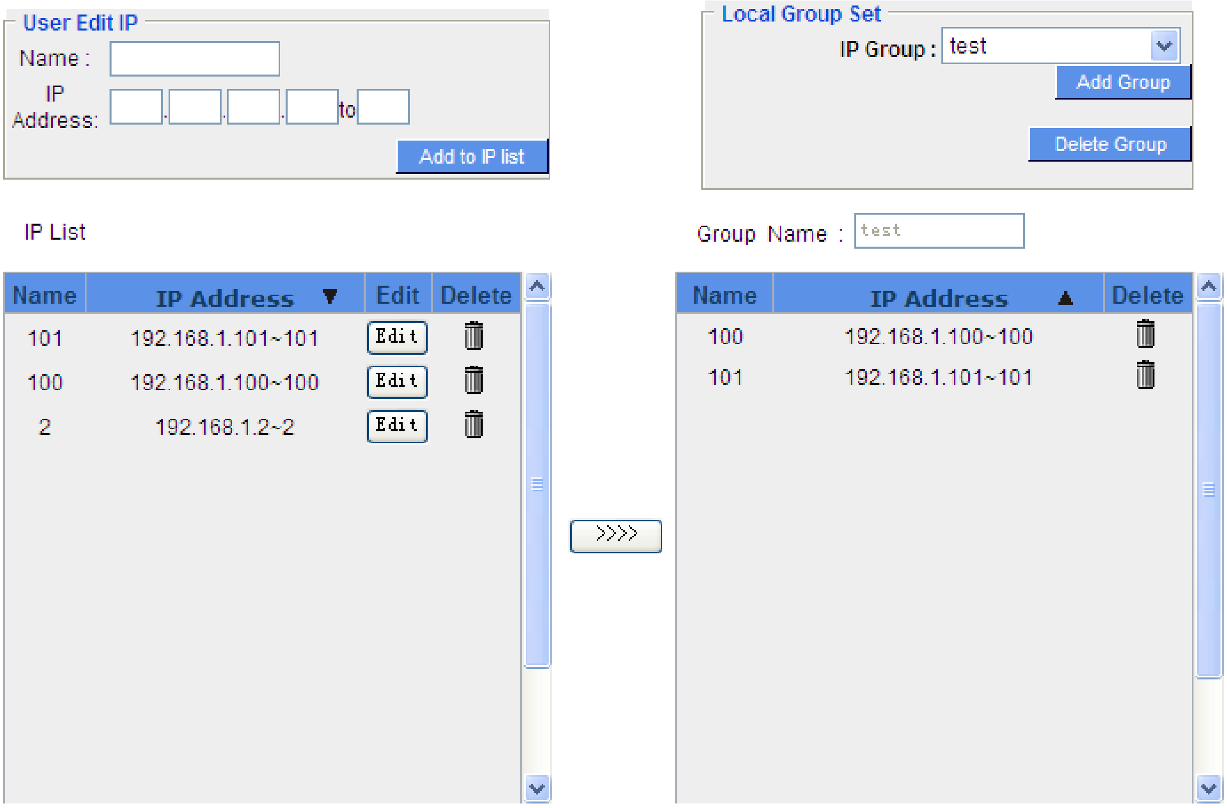
IP Address	MAC Address	Name	Enable
192.168.1.100	00:1f:c6:7b:8a:bd		□

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



User Edit IP

Name :

IP Address: . . . to

Add to IP list

Local Group Set

IP Group : test

Add Group

Delete Group

IP List

Name	IP Address ▼	Edit	Delete
101	192.168.1.101~101	Edit	🗑
100	192.168.1.100~100	Edit	🗑
2	192.168.1.2~2	Edit	🗑

>>>>

Group Name : test

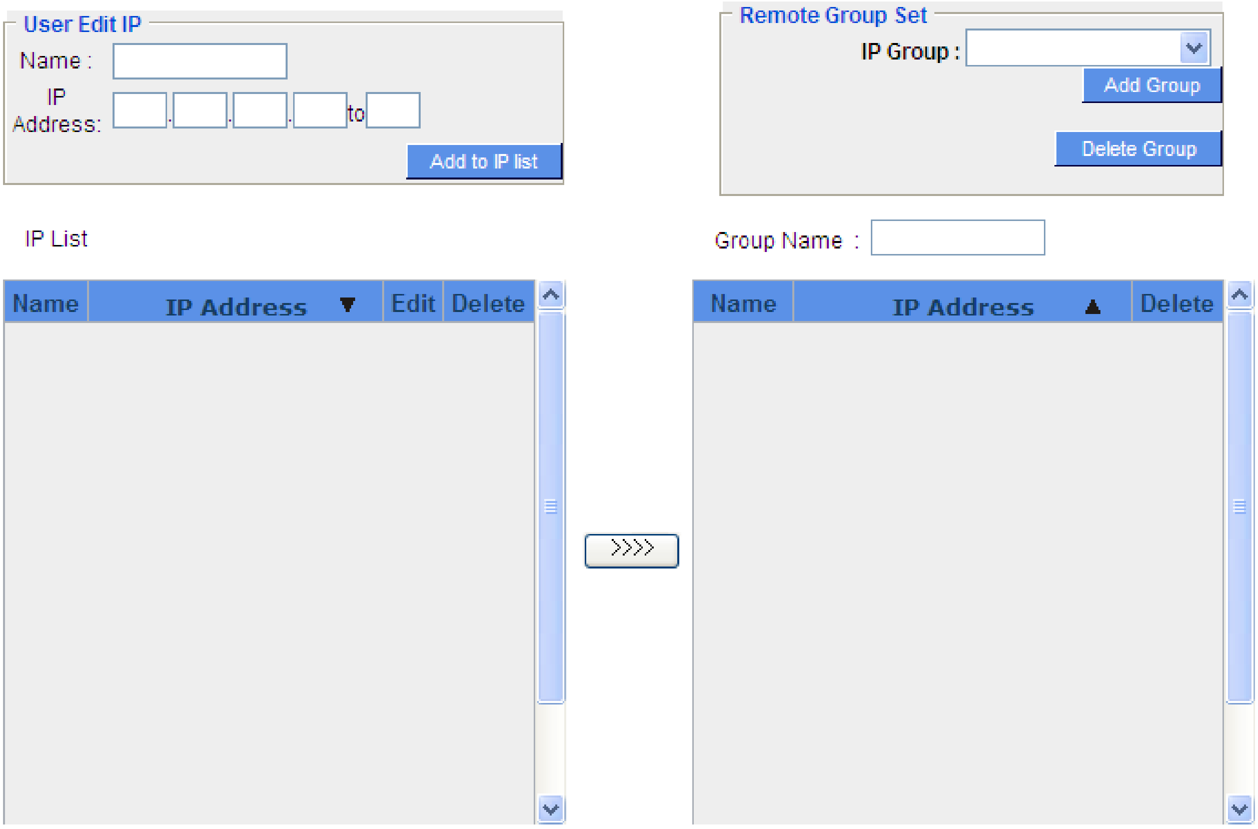
Name	IP Address ▲	Delete
100	192.168.1.100~100	🗑
101	192.168.1.101~101	🗑

Item	Description
User Edit IP	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.
Name	Input the name of IP address (or range) showed below.
IP Address	Input IP address (or range). For example, 192.168.1.200 ~ 250.
Add to IP List	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.

Local Group Set	You can choose from the IP list on the left side to set up a local IP group.
IP Group	Choose IP Group that you would like to modify. If you would like to add new groups, please push “Add new group” button.
Group Name	When you add new groups, please note if the group name is in the column.
Delete Group	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.
Delete 🗑	Delete self- defined IP or IP range.
Apply	Click “Apply” to save the network configuration modification
Cancel	Click “Cancel" to leave without making any changes.

Remote IP Group Management:

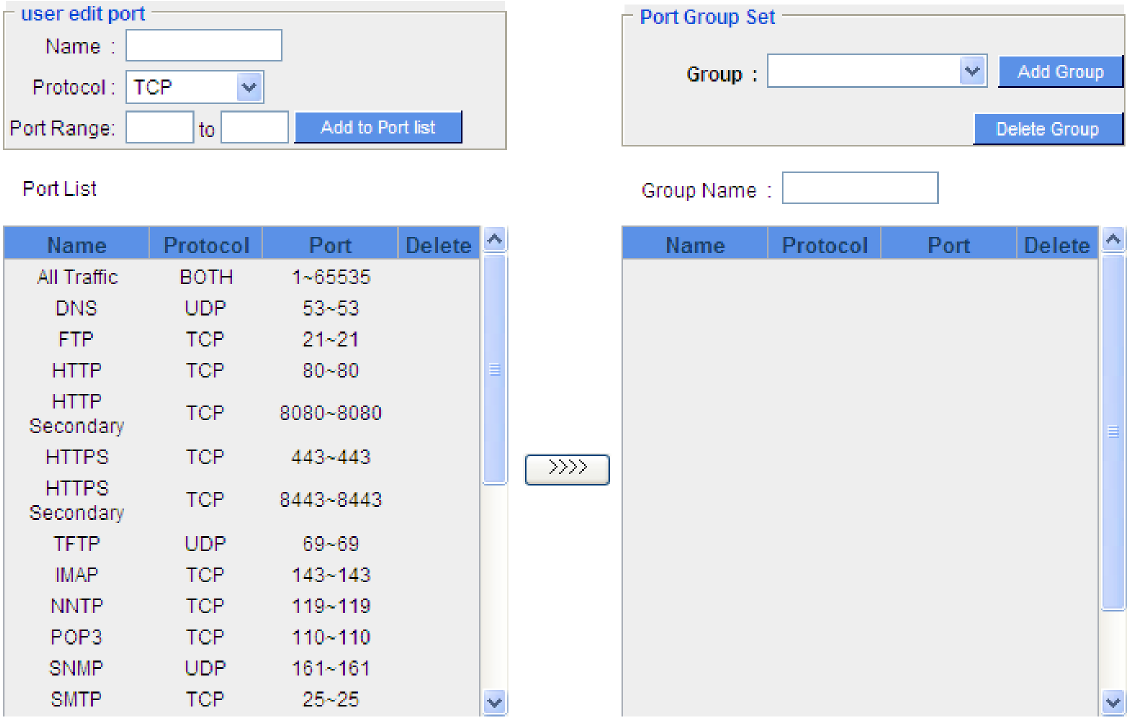
Basically, Remote IP Group setups are exactly the same as Local IP Group setups. However, remote IP group does not have automatically learning functions. Instead, you need to define addresses, ranges and groups manually. For example, 220.130.188.1 to 200 (range).



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.



Name :

Protocol : TCP

Port Range: to

Group :

Group Name :

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	

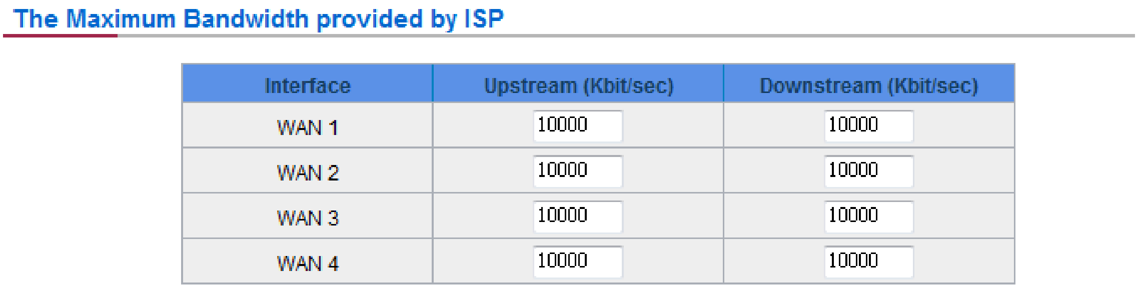
Name	Protocol	Port	Delete

Item	Description
User edit port	Input the name, protocol, and port range for the specific service port.
Name	Name the Port in order to identify its property. For example, Virus 135.
Protocol	Choose the port protocol form the pull down list like TCP, UDP or TCP and UDP.
Port Range	Input the port range. For example, 135 to 135.
Add to Port List	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.
Group Name	When you add new groups, please note if the group name is in the column. For example, Virus.
Delete Group	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.
Delete	Delete self- defined port or port range.
Apply	Click "Apply" to save the network configuration modification

Chapter 8: QoS (Quality of Service)

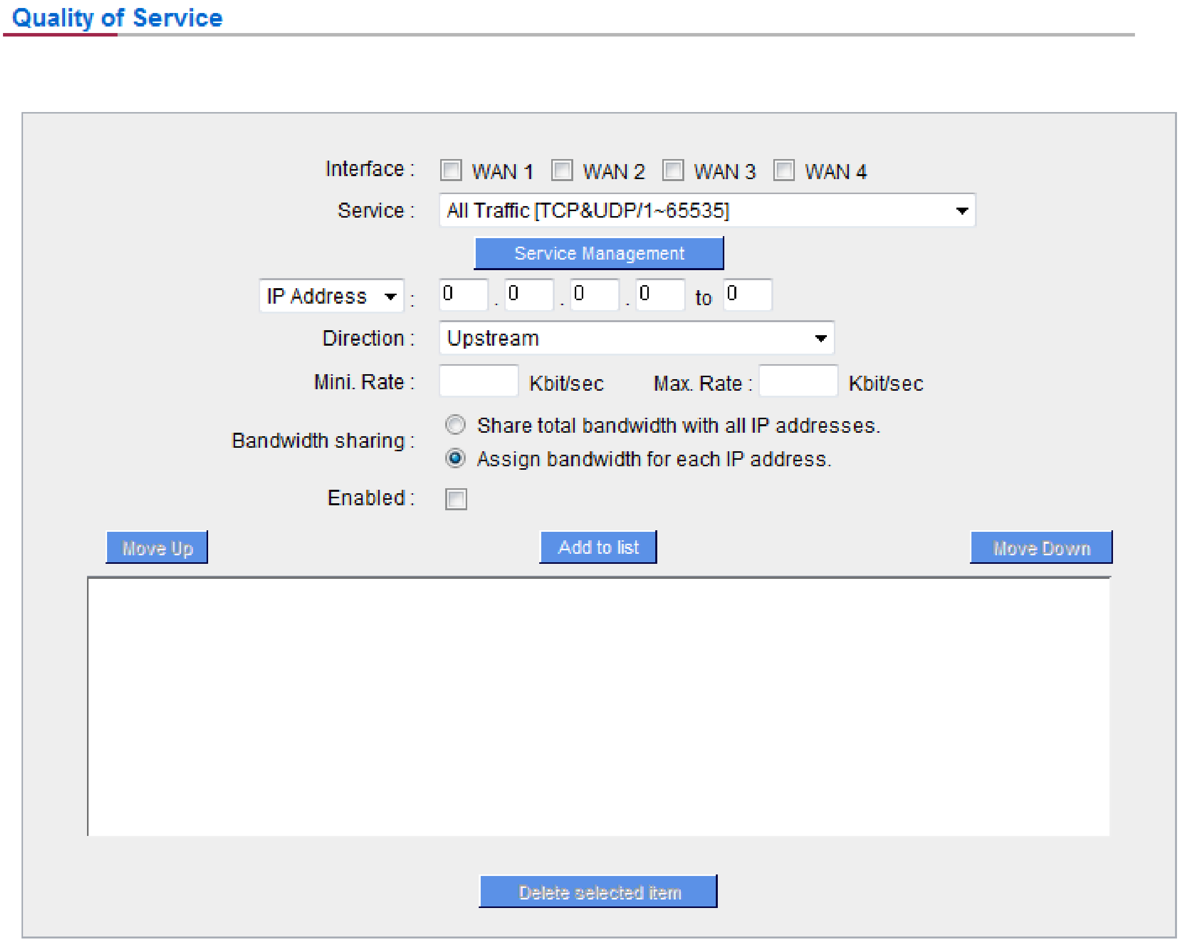
QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IP addresses to save bandwidth or provide priority to specific applications or services, and also to enable other users to share bandwidth, as well as to ensure stable and reliable network 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



Quality of Service

Interface : □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4

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

Service Management

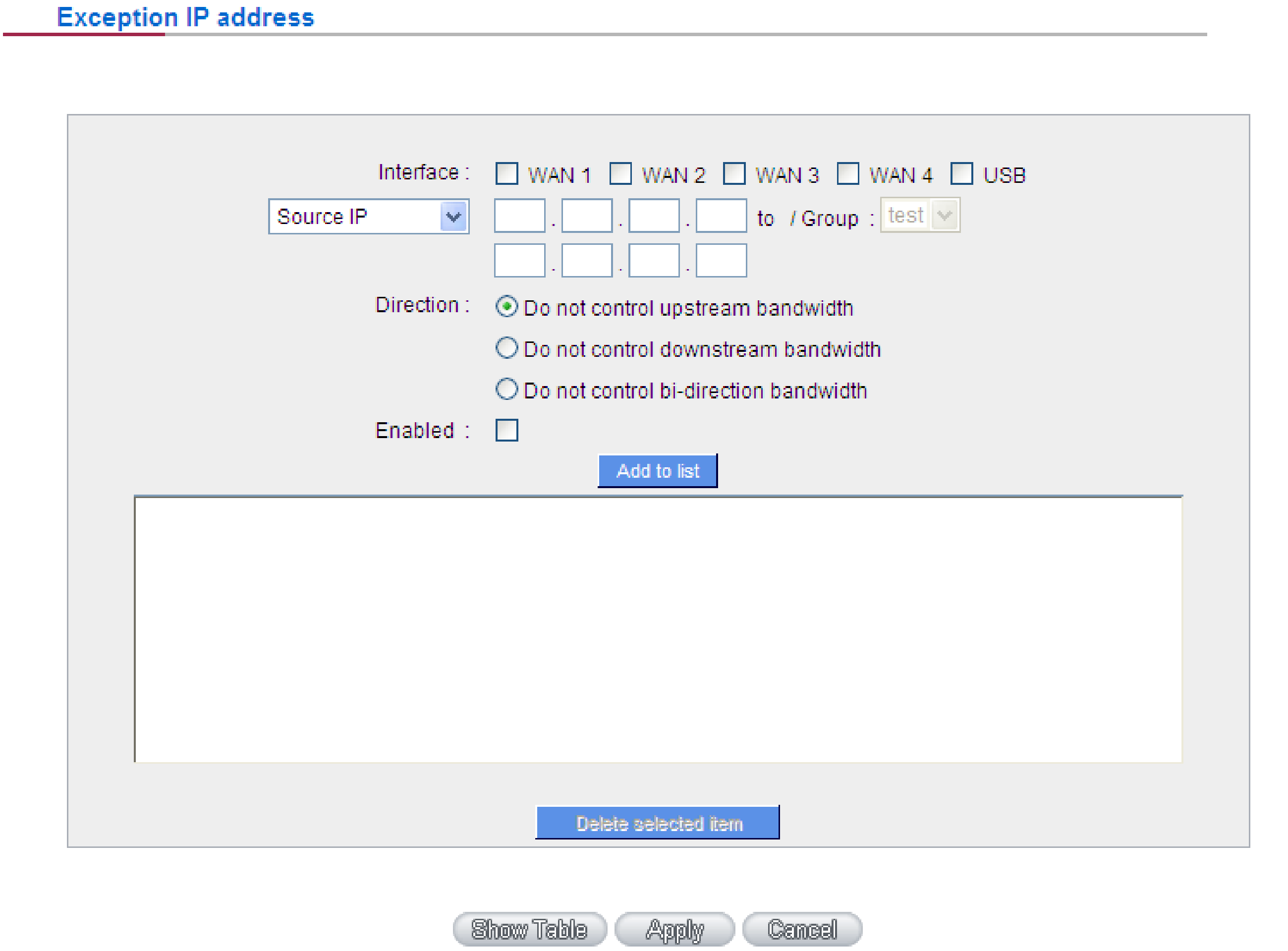
IP Address : 0 . 0 . 0 . 0 to 0

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 : □



Exception IP address

Interface : □ WAN 1 □ WAN 2 □ WAN 3 □ WAN 4 □ USB

Source IP ▾ [ ] . [ ] . [ ] . [ ] to / Group : test ▾

[ ] . [ ] . [ ] . [ ]

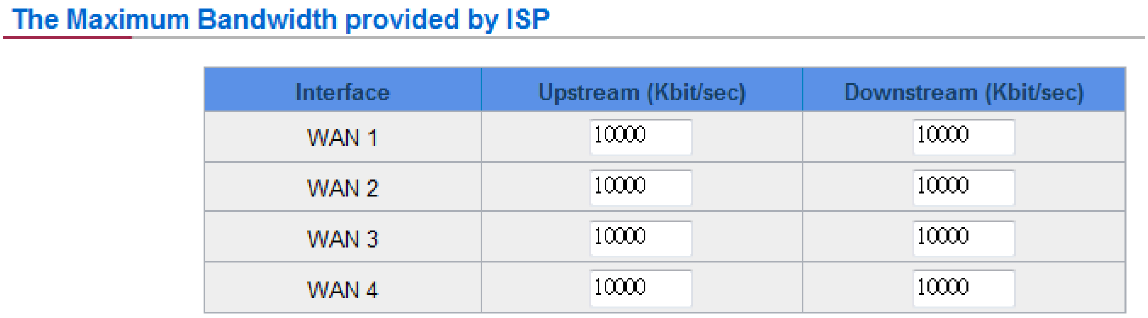
Direction : ● Do not control upstream bandwidth

○ 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	10000	10000
WAN 2	10000	10000
WAN 3	10000	10000
WAN 4	10000	10000

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.

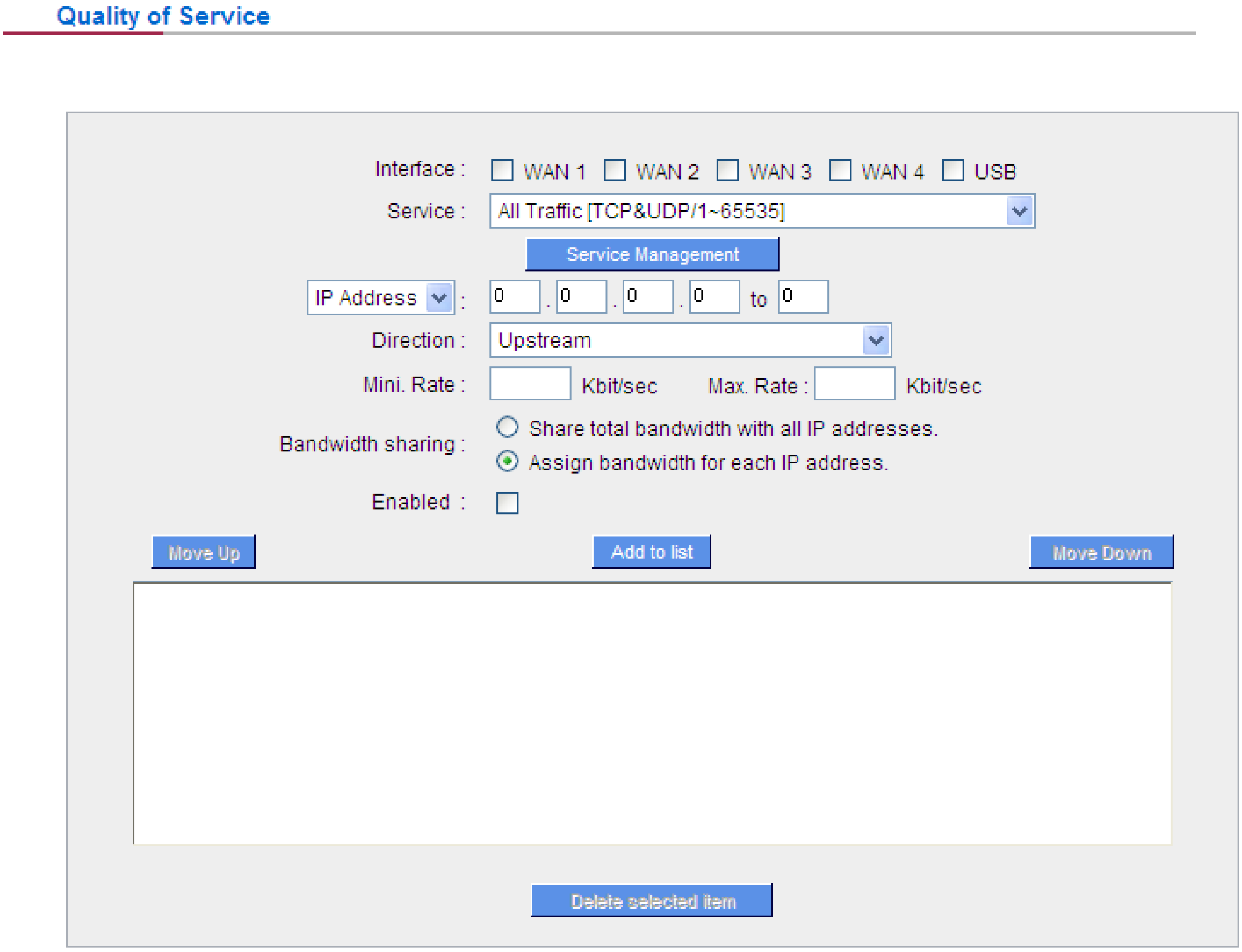
✍ **Attention**	The rules configured in Protocol Binding will be executed by the device according to their priorities too. The higher up on the list, the higher the priority of execution. The unit of calculation in this example is Kbit. Some software indicates the downstream/upstream speed with the unit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

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

Direction : Upstream

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

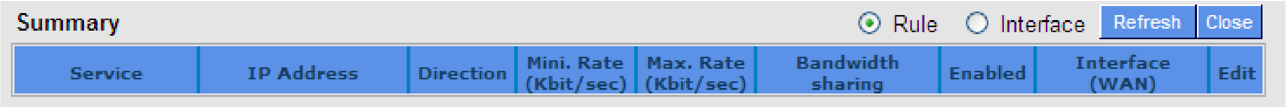
Bandwidth sharing : ○ Share total bandwidth with all IP addresses. ● Assign bandwidth for each IP address.

Enabled : □

Item	Description
Interface	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service Port	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.
IP Address	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.
Direction	**Upstream:** Means the upload bandwidth for Intranet IP. **Downstream:** Means the download bandwidth for Intranet IP. 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. 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.
Min. & Max. Rate(Kbit/Sec)	**The minimum bandwidth:** The rule is to guarantee minimum available bandwidth. **The maximum bandwidth:** This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule. ✍ **Attention** The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.
Bandwidth Assign Type	**Sharing total bandwidth with all IP addresses**: If this option is selected, all IP addresses or Service Ports will share the bandwidth range (from minimum to maximum bandwidth). 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

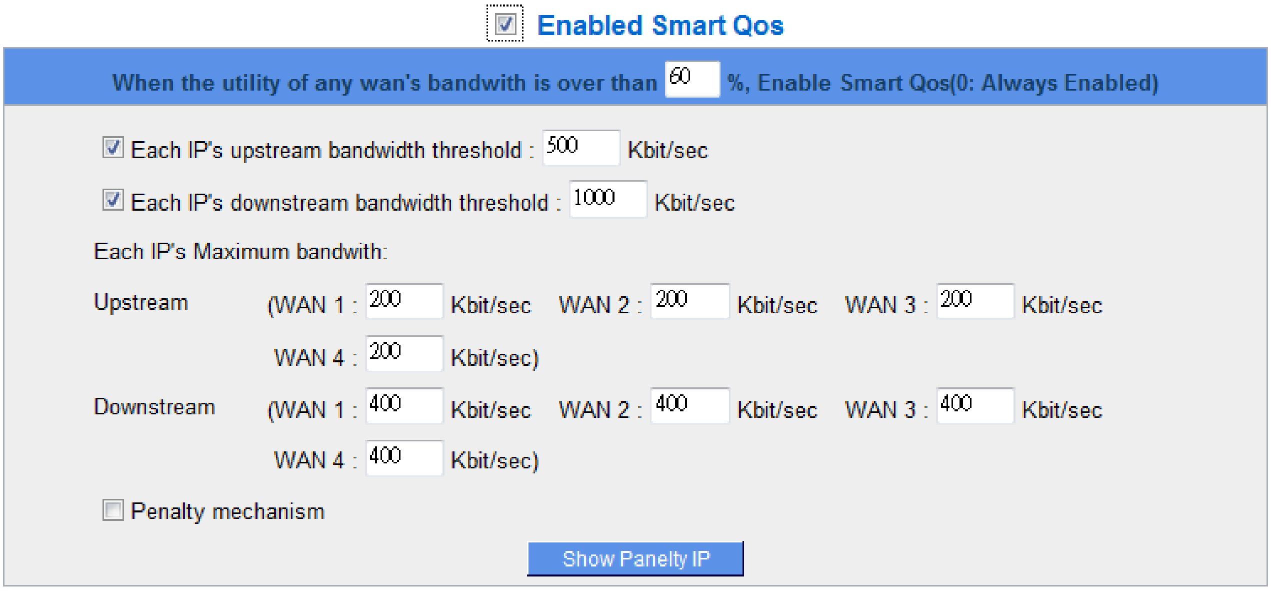
	example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth. ✍ **Attention** If "Share-Bandwidth" is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small. 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.
Enable	Activate the rule.
Add to list	Add this rule to the list.
Move up & Move down	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.
Delete selected items	Remove the rules selected from the Service List.
Show Table	Display all the Rate Control Rules users made for the bandwidth. Click "Edit" to modify.
Apply	Click "Apply" to save the configuration
Cancel	Click "Cancel" to leave without making any change.

Show Table



Service	IP Address	Direction	Mini. Rate (Kbit/sec)	Max. Rate (Kbit/sec)	Bandwidth sharing	Enabled	Interface (WAN)	Edit

8.1.3 Smart QoS



☑ Enabled Smart Qos

When the utility of any wan's bandwith is over than 60 %, Enable Smart Qos(0: Always Enabled)

☑ Each IP's upstream bandwidth threshold : 500 Kbit/sec

☑ Each IP's downstream bandwidth threshold : 1000 Kbit/sec

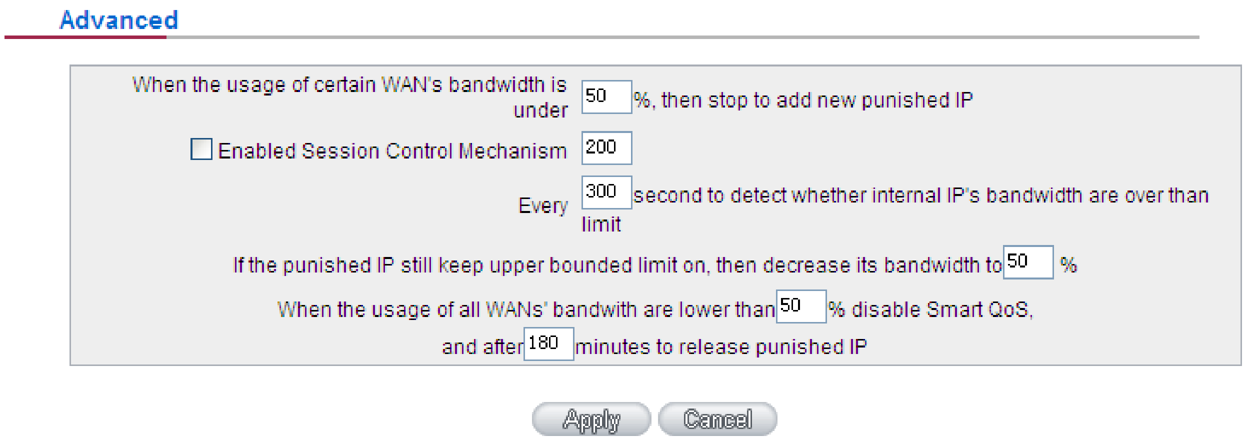
Each IP's Maximum bandwith:

Upstream (WAN 1 : 200 Kbit/sec WAN 2 : 200 Kbit/sec WAN 3 : 200 Kbit/sec WAN 4 : 200 Kbit/sec)

Downstream (WAN 1 : 400 Kbit/sec WAN 2 : 400 Kbit/sec WAN 3 : 400 Kbit/sec WAN 4 : 400 Kbit/sec)

☐ Penalty mechanism

Item	Description
Enabled QoS	Choose to apply QoS function.
When the usage of any WAN's bandwidth is over___%, Enable Smart QoS	Input the required rate value into the column. The default is 60%.
Each IP's upstream bandwidth threshold (for all WAN)	Input the max. upstream rate for intranet IPs.
Each IP's downstream bandwidth threshold (for all WAN)	Input the max. downstream rate for intranet IPs.
Each IP's bandwidth is over maximum threshold, its maximum bandwidth will remain	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.
Penalty Mechanism	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.
Show Penalty List	The IPs which are under penalty mechanism will be shown on the list.



Advanced

When the usage of certain WAN's bandwidth is under 50 %, then stop to add new punished IP

□ Enabled Session Control Mechanism 200

Every 300 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 50 %

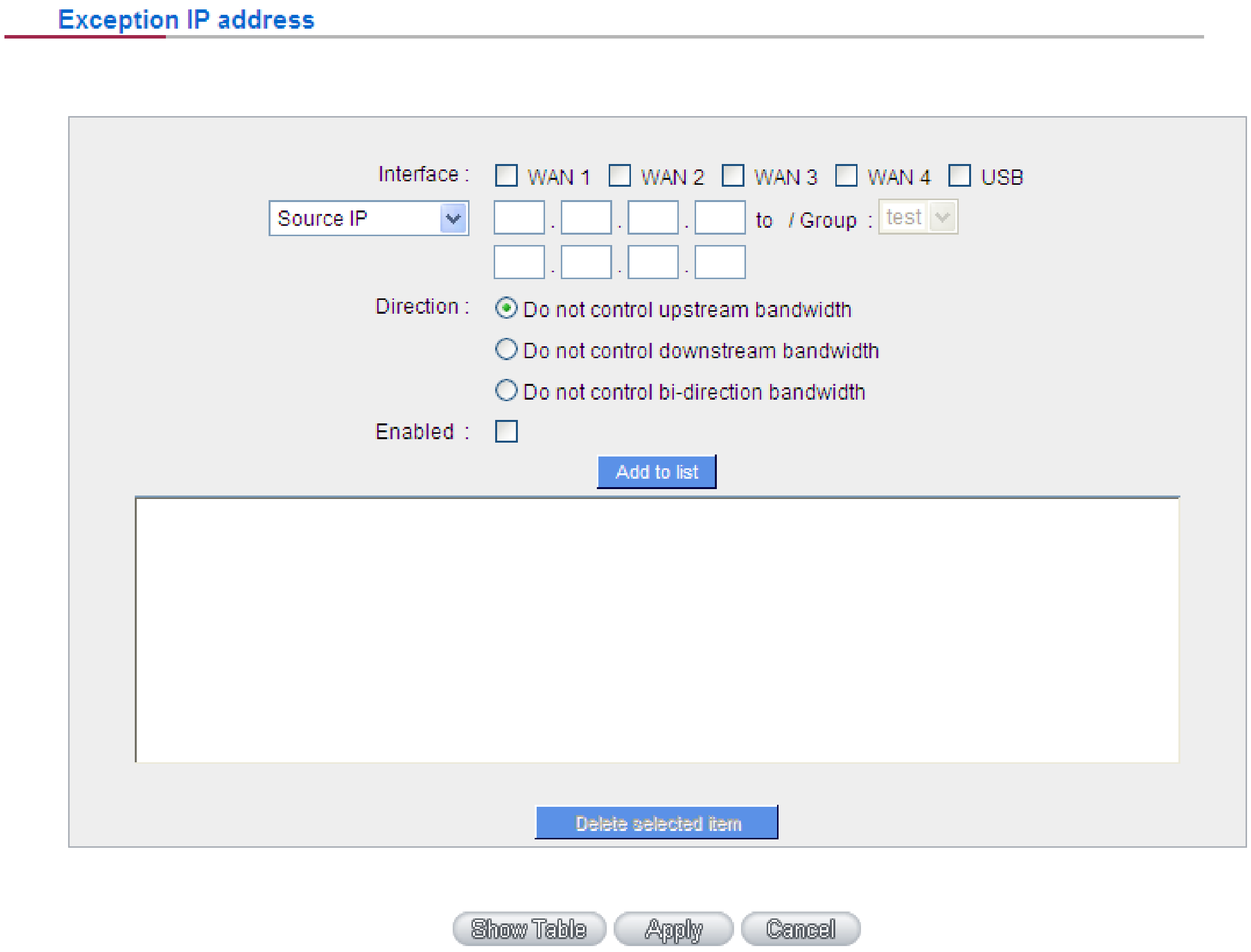
When the usage of all WANs' bandwith are lower than 50 % disable Smart QoS,

and after 180 minutes to release punished IP

Item	Description
When the usage of certain WAN's bandwidth is under__%, then stop to add new punished IP	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 actived.
Every __ second to detect whether internal IP's bandwidth are over than limit	Detect usage of internal IP's bandwidth every __ second.
If the punished IP still keep upper bounded limit on, then decrease its bandwidth to__%	If the punished IP still keep over the limit, the limit badwidth will be decrase to __%.
When the usage of all WANs' bandwith are lower than__% disable Smart Qos, and after__minutes to release punished IP	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

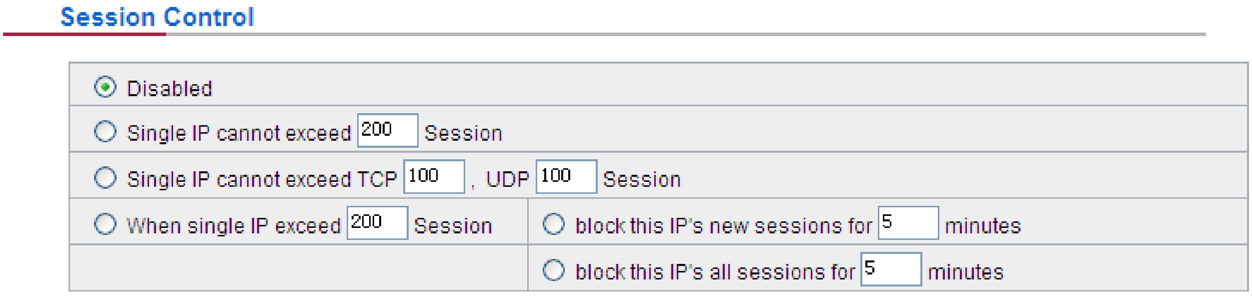
Item	Description
WAN	Select WAN ports.
Source IP	Enter the exempted IP range, or select the exempted IP group.
Do not control Direction	Select do not control upload, download, or both of them.
Enabled	Enable this policy.
Add to List	Add this policy into the exempted list.
Delete Selected item	Delete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

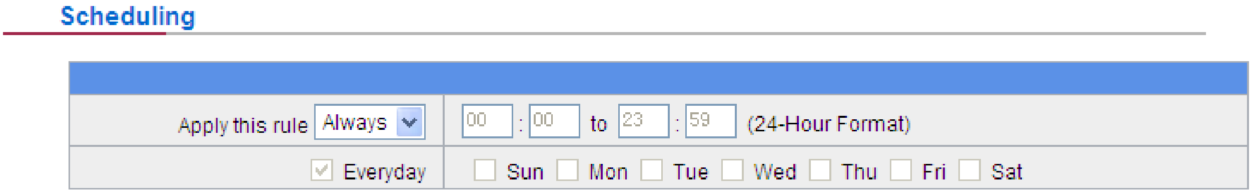
● Disabled

○ Single IP cannot exceed 200 Session

○ Single IP cannot exceed TCP 100 , UDP 100 Session

○ When single IP exceed 200 Session ○ block this IP's new sessions for 5 minutes

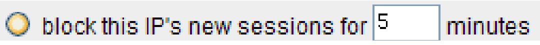
○ block this IP's all sessions for 5 minutes



Scheduling

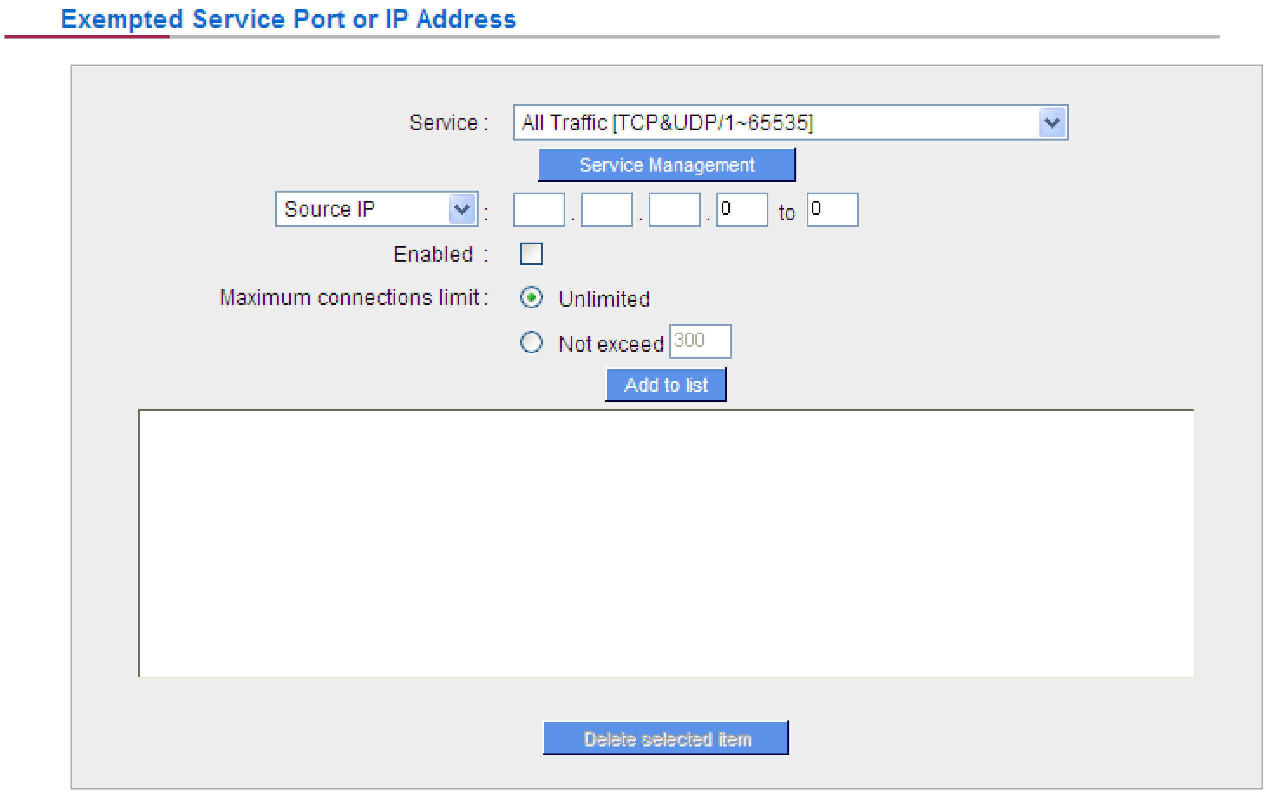
Apply this rule Always 00 : 00 to 23 : 59 (24-Hour Format)

☑ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Item	Description
Disabled	Disable Session Control function.
Single IP cannot exceed __ session	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.
When single IP exceed __	 ○ block this IP's new sessions for 5 minutes 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. ○ block this IP's all sessions for 5 minutes If this function is selected, when the user's port connections reach the limit, all the

	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.
Scheduling	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.
Apply	Click "Apply" to save the configuration.
Cancel	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]

Source IP : . . . 0 to 0

Enabled : □

Maximum connections limit : ● Unlimited

○ Not exceed 300

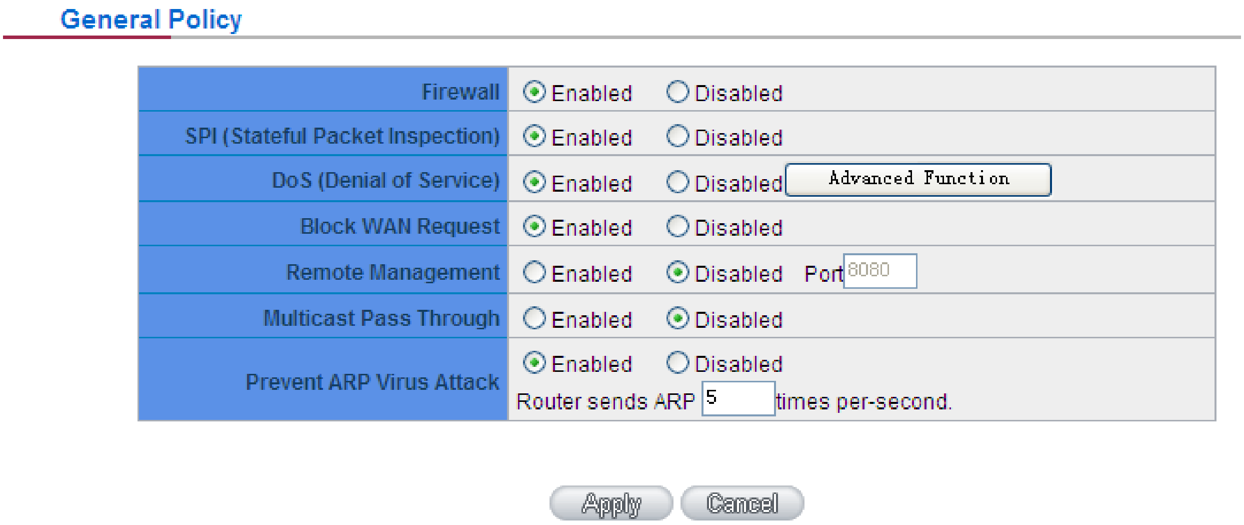
Item	Description
Service Port	Choose the service port.
IP Address	Input the IP address range or IP group.
Enabled	Activate the rule.
Add to list	Add this rule to the list.
Delete seleted item	Remove the rules selected from the Service List.
Apply	Click **"Apply"** to save the configuration.
Cancel	Click **"Cancel"** 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.



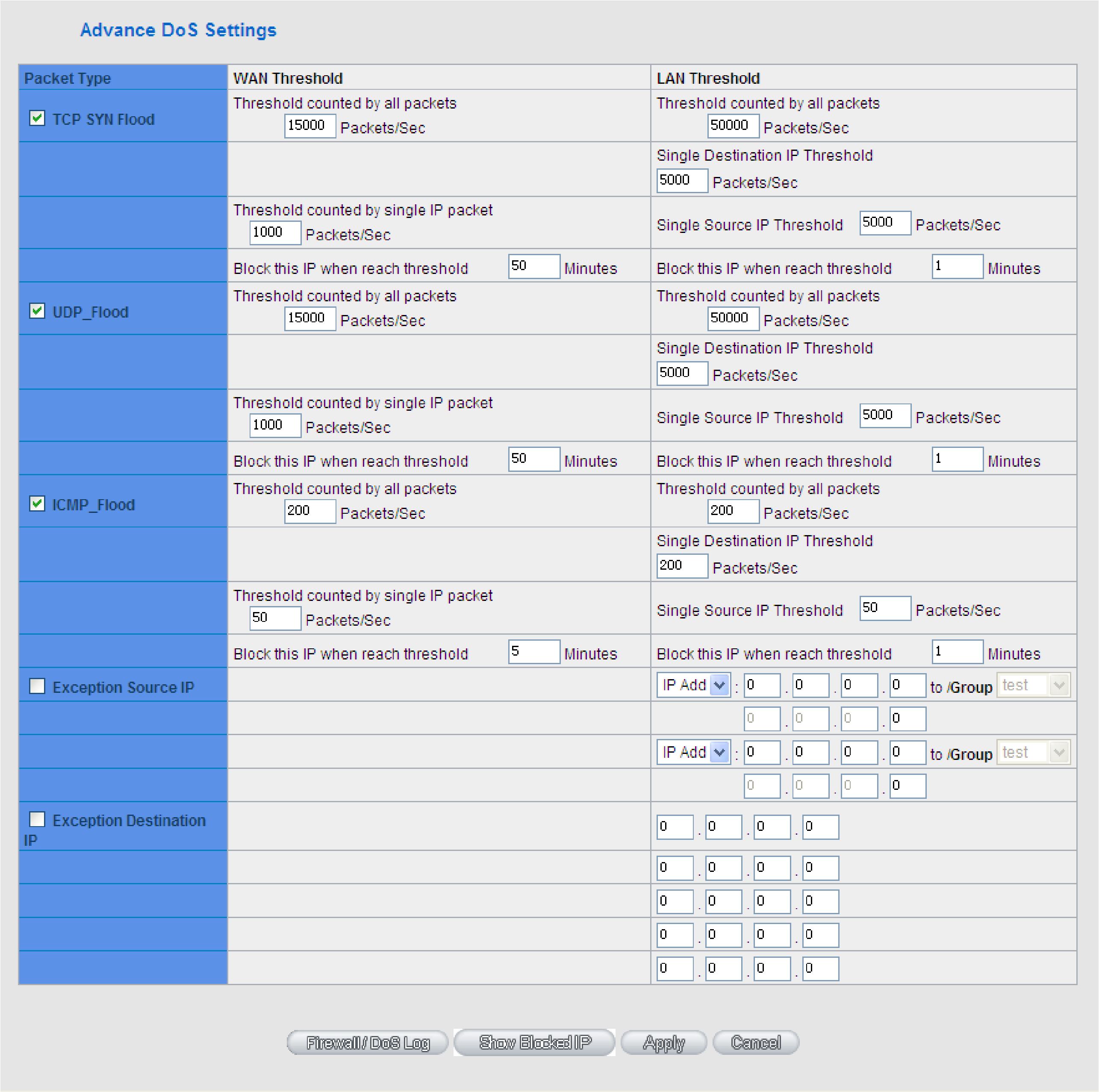
General Policy

Firewall	● Enabled ○ Disabled
SPI (Stateful Packet Inspection)	● Enabled ○ Disabled
DoS (Denial of Service)	● Enabled ○ Disabled [Advanced Function]
Block WAN Request	● Enabled ○ Disabled
Remote Management	○ Enabled ● Disabled Port 8080
Multicast Pass Through	○ Enabled ● Disabled
Prevent ARP Virus Attack	● Enabled ○ Disabled Router sends ARP 5 times per-second.

Item	Description
Firewall	This feature allows users to turn on/off the firewall.
SPI (Stateful Packet Inspection)	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.
DoS (Denial of Service)	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, IP Spoofing and so on.
Block WAN request	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.
Remote Management	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).
Multicast Pass	There are many audio and visual streaming media on the network. Broadcasting

Through	may allow the client end to receive this type of packet message format. This feature is off by default.
Prevent ARP Virus Attack	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

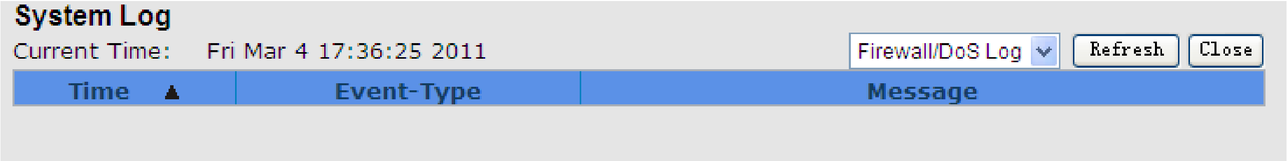


Advance DoS Settings

Packet Type	WAN Threshold	LAN Threshold
☑ TCP SYN Flood	Threshold counted by all packets 15000 Packets/Sec	Threshold counted by all packets 50000 Packets/Sec
		Single Destination IP Threshold 5000 Packets/Sec
	Threshold counted by single IP packet 1000 Packets/Sec	Single Source IP Threshold 5000 Packets/Sec
	Block this IP when reach threshold 50 Minutes	Block this IP when reach threshold 1 Minutes
☑ UDP_Flood	Threshold counted by all packets 15000 Packets/Sec	Threshold counted by all packets 50000 Packets/Sec
		Single Destination IP Threshold 5000 Packets/Sec
	Threshold counted by single IP packet 1000 Packets/Sec	Single Source IP Threshold 5000 Packets/Sec
	Block this IP when reach threshold 50 Minutes	Block this IP when reach threshold 1 Minutes
☑ ICMP_Flood	Threshold counted by all packets 200 Packets/Sec	Threshold counted by all packets 200 Packets/Sec
		Single Destination IP Threshold 200 Packets/Sec
	Threshold counted by single IP packet 50 Packets/Sec	Single Source IP Threshold 50 Packets/Sec
	Block this IP when reach threshold 5 Minutes	Block this IP when reach threshold 1 Minutes
☐ Exception Source IP		IP Add : 0 . 0 . 0 . 0 to /Group test
		0 . 0 . 0 . 0
		IP Add : 0 . 0 . 0 . 0 to /Group test
		0 . 0 . 0 . 0
☐ Exception Destination IP		0 . 0 . 0 . 0
		0 . 0 . 0 . 0
		0 . 0 . 0 . 0
		0 . 0 . 0 . 0
		0 . 0 . 0 . 0

Item	Description
Packet Type	This device provides three types of data packet transmission: TCP-SYN-Flood, UDP-Flood and ICMP-Flood.
WAN Threshold	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.
LAN Threshold	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.
Exempted Source IP	Input the exempted source IP.
Exempted Dest. IP	Input the exempted Destination IP addresses.
Apply	Click **"Apply"** to save the configuration.
Cancel	Click **"Cancel"** to leave without making any change.

Firewall / DoS Log

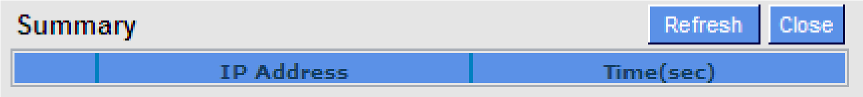


Current Time: Fri Mar 4 17:36:25 2011

Time ▲	Event-Type	Message

Show the Firewall/Log.

Show Blocked IP



	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.

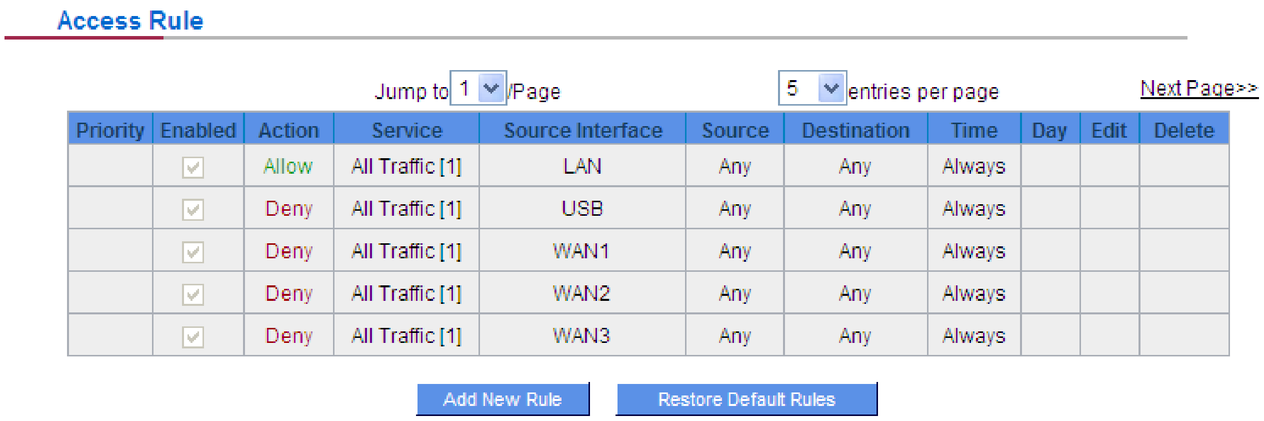
Users may define access rules and do more than the default rules. However, the following four extra service items are always on and are not affected by other user-defined settings.

* 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

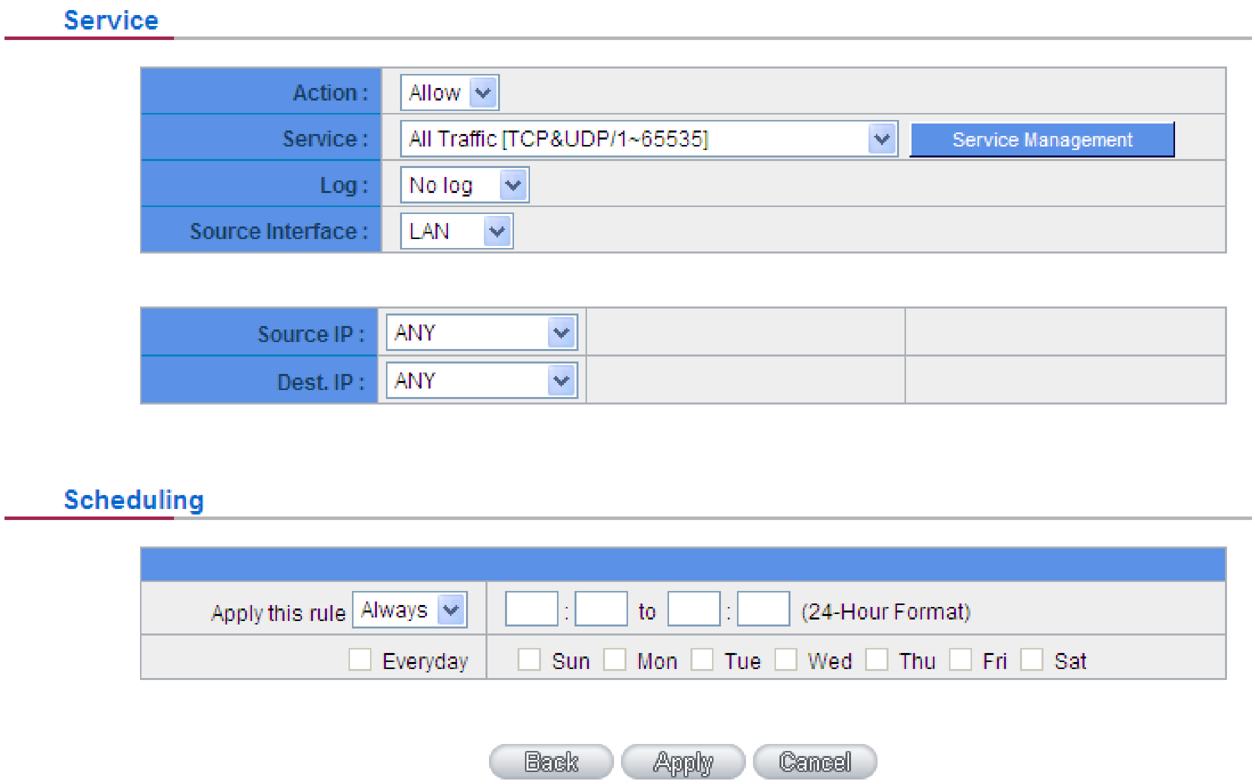
Jump to 1 /Page 5 entries per page Next Page>>

Priority	Enabled	Action	Service	Source Interface	Source	Destination	Time	Day	Edit	Delete
	☑	Allow	All Traffic [1]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [1]	USB	Any	Any	Always			
	☑	Deny	All Traffic [1]	WAN1	Any	Any	Always			
	☑	Deny	All Traffic [1]	WAN2	Any	Any	Always			
	☑	Deny	All Traffic [1]	WAN3	Any	Any	Always			

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
Edit:	Define the network access rule item
Delete:	Remove the item.
Add New Rule:	Create a new network access rule
Return to Default Rule:	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]
Log :	No log
Source Interface :	LAN

Source IP :	ANY
Dest. IP :	ANY

Scheduling

Apply this rule Always : to : (24-Hour Format)

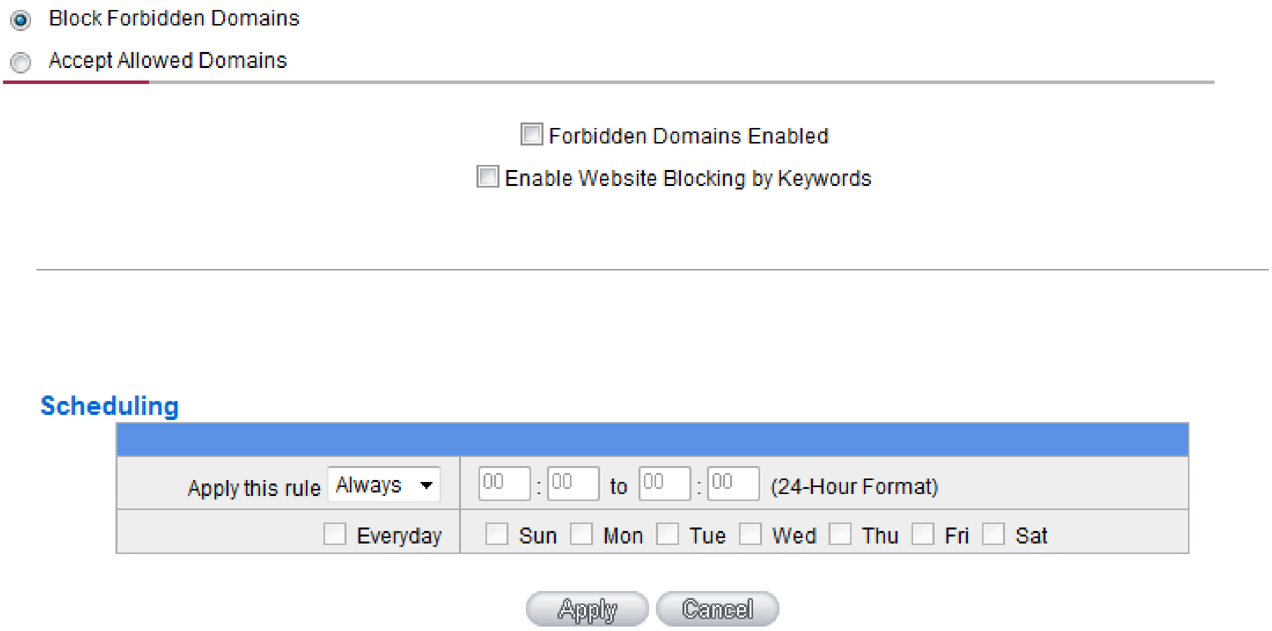
□ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Item	Description
Action	Allow: Permits the pass of packets compliant with this control rule. Deny: Prevents the pass of packets not compliant with this control rule.
Service Port	From the drop-down menu, select the service that users grant or do not give permission.
Service Port Management	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.
Log	No Log: There will be no log record. Create Log when matched: Event will be recorded in the log.
Interface	Select the source port whether users are permitted or not (for example: LAN, WAN1,

	WAN2 or Any). Select from the drop-down menu.
Source IP	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.
Dest. IP	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.
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.
Apply this rule	Select "Always" to apply the rule on a round-the-clock basis. If "From" is selected, the activation time is introduced as below
… to …	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.)
Day Control	"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.
Apply	Click "Apply" to save the configuration.
Cancel	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 Keywords

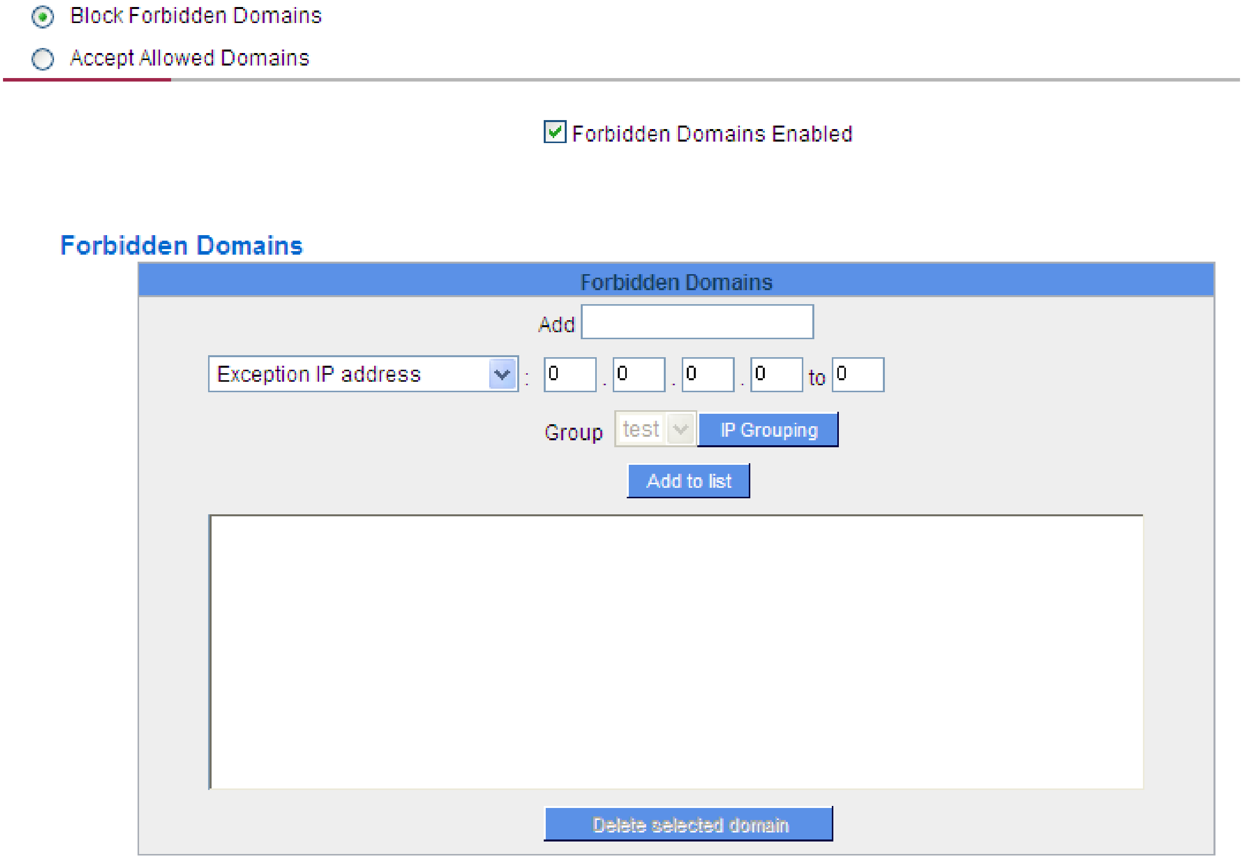
Scheduling

Apply this rule Always | 00 : 00 to 00 : 00 (24-Hour Format)

□ Everyday | □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

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

Forbidden Domains

Add

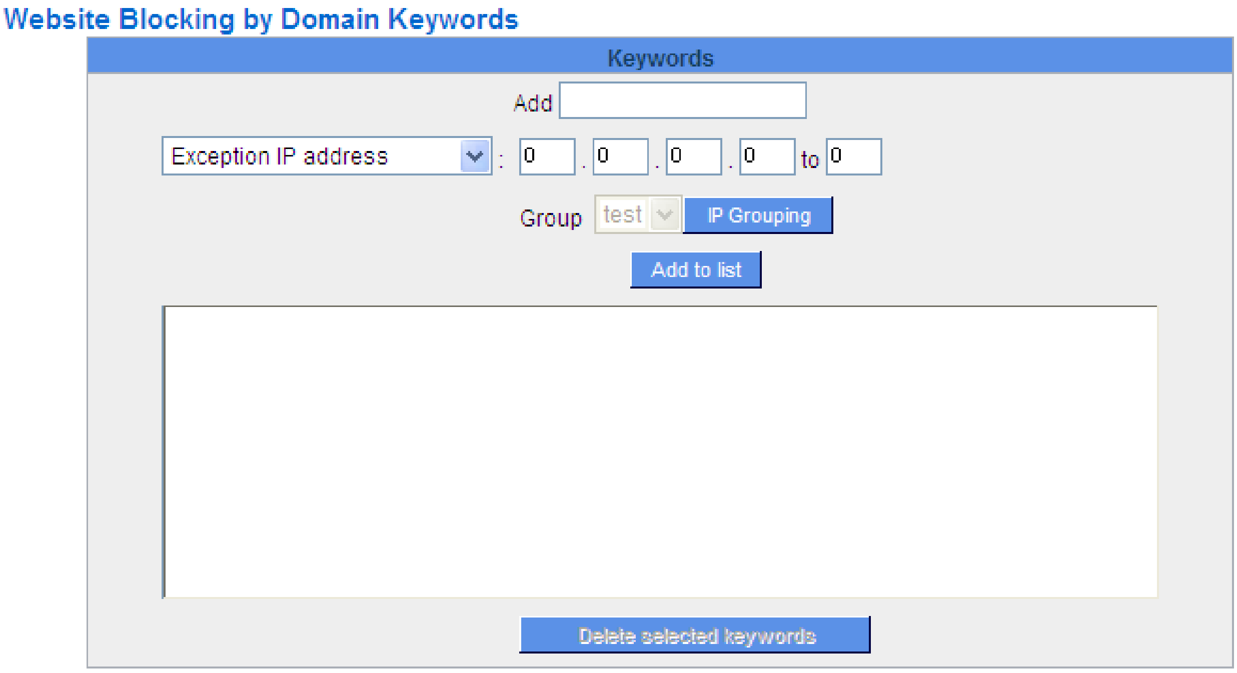
Exception IP address : 0 . 0 . 0 . 0 to 0

Group test

Item	Description
Forbidden Domains Enabled	Click to enable the forbidden domains function. Default is Disabled.
Add	Input the website to be controlled. For example, www.playboy.com
Exception IP Address	Input the IP or IP ranges not to be controlled.
Add to list	Click "Add to list" to create a new website to be controlled.
Delete selected domain	Click to select one or more controlled websites and click this option to delete.
Apply	Click **"Apply"** to save the configuration.
Cancel	Click **"Cancel"** to leave without making any change.

Website Blocking by Keywords

☑ Enable Website Blocking by Domain Keywords



Website Blocking by Domain Keywords

Exception IP address: 0 . 0 . 0 . 0 to 0

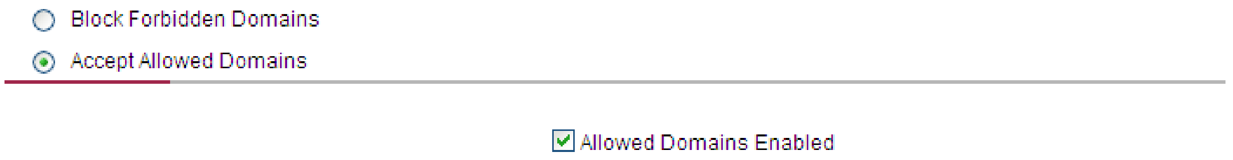
Group: test

Item	Description
Enabled	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.
Keywords（Only for English keyword）	Enter keywords.
Add to List	Add this new service item content to the list.
Delete selected item	Delete the service item content from the list

Apply	Click “Apply” to save the modified parameters.
Cancel	Click “Cancel” to cancel all the changes made to the parameters.

Accept Allowed Domains

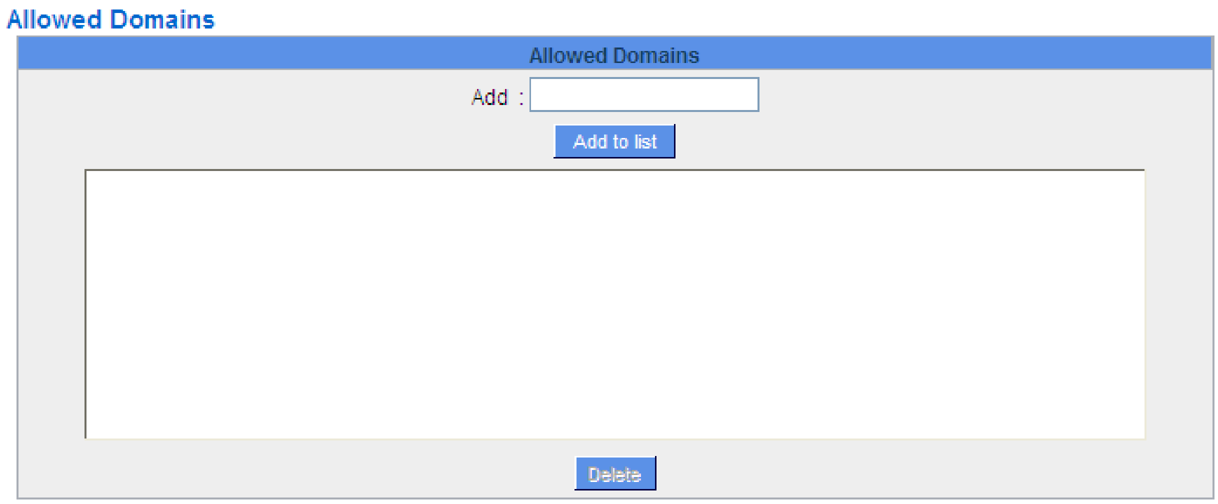
In some companies or schools, employees and students are only allowed to access some specific websites. This is the purpose of the function.



○ Block Forbidden Domains

● Accept Allowed Domains

☑ Allowed Domains Enabled



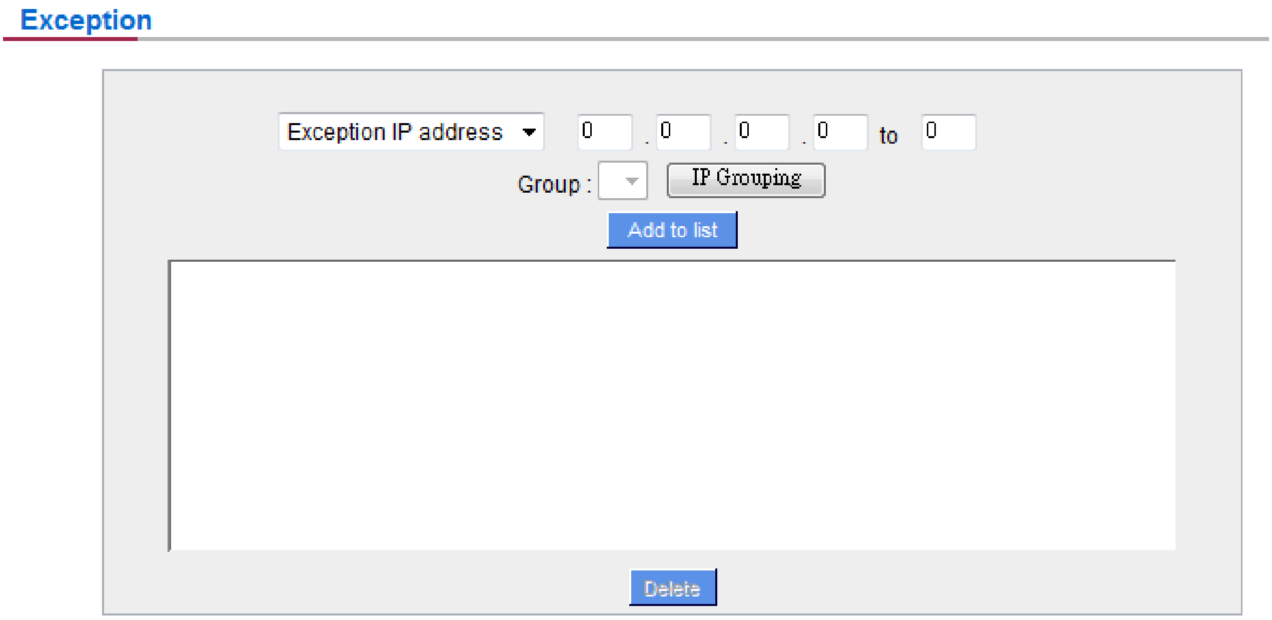
Allowed Domains

Add :

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.”

Exception IP address：

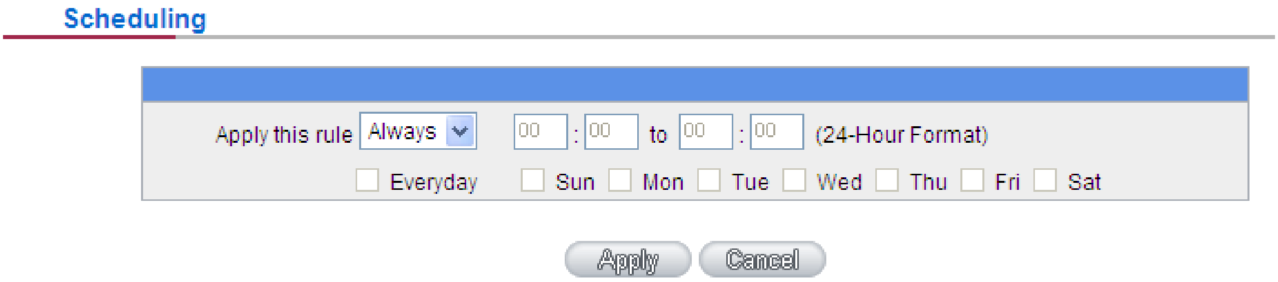
You can exempted some IP addresses or IP group from the “Allow Domain”.



Item	Description
Exception IP address/Group	Enter the exempted IP addresses or IP group.
Add to list	Click this button to add exempted IP addresses or IP group.
Delete selected range	Click this button to delete selected exempted IP address or IP group.

Content Filter Scheduling

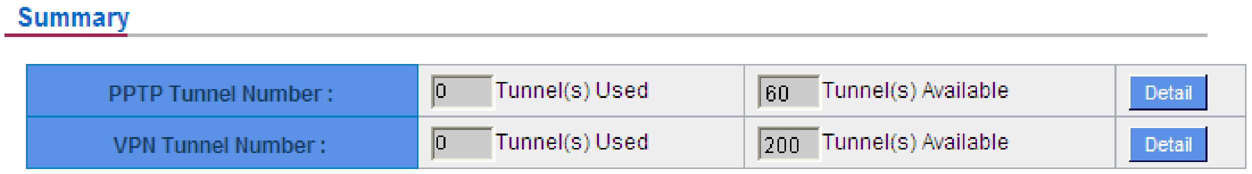
Select **"Always"** to apply the rule on a round-the-clock basis. Select **"from"**, and the operation will run according to the defined time. For example, if the control time runs from 8 a.m. to 6 p.m., Monday to Friday, users may control the operation according to the following illustrated example.


Scheduling
Apply this rule Always
00 : 00 to 00 : 00 (24-Hour Format)
□ Everyday □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Apply
Cancel

Item	Description
Always:	Select **"Always"** to apply the rule on a round-the-clock basis. Select **"from",** and the operation will run according to the defined time.
…to…:	Select "**Always**" to apply the rule on a round-the-clock basis. If "**From**" is selected, the activation time is introduced as below
Day Control:	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.)

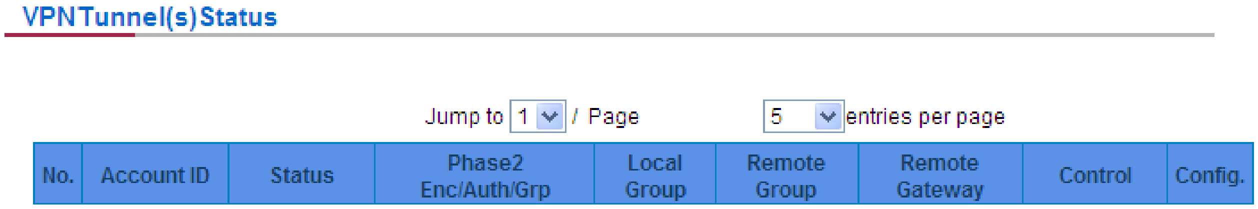
Chapter 10 : VPN (Virtual Private Network)

10.1. Display All VPN Summary



Summary

PPTP Tunnel Number :	0 Tunnel(s) Used	60 Tunnel(s) Available	Detail
VPN Tunnel Number :	0 Tunnel(s) Used	200 Tunnel(s) Available	Detail

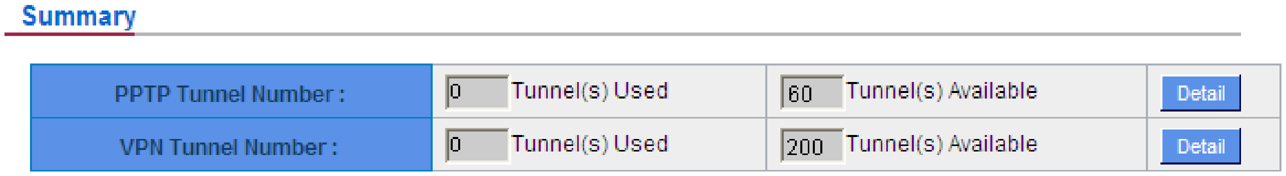


VPN Tunnel(s) Status

Jump to 1 / Page 5 entries per page

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

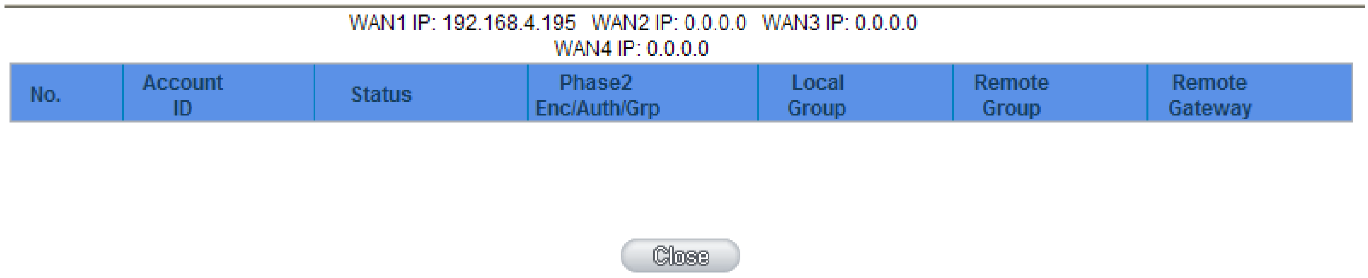
This VPN Summary displays the real-time data with regard to VPN status. These data include: all tunnel numbers, setting parameters and Group VPN and so forth.



Summary

PPTP Tunnel Number :	0 Tunnel(s) Used	60 Tunnel(s) Available	Detail
VPN Tunnel Number :	0 Tunnel(s) Used	200 Tunnel(s) Available	Detail

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

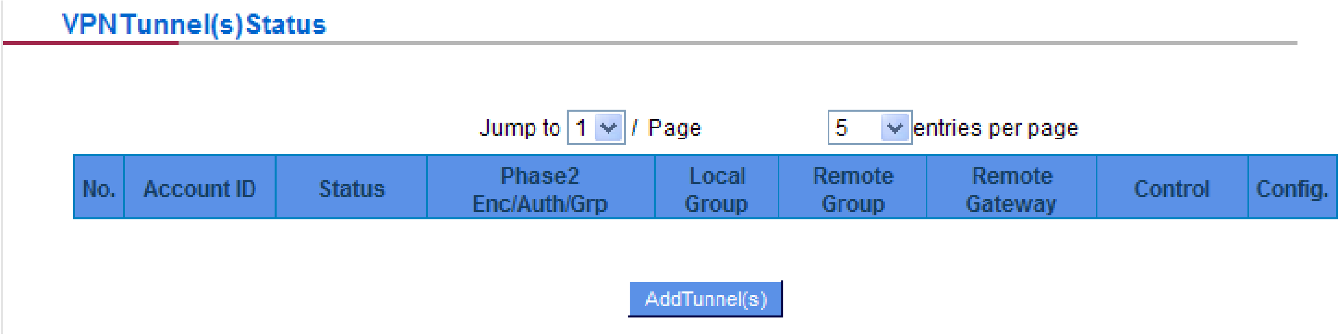


WAN1 IP: 192.168.4.195 WAN2 IP: 0.0.0.0 WAN3 IP: 0.0.0.0
WAN4 IP: 0.0.0.0

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

VPN Tunnel Status:

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



VPNTunnel(s)Status

Jump to 1 / Page 5 entries per page

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

Item	Description
Previous Page/Next Page, Jump to __/__ Page, __ Entries Per Page	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.
Tunnel No.	To set the embedded VPN feature, please select the tunnel number. It supports up to 200 IPSec VPN tunnel Setting (gateway to gateway as well as client to gateway).
Status	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.
Account ID:	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. **Note**: 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.
Phase2 Encrypt/Auth/Group:	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.
Local Group	Displays the setting for VPN connection secure group of the local end.
Remote Group	Displays the setting for remote VPN connection secure group.
Remote Gateway	Set the IP address to connect the remote VPN device. Please set the VPN device

	with a valid IP address or domain name.
Control	Click "Connect" to verify the tunnel status. The test result will be updated. To disconnect, click "Disconnect" to stop the VPN connection.
Config	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.
__ Tunnel(s) Enabled **__ Tunnel(s) Defined**	This displays how many tunnels are enabled and how many tunnels are set.

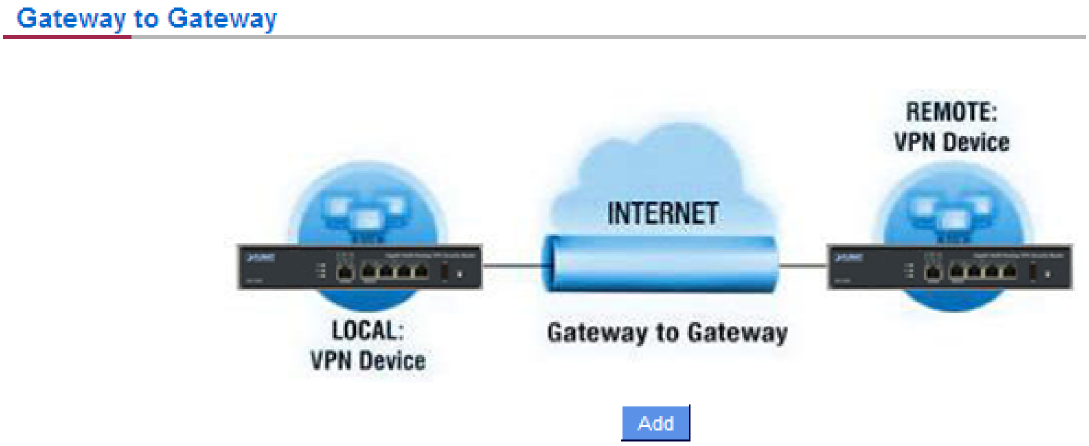
10.1.1. Add a New VPN Tunnel

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.

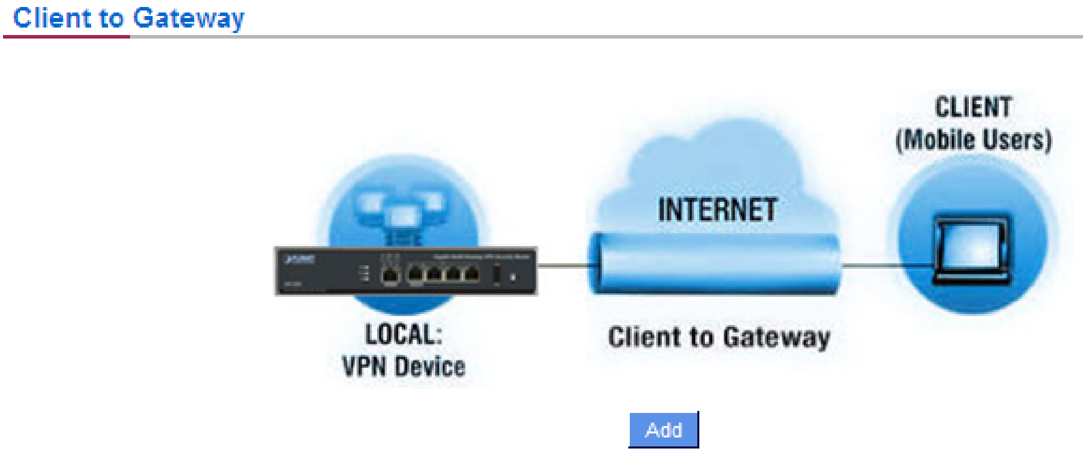
Gateway to Gateway

Click “Add” to enter the setting page of Gateway to Gateway.



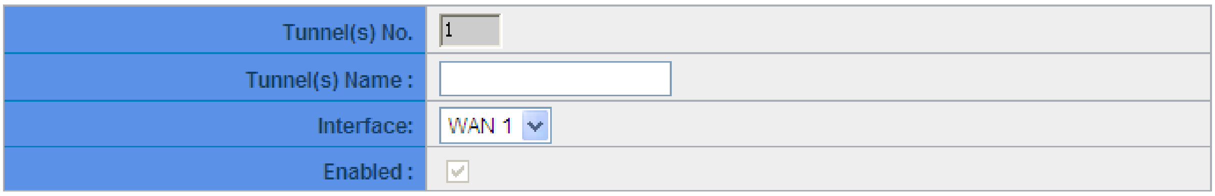
Client to Gateway

Click “Add” to enter the setting page of Client to Gateway.



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

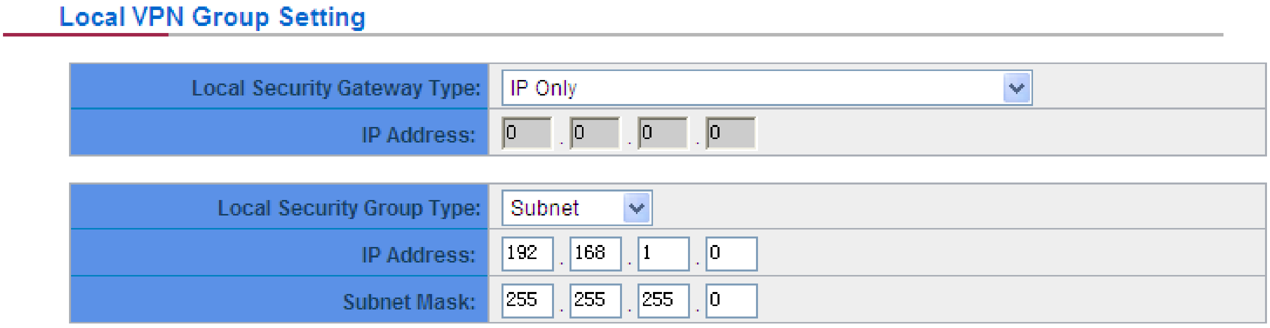
10.1.1.1 Gateway to Gateway Setting



Tunnel(s) No.	1
Tunnel(s) Name :	
Interface:	WAN 1
Enabled :	☑

Item	Description
Tunnel No.	Set the embedded VPN feature, please select the Tunnel number.
Tunnel Name	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion. ✍ **Note**: 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.
Interface	From the pull-down menu, users can select the Interface for this VPN tunnel.
Enabled	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

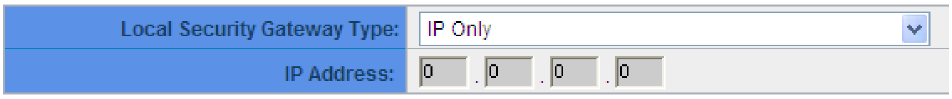


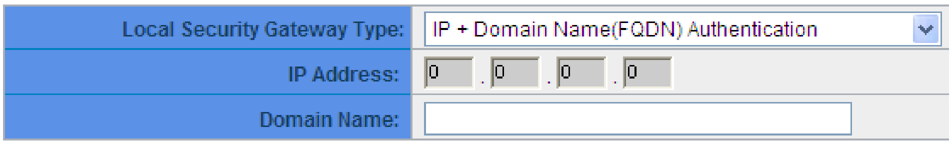
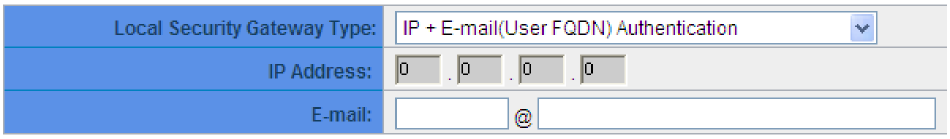
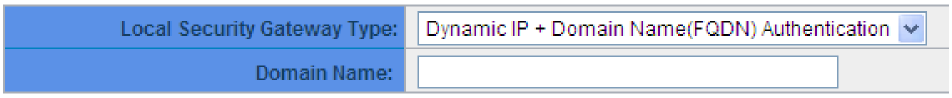
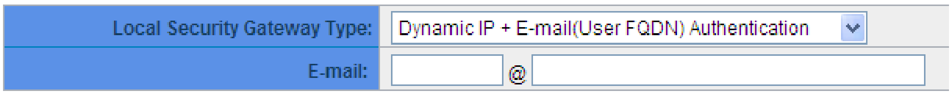
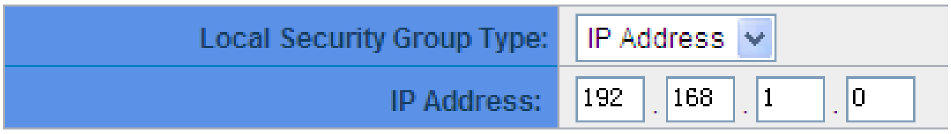
Local VPN Group Setting

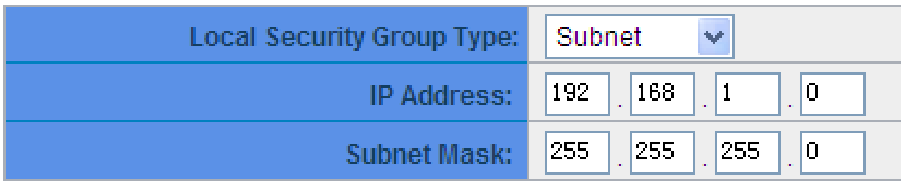
Local Security Gateway Type:	IP Only
IP Address:	0 . 0 . 0 . 0

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

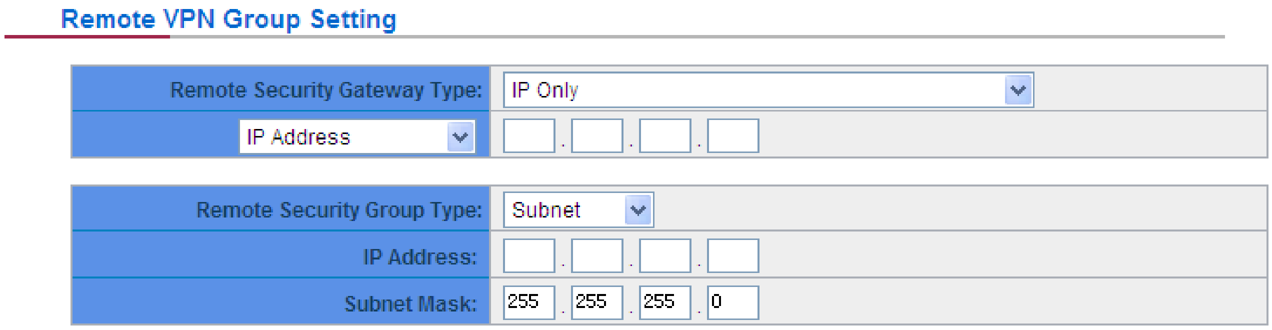
This Local Security Gateway Type must be identical with that of the remote type (Remote Security Gateway Type).

Item	Description
Local Security	This local gateway authentication type comes with five operation modes, which are:
Gateway Type	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 **(1) IP only:** 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.  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: @
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.  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 Group Setup

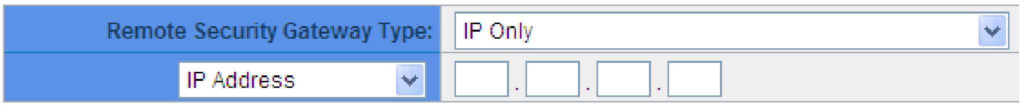
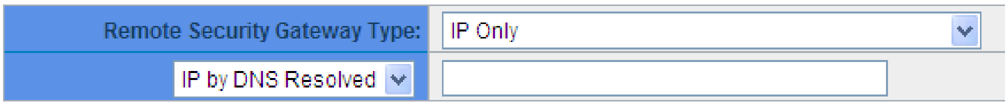


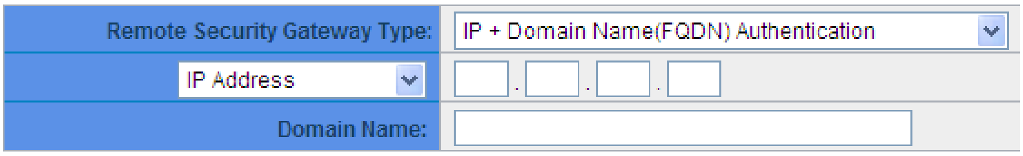
Remote VPN Group Setting

Remote Security Gateway Type:	IP Only
IP Address	. . .

Remote Security Group Type:	Subnet
IP Address:	. . .
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	This remote gateway authentication type comes with five operation modes, which are: **IP only-**Authentication by use of IP only **IP + Domain Name (FQDN) Authentication**, -IP + Domain name **IP + E-mail Addr. (USER FQDN) Authentication**, -IP + Email address **Dynamic IP + Domain Name (FQDN) Authentication**, -Dynamic IP address + Domain name **Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** Dynamic IP address + Email address name **(1) IP only:** If users select the IP Only type, entering this IP allows users to gain access to this tunnel.  Remote Security Gateway Type: IP Only IP Address . . . 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.  Remote Security Gateway Type: IP Only IP by DNS Resolved **(2) IP + Domain Name(FQDN) Authentication**: 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.

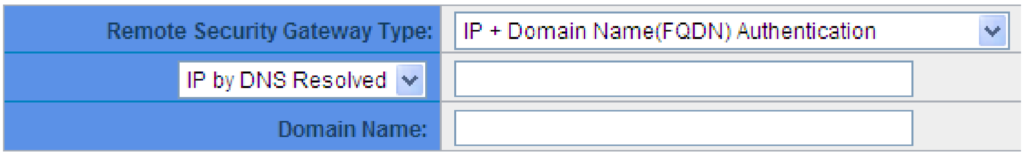


Remote Security Gateway Type: IP + Domain Name(FQDN) Authentication

IP Address: . . .

Domain Name:

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.



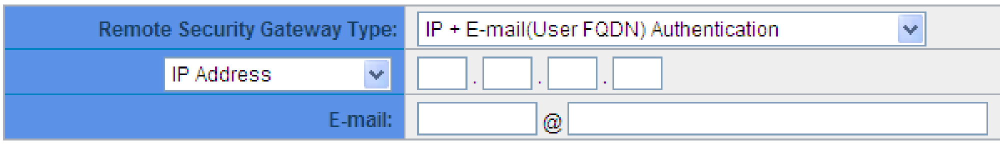
Remote Security Gateway Type: IP + Domain Name(FQDN) Authentication

IP by DNS Resolved:

Domain Name:

(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.

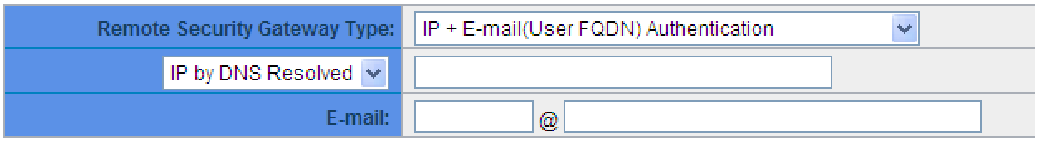


Remote Security Gateway Type: IP + E-mail(User FQDN) Authentication

IP Address: . . .

E-mail: @

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.



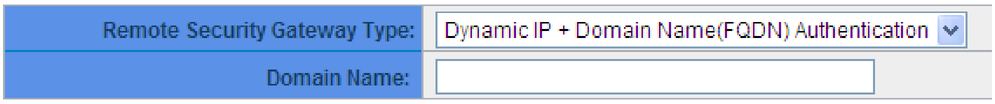
Remote Security Gateway Type: IP + E-mail(User FQDN) Authentication

IP by DNS Resolved:

E-mail: @

(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.

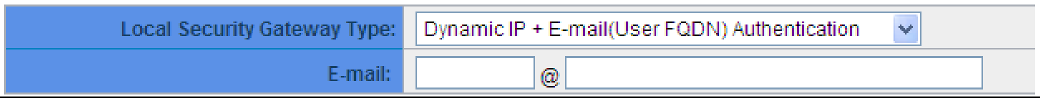


Remote Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name:

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

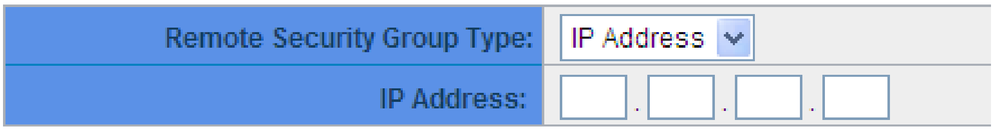
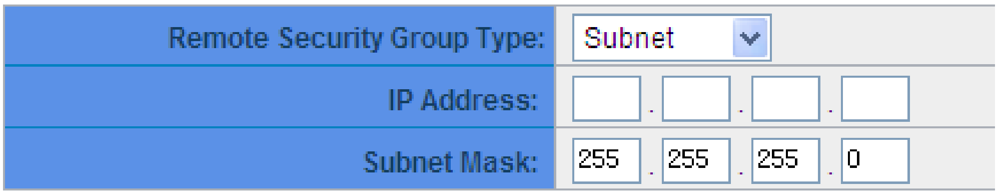
If users use dynamic IP address to connect with the device, users may select this type to link to VPN. When the remote VPN gateway requires connection to facilitate VPN connection, the device will start authentication and respond to the VPN tunnel connection; Please enter the E-Mail to the empty space.



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

E-mail: @

Remote Security	This option allows users to set the remote VPN connection access type. The following

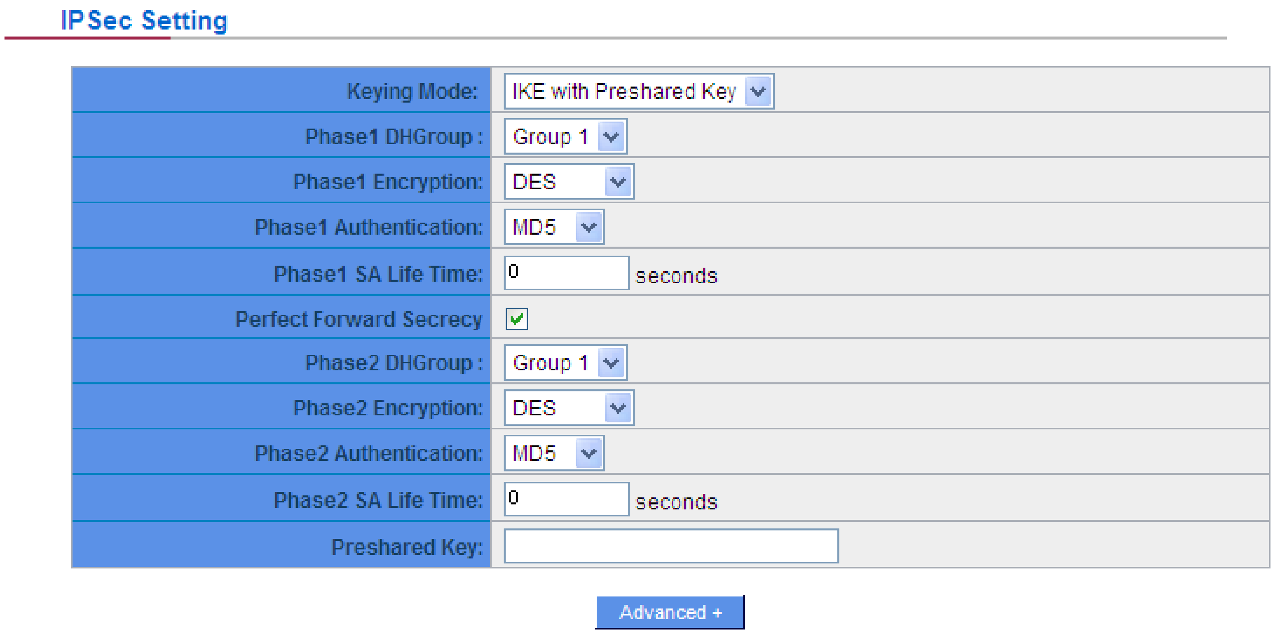
Group Type	offers a few items for remote settings. Please select and set appropriate parameters: **(1) IP address** This option allows the only IP address which is entered to build the VPN tunnel.  Remote Security Group Type: IP Address IP Address: . . . Reference: When this VPN tunnel is connected, computers with the IP address of 192.168.2.1 can establish connection. **(2) Subnet** This option allows local computers in this subnet can be connected to the VPN tunnel.  Remote Security Group Type: Subnet IP Address: . . . Subnet Mask: 255 . 255 . 255 . 0 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.

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	☑
Phase2 DHGroup :	Group 1
Phase2 Encryption:	DES
Phase2 Authentication:	MD5
Phase2 SA Life Time:	0 seconds
Preshared Key:	

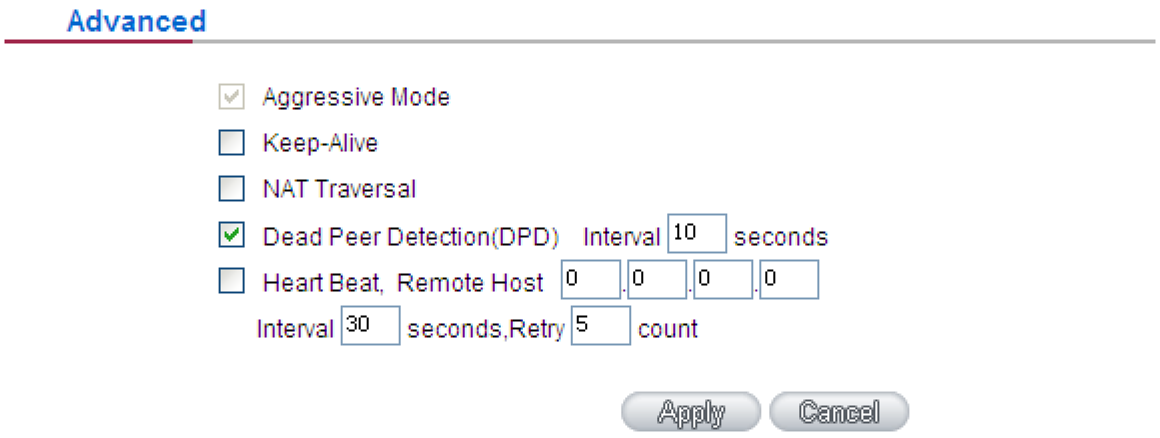
Use IKE Protocol

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
Perfect Forward Secrecy:	When users check the PFS option don't forget to activate the PFS function of the VPN device and the VPN Client as well.
Phase 1/ Phase 2 DH Group	This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
Phase 1/ Phase 2 Encryption	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.
Phase 1/Phase 2 Authentication	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".
Phase 1 SA Life Time	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.
Phase2 SA Life Time	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.
Preshared Key	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 10 seconds

□ Heart Beat, Remote Host 0 .0 .0 .0

Interval 30 seconds,Retry 5 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.

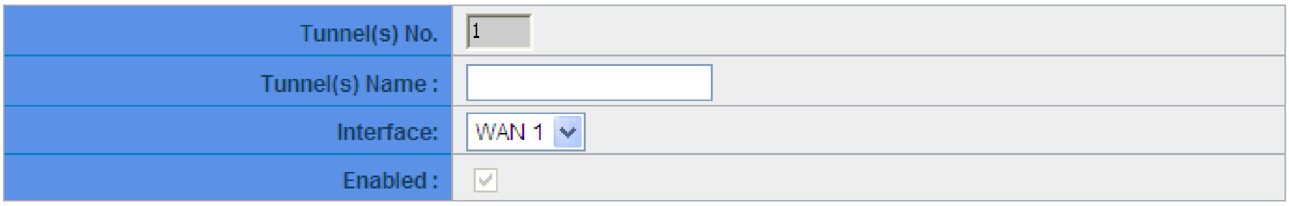
Item	Description
Aggressive Mode	This mode is mostly adopted by remote devices. The IP connection is designed to enhance the security control if dynamic IP is used for connection.
Keep Alive	If this option is selected, VPN tunnel will keep this VPN connection. This is mostly used to connect the remote node of the branch office and headquarter or used for the remote dynamic IP address.
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.
Heart Beat	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 (future feature)

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.	1
Tunnel(s) Name :	
Interface:	WAN 1
Enabled :	☑

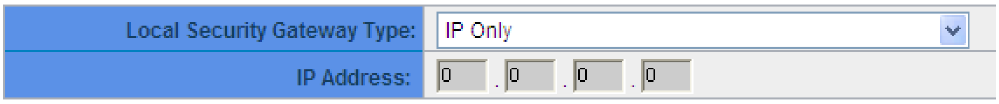
Item	Description
Tunnel No.	Set the embedded VPN feature, please select the Tunnel number.
Tunnel Name	Displays the current VPN tunnel connection name, such as XXX Office. Users are well-advised to give them different names to avoid confusion. **Note**: If this tunnel is to be connected to the other 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.
Interface	Users may select which port to be the node for this VPN channel. They can be applied for VPN connections.
Enabled	Click to **Enable** 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
Local Security Gateway Type:	This local gateway authentication type comes with five operation modes, which are: **IP only -** Authentication by the use of IP only **IP + Domain Name (FQDN) Authentication**, -IP + Domain name **IP + E-mail Addr. (USER FQDN) Authentication,**-IP + Email address **Dynamic IP + Domain Name (FQDN) Authentication,** -Dynamic IP address + Domain name **Dynamic IP + E-mail Addr. (USER FQDN) Authentication.** Dynamic IP address + Email address name **(1) IP only:** If users decide to use **IP only**, entering the IP address is the only way to gain access to

<table>
<tr>
<td></td>
<td>
this tunnel. The WAN IP address will be automatically filled into this space. Users don't need to do further settings.

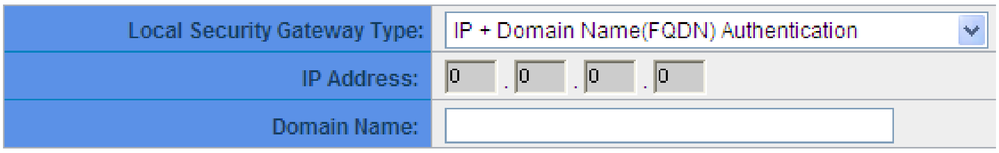


Local Security Gateway Type: IP Only

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.



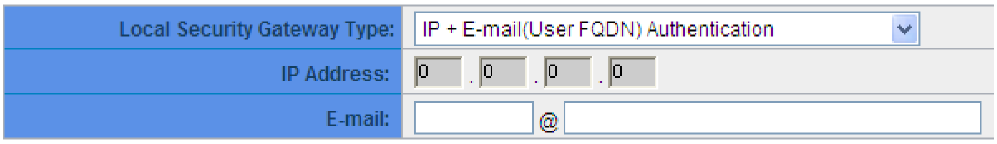
Local Security Gateway Type: IP + Domain Name(FQDN) Authentication

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.



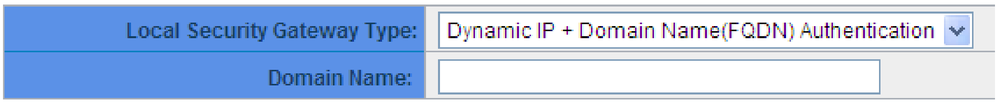
Local Security Gateway Type: IP + E-mail(User FQDN) Authentication

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.

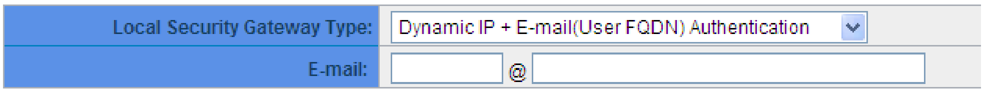


Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name:

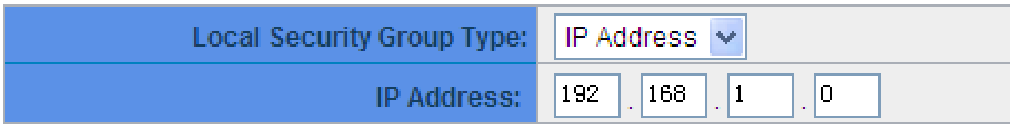
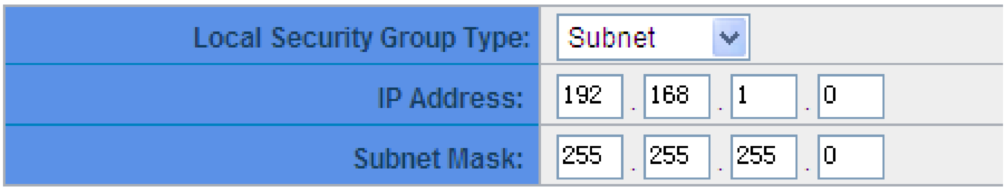
(5) Dynamic IP + E-mail Addr. (USER FQDN) Authentication.

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.

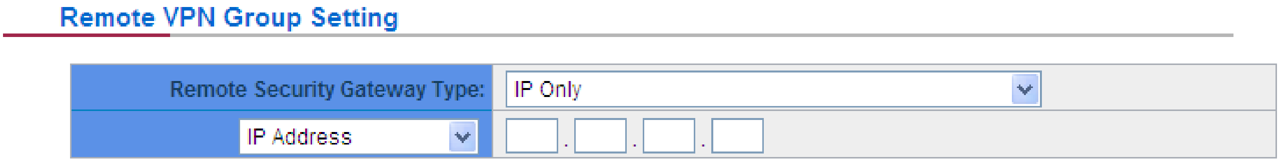


Local Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication

E-mail: @
</td>
</tr>
<tr>
<td><b>Local Security Group Type:</b></td>
<td>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:</td>
</tr>
</table>

	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

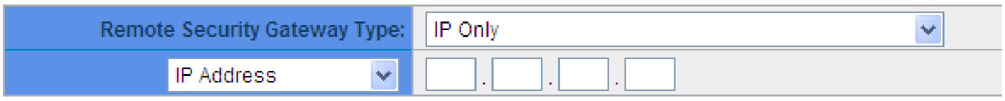
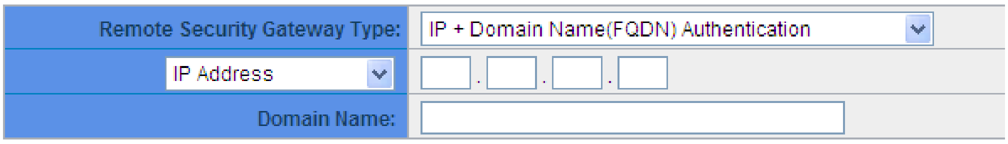
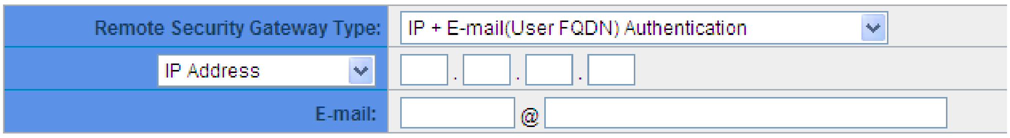


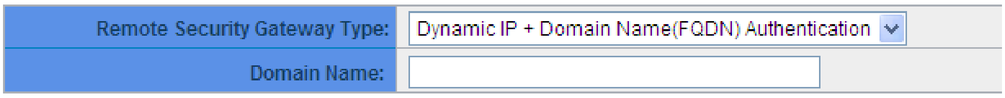
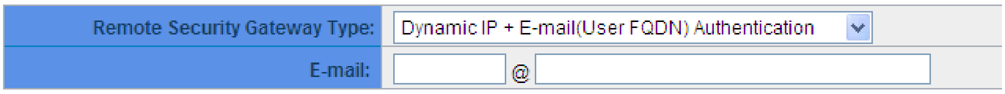
Remote VPN Group Setting

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
Remote Security Gateway Type:	This local gateway authentication type comes with five operation modes, which are: **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** **(1) IP only:** 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.  Remote Security Gateway Type: IP Only IP Address: . . . **(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.  Remote Security Gateway Type: IP + Domain Name(FQDN) Authentication IP Address: . . . 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.  Remote Security Gateway Type: IP + E-mail(User FQDN) Authentication IP Address: . . . 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

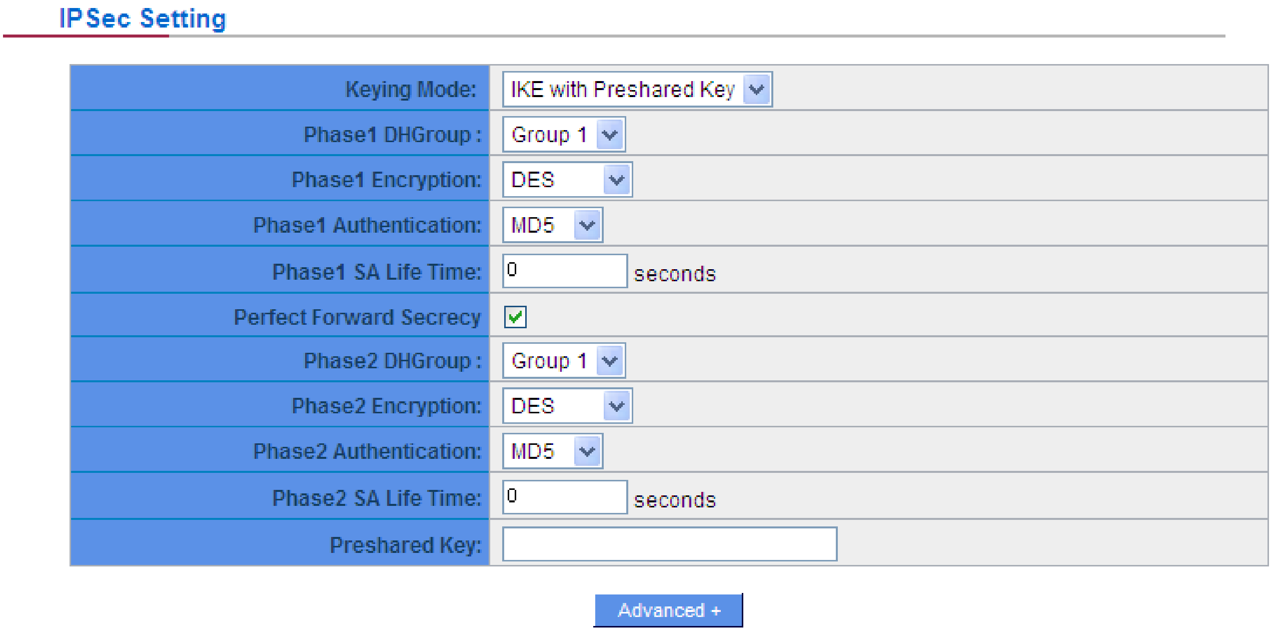
	connection, this device will start authentication and respond to this VPN tunnel connection; if users select this option to link to VPN, please enter the domain name.  Remote Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication Domain Name: **(5) Dynamic IP + E-mail Addr. (USER FQDN) 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.  Remote Security Gateway Type: Dynamic IP + E-mail(User FQDN) Authentication E-mail: @

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

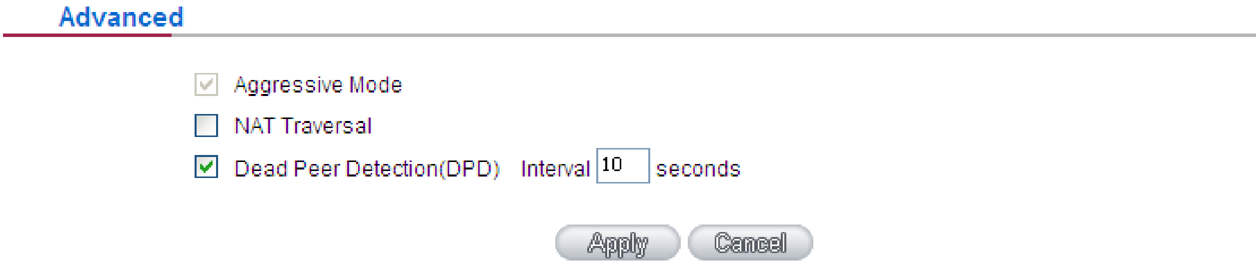
Keying Mode:	IKE with Preshared Key
Phase1 DHGroup :	Group 1
Phase1 Encryption:	DES
Phase1 Authentication:	MD5
Phase1 SA Life Time:	0 seconds
Perfect Forward Secrecy	☑
Phase2 DHGroup :	Group 1
Phase2 Encryption:	DES
Phase2 Authentication:	MD5
Phase2 SA Life Time:	0 seconds
Preshared Key:	

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
Perfect Forward Secrecy	When users check the PFS option, don't forget to activate the PFS function of the VPN device and the VPN Client as well.
Phase 1/ Phase 2 DH Group	This option allows users to select Diffie-Hellman groups: Group 1/ Group 2/ Group 5.
Phase 1/ Phase 2 Encryption	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.
Phase 1/Phase 2 Authentication	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".
Phase 1 SA Life Time	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.
Phase2 SA Life Time	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 Preshareed Key Only



☑ Aggressive Mode

□ NAT Traversal

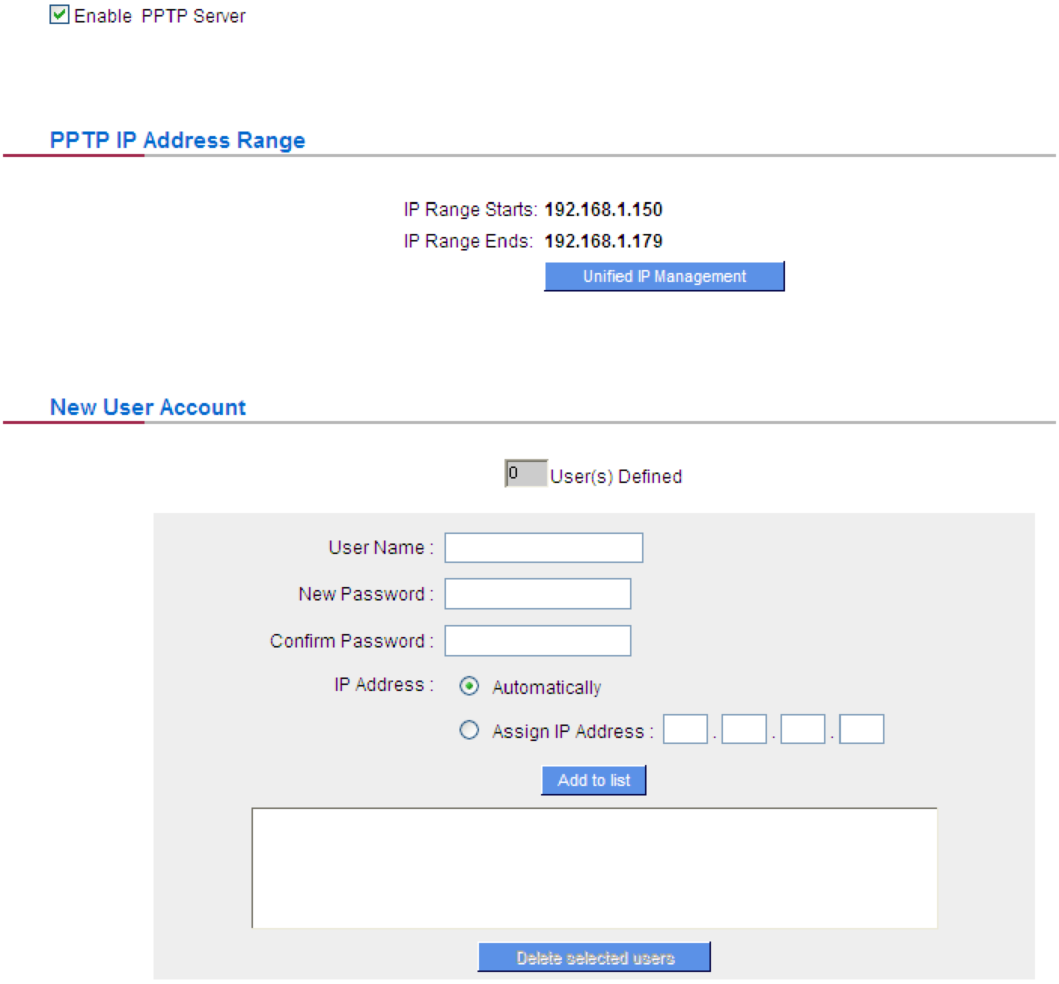
☑ Dead Peer Detection(DPD) Interval 10 seconds

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 Server

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

New User Account

0 User(s) Defined

User Name :

New Password :

Confirm Password :

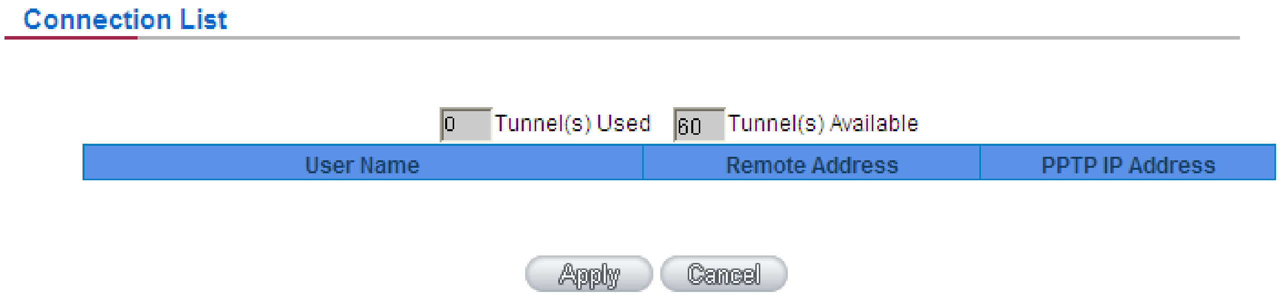
IP Address : ● Automatically

○ Assign IP Address : . . .

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

All PPTP Status

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

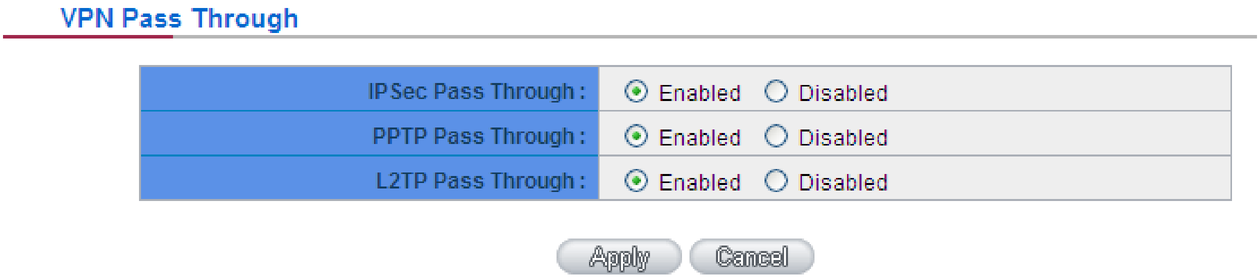


Connection List

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

User Name	Remote Address	PPTP IP Address

10.1.3. VPN Pass Through



VPN Pass Through

IPSec Pass Through :	● Enabled ○ Disabled
PPTP Pass Through :	● Enabled ○ Disabled
L2TP Pass Through :	● Enabled ○ Disabled

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

Through	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.

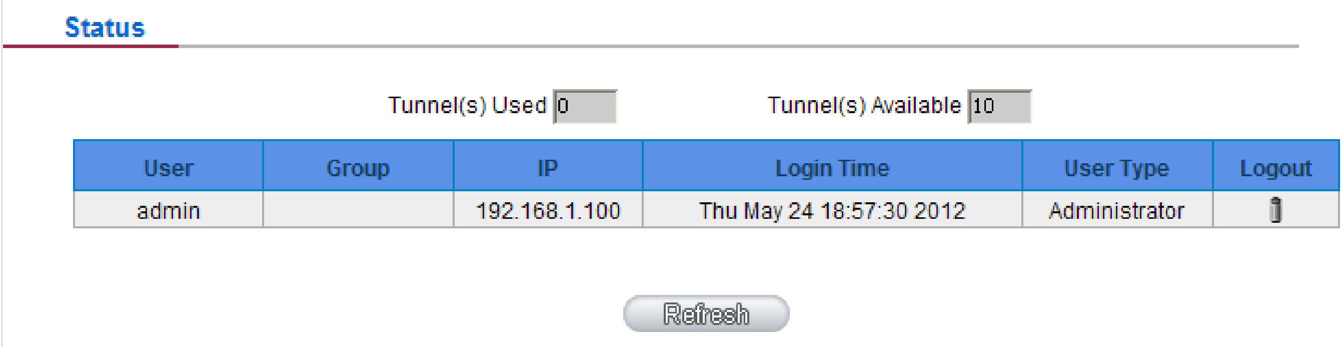
Chapter 11: SSL VPN

For SSL VPN, client only need a web browser to access to Central servers. Passing the ID, and you get the portal to the company's internal resources, such as Internet services, Microsoft terminal services, remote desktop services, online neighborhood networks, and secure tunnel functions. Meanwhile, different users or groups can access to different interfaces according to the web administrator's configurations, which satisfies external and mobile users' security requirements.

Below introduces SSL VPN related settings.SSL (Secure Sockets Layer) is a protocol that ensures secure data transmission over the Internet via HTTPS encryption; including server authentication, user authentication, and SSL data link integrity and security.

11.1 Status

Block Status shows current SSL VPN users' online status.



Status

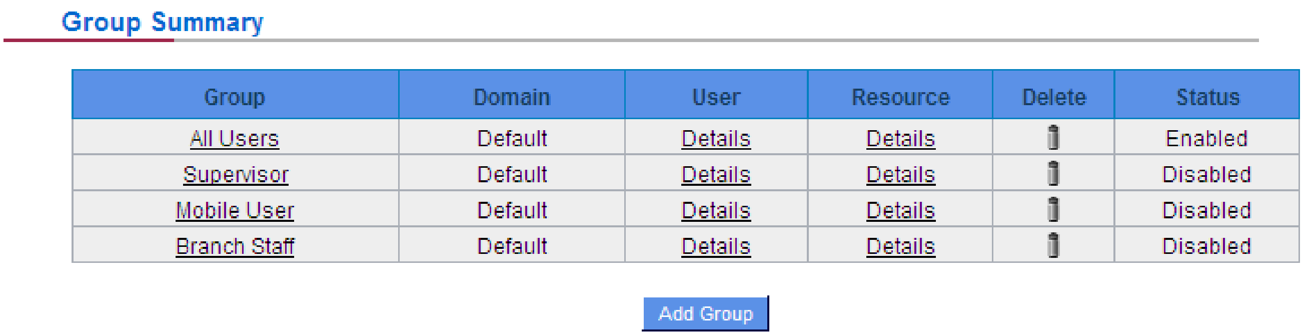
Tunnel(s) Used 0 Tunnel(s) Available 10

User	Group	IP	Login Time	User Type	Logout
admin		192.168.1.100	Thu May 24 18:57:30 2012	Administrator	🗑

Item	Description
Tunnel(s) Used	Display the amount of previously set tunnels.
Tunnel(s) Available	Display the amount of available tunnels.
User	Display the current SSL tunnel user name.
Group	Display the name of current SSL tunnel using Group.
IP	Display current users' SSL tunnel remote IP addresses.
Login Time	Display current SSL tunnel users' login time.
User Type	Display whether the user is an administrator or a staff.
Logout	Logout when clicking on the icon.

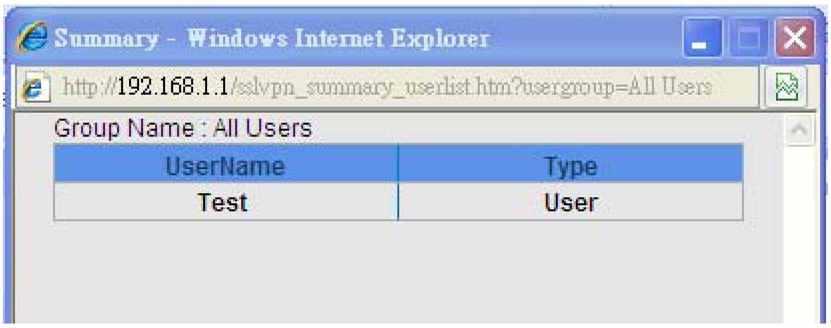
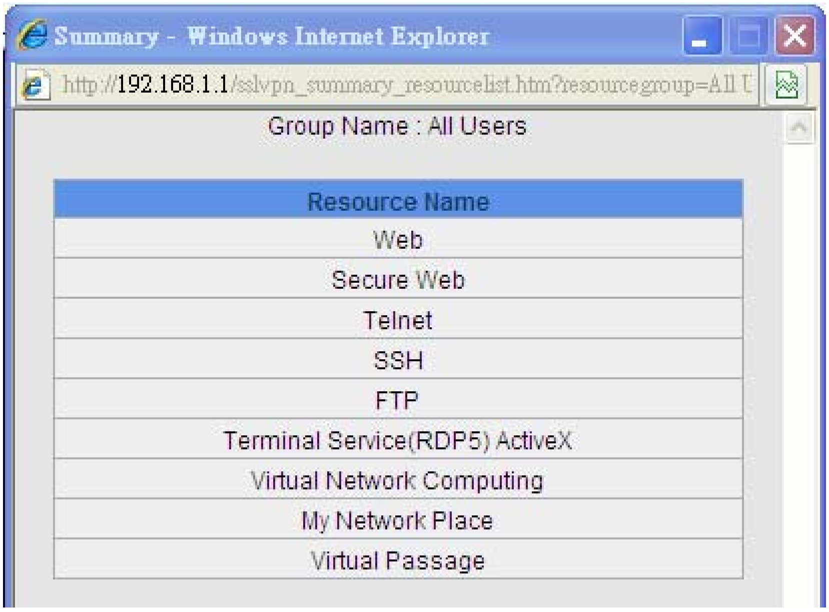
11.2 Group Summary

Group Summary table displays group setting information. Group settings can be modified here and new users can also be added.



Group Summary

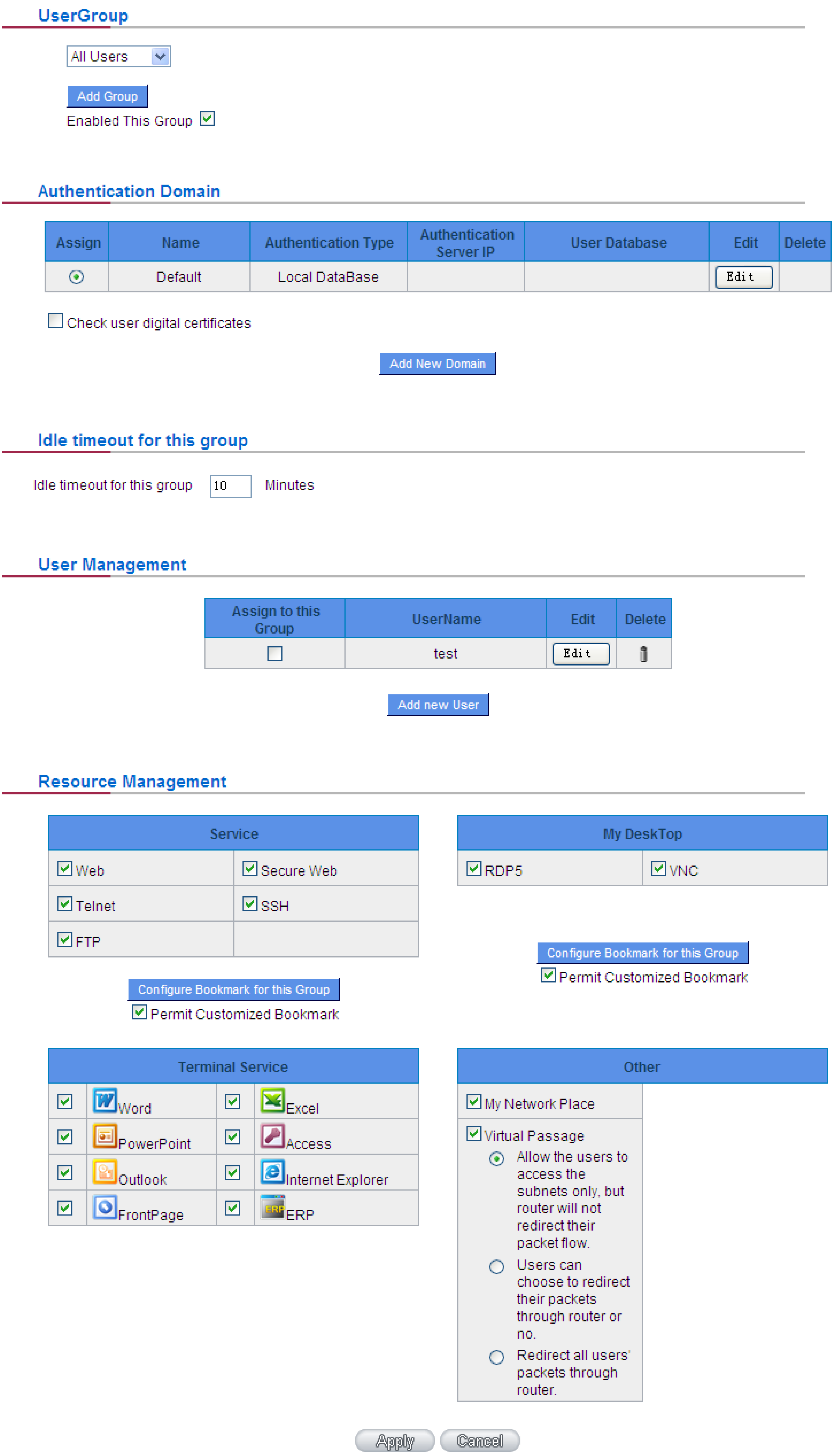
Group	Domain	User	Resource	Delete	Status
All Users	Default	Details	Details	🗑	Enabled
Supervisor	Default	Details	Details	🗑	Disabled
Mobile User	Default	Details	Details	🗑	Disabled
Branch Staff	Default	Details	Details	🗑	Disabled

Item	Description
Group	Display the group's name. SSL VPN has 4 built-in groups by default (All Users, Supervisor, Mobile User, & Branch Staff). If one group needs to be edited, click on its name to access the group management page.
Domain	Display the authentication server name used corresponding to certain group, which is served as Local Database by default.
User	Click "Detail" to view a specific group's user names and types.  http://192.168.1.1/sslvpn_summary_userlist.htm?usergroup=All Users Group Name : All Users UserName | Type Test | User
Resource	Click "Detail" to view a specific group's available service resources. The 4 default group's authentication service resources are all listed in the following service resource configuration explanation.  http://192.168.1.1/sslvpn_summary_resourcelist.htm?resourcegroup=All U Group Name : All Users Resource Name Web Secure Web Telnet SSH FTP Terminal Service(RDP5) ActiveX Virtual Network Computing My Network Place Virtual Passage

Delete	Click the recycle bin icon to delete a group.
Status	Display whether the group configuration is Enabled or Disabled. Defaults for the All Users group are Enabled and for others are Disabled.
Add Group	Click the "Add New Group" tab, entering the group admin section to add a new group.

11.3 Group Management:

Group Management helps the web administrator organize users' access to internal service resources in groups. It can be configured by following 3 steps: **Domain Management, User management, and Service Resource management**. In addition, SSL VPN's unique **"One- Click"** makes your basic configurations fast.



UserGroup

All Users

Add Group

Enabled This Group ☑

Authentication Domain

Assign	Name	Authentication Type	Authentication Server IP	User Database	Edit	Delete
●	Default	Local DataBase			Edit	

□ Check user digital certificates

Add New Domain

Idle timeout for this group

Idle timeout for this group 10 Minutes

User Management

Assign to this Group	UserName	Edit	Delete
□	test	Edit	

Add new User

Resource Management

Service	
☑ Web	☑ Secure Web
☑ Telnet	☑ SSH
☑ FTP	

Configure Bookmark for this Group

☑ Permit Customized Bookmark

My DeskTop	
☑ RDP5	☑ VNC

Configure Bookmark for this Group

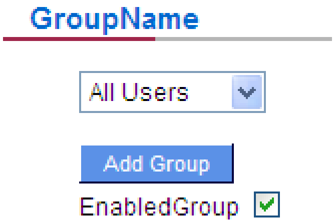
☑ Permit Customized Bookmark

Terminal Service			
☑	Word	☑	Excel
☑	PowerPoint	☑	Access
☑	Outlook	☑	Internet Explorer
☑	FrontPage	☑	ERP

Other
☑ My Network Place
☑ Virtual Passage ● Allow the users to access the subnets only, but router will not redirect their packet flow. ○ Users can choose to redirect their packets through router or no. ○ Redirect all users' packets through router.

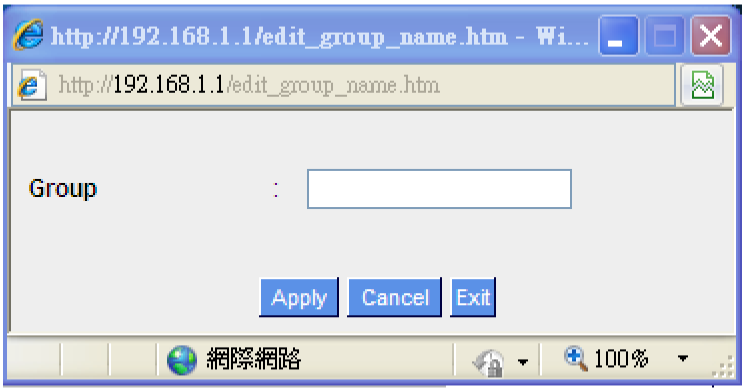
Apply Cancel

Group Name



Item	Description
Group Name	Display all group names in the drop down list. There are four group for default: **All Users, Supervisor, Mobile User, Branch Staff.**
Add Group	Click it to create a new group.

Add New Group :

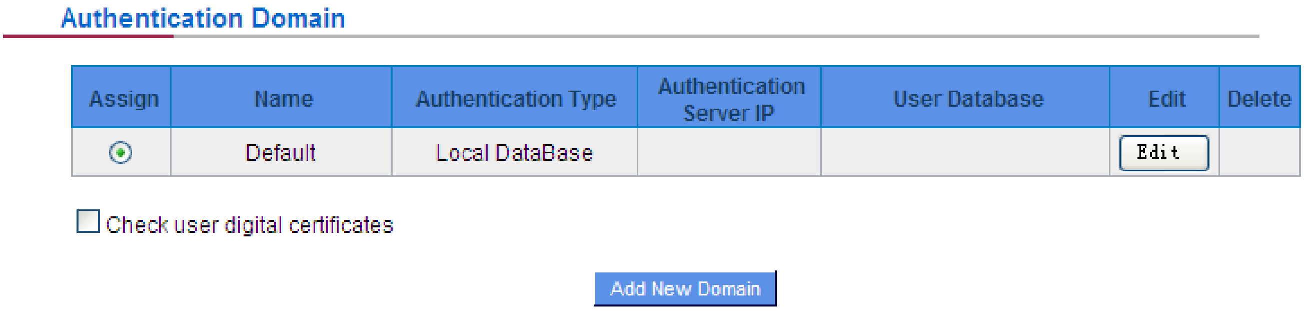

http://192.168.1.1/edit_group_name.htm - Wi...
http://192.168.1.1/edit_group_name.htm
Group :
Apply
Cancel
Exit
網際網路
100%

Item	Description
Group Name	Import a group name.
Apply	Click "**Apply**" tab to save recent changed settings; new group names will appear in the drop down menu.
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

Each group must follow below steps (Domain Management, User management, and Service resource management) to complete group settings.

Step 1: Domain Management

Domain Management is used to determine which authentication server will be used to authenticate users at login. The default authentication server type is local database. SSL VPN supports external authentication services and can be combined with an enterprise's current authentication server for a simplified deployment. If no suitable authentication servers can be chosen from the list, click "Add New Domain" to create a new one.

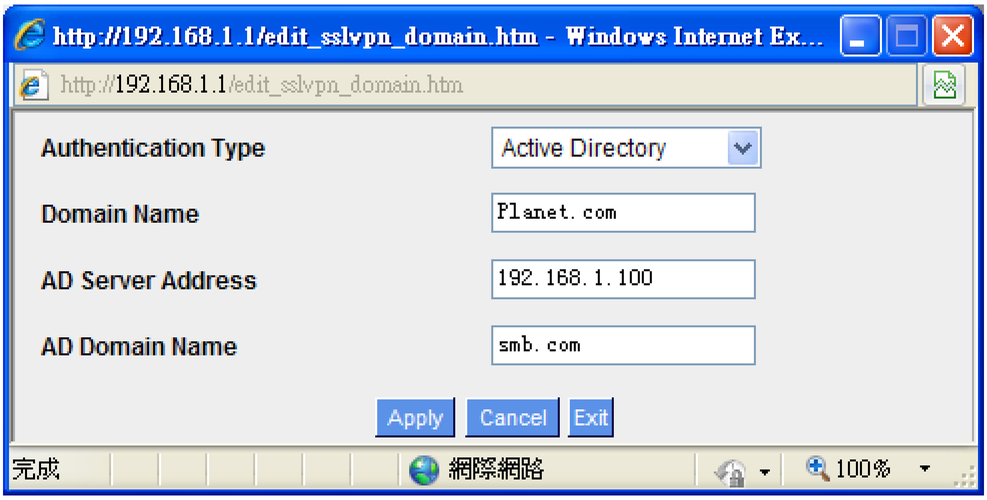


Authentication Domain

Assign	Name	Authentication Type	Authentication Server IP	User Database	Edit	Delete
●	Default	Local DataBase			Edit	

□ Check user digital certificates

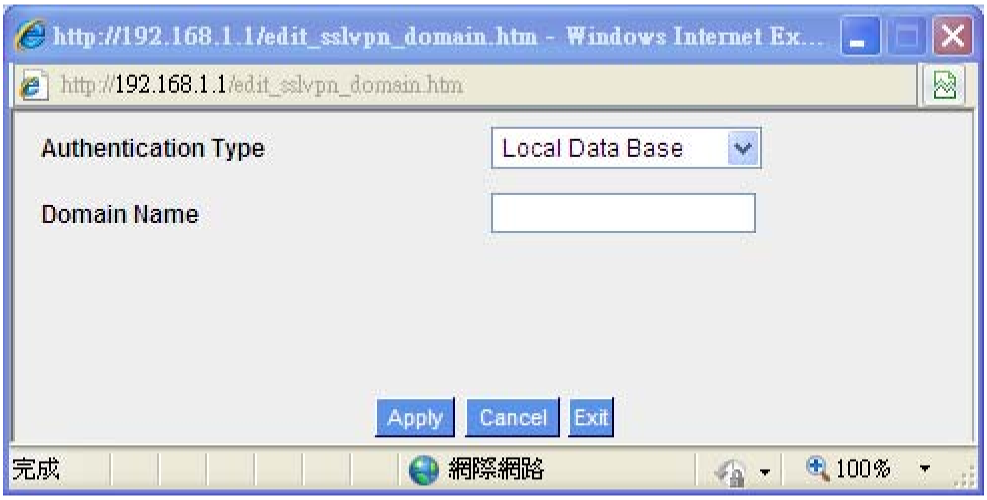
Item	Description
Assign	All authentication servers with defined settings will be displayed on Domain Management list. You are required to choose one authentication server to be assigned to this group. **Each group can only be assigned to one type of authentication server.** Default is Local Database. If there are changes to the domain servers designated by All Users, other groups that have yet to enable will also be modified accordingly.
Domain Names	Display all authentication server names.
Authentication Type	Display authentication server type.
Authentication server IP	Display external authentication server IP addresses. If the Authentication Type is Local Database, the authentication server IP address will not be displayed.
User Database	For external authentication servers, the user database will be: "Apply User Database" and "Customize User Database". Click "**Apply User database**", then there is no need to establish additional user data, and the system will directly apply the external authentication server's internal user database settings. As long as the users belong to this authentication server group, they can use the group's resources. **Note:** If multiple groups designate the same authentication server for users, only one group will be able to use the built-in user database at one time. For this reason, it is recommended that the largest group be designated to use the built-in user database and other smaller groups use the "Customize User Database". Select the "**Customize User Database**", the administrator must add a new user to the group (See step two: User management). If users have not been set by the administrator, users of the authentication server can still pass the authentication, but they will not be able to access the web portal to use internal enterprise resources.
Edit	Click on the "Edit" tab to make changes to the server addresses and authentication domain names. Authentication server type and authentication service name cannot be altered. If you want to change the authentication server type and authentication service name, delete them, and then set up a new authentication server.

	 http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex... Authentication Type: Active Directory Domain Name: Planet.com AD Server Address: 192.168.1.100 AD Domain Name: smb.com
Delete	Click on the recycle bin icon to delete authentication server settings.

Adding New Authentication Service :

SSL VPN, in addition to Local Database, supports another 7 kinds of authentication server types: **Radius-PAP / CHAP/MSCHAP / MSCHSPV2, NT-Domain, Active Directory, and LDAP.**

1. Local Database



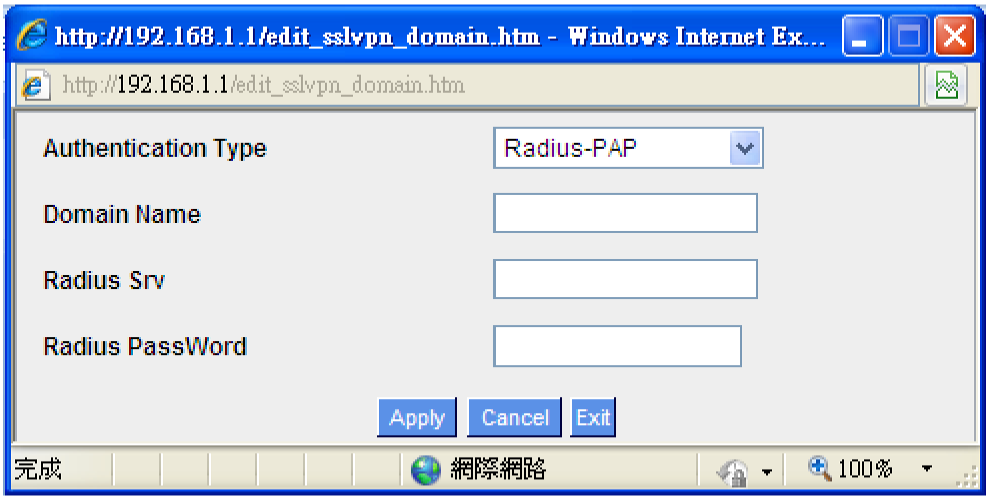
http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...

Authentication Type: Local Data Base

Domain Name:

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Names	Name the selected authentication server.
Apply	Click on the "**Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

2. Radius-PAP



http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...
http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type: Radius-PAP

Domain Name

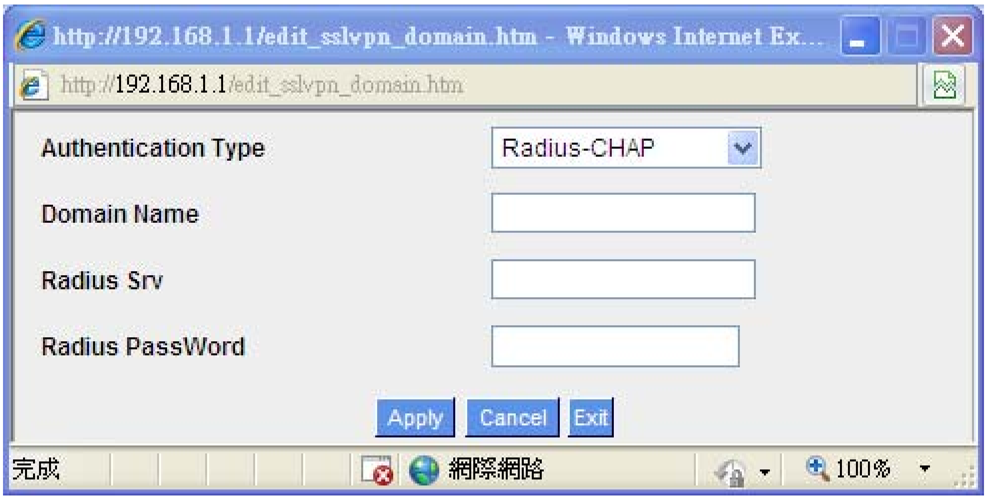
Radius Srv

Radius PassWord

Apply
Cancel
Exit
完成
網際網路
100%

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Names	Name the selected authentication server.
RADIUS Srv	Enter authentication server address.
Radius Password	Enter the password for RADIUS.
Apply	Click on the "**Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

3. Radius-CHAP



http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...
http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type: Radius-CHAP

Domain Name

Radius Srv

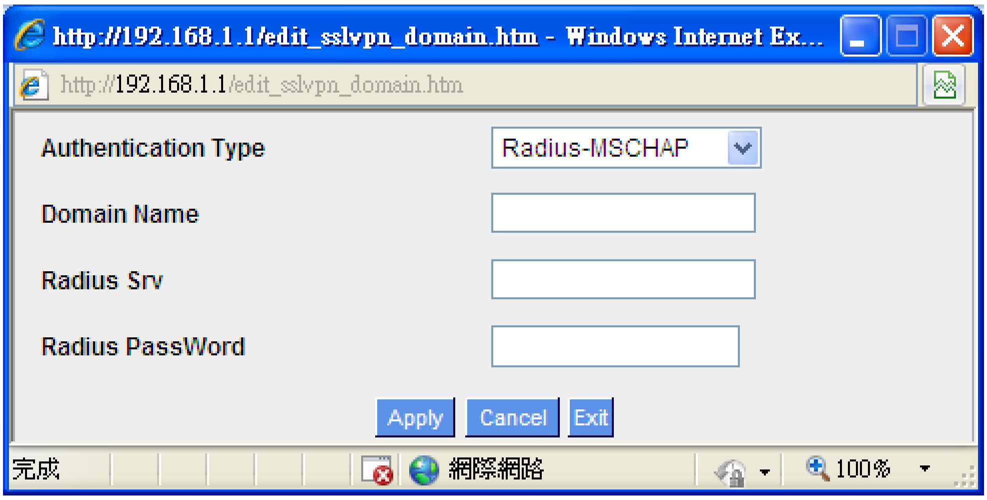
Radius PassWord

Apply
Cancel
Exit
完成
網際網路
100%

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.

Domain Name	Name the selected authentication server.
RADIUS Srv	Enter authentication server address.
Radius Password	Enter the password for RADIUS.
Apply	Click on the " **Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

4. Radius-MSCHAP



http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...

http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type: Radius-MSCHAP

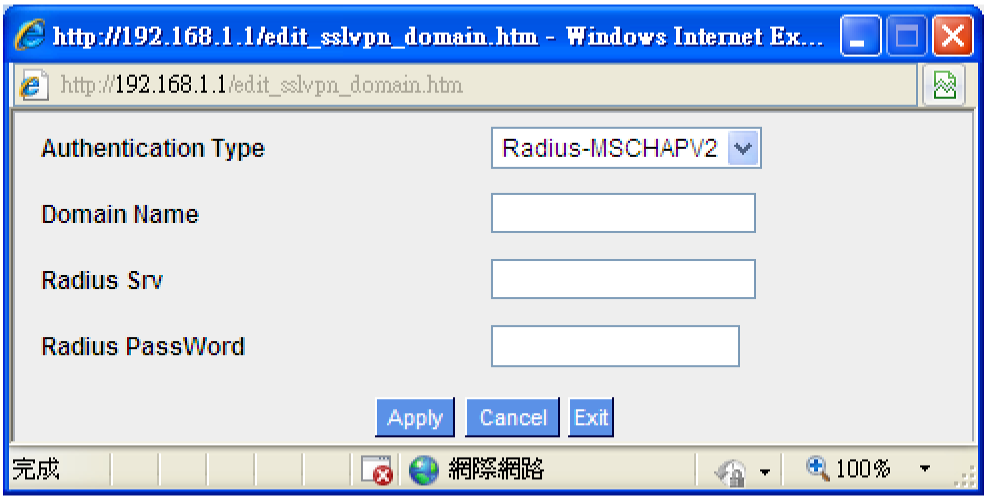
Domain Name:

Radius Srv:

Radius PassWord:

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Names	Name the selected authentication server.
RADIUS Srv	Enter authentication server address.
Radius Password	Enter the password for RADIUS.
Apply	Click on the " **Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

5. Radius-MSCHAPV2



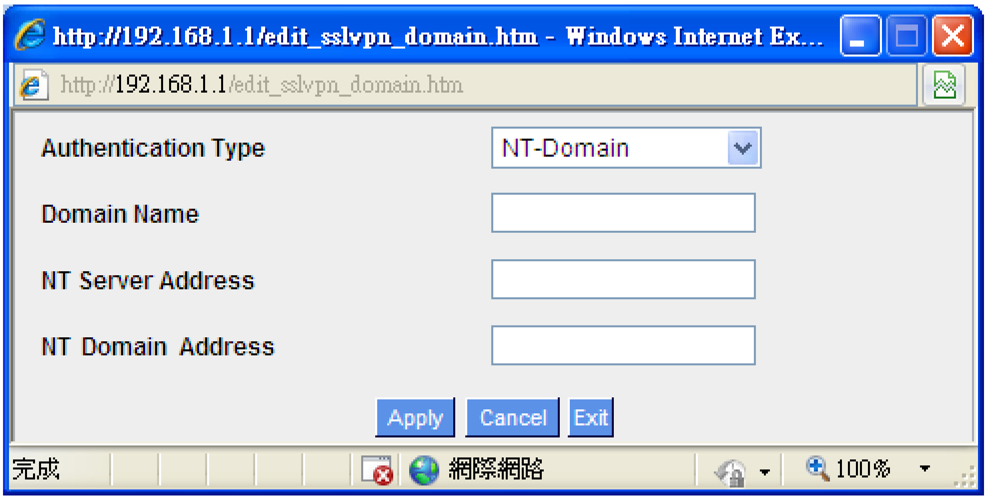
http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...

http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type	Radius-MSCHAPV2
Domain Name	
Radius Srv	
Radius PassWord	

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Names	Name the selected authentication server.
RADIUS Srv	Enter authentication server address.
Radius Password	Enter the password for RADIUS.
Apply	Click on the " **Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

6. NT-Domain



http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...

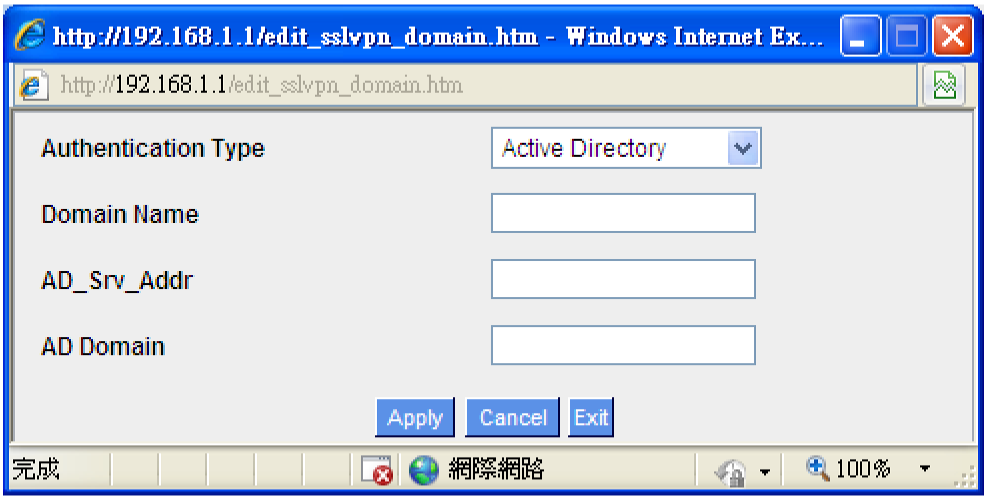
http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type	NT-Domain
Domain Name	
NT Server Address	
NT Domain Address	

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Names	Name the selected authentication server.

NT Server Address	Enter the NT-Domain authentication server address.
NT Domain Name	Enter NT-Domain authentication domain name. For example, planet.com.
Apply	Click on the " **Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

7. Active Directory


http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...
http://192.168.1.1/edit_sslvpn_domain.htm
Apply
Cancel
Exit
完成
網際網路
100%

Authentication Type: Active Directory

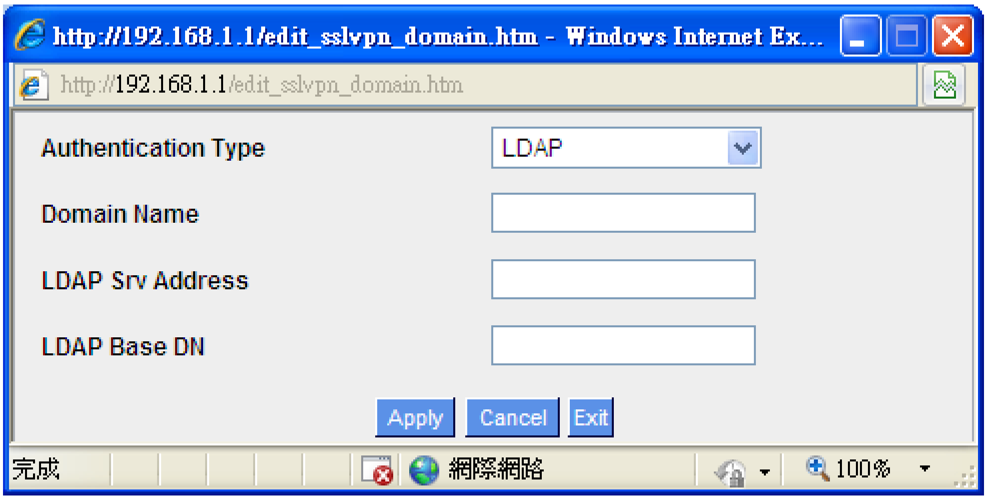
Domain Name

AD_Srv_Addr

AD Domain

Item	Description
Authentication Type	Select the authentication server type from the drop down menu.
Domain Name	Name the selected authentication server.
AD_Srv_Add	Enter Active Directory authentication server address.
AD Domain	Enter Active Directory authentication server's domain name. For example, planet.com
Apply	Click on the "**Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

8. LDAP



http://192.168.1.1/edit_sslvpn_domain.htm - Windows Internet Ex...

http://192.168.1.1/edit_sslvpn_domain.htm

Authentication Type: LDAP

Domain Name

LDAP Srv Address

LDAP Base DN

Item	Description
Authentication Type	Select the authentication service type you wish to use from the drop down menu.
Domain Names	Name the selected authentication server.
LDAP Srv Address	Enter authentication server address.
LDAP Base DN	Enter LDAP authentication server's authentication domain name (LDAP BaseDN*).
Apply	Click on the "**Apply**" tab to save changes
Cancel	Click "**Cancel**" to clear any recent changes to the settings.

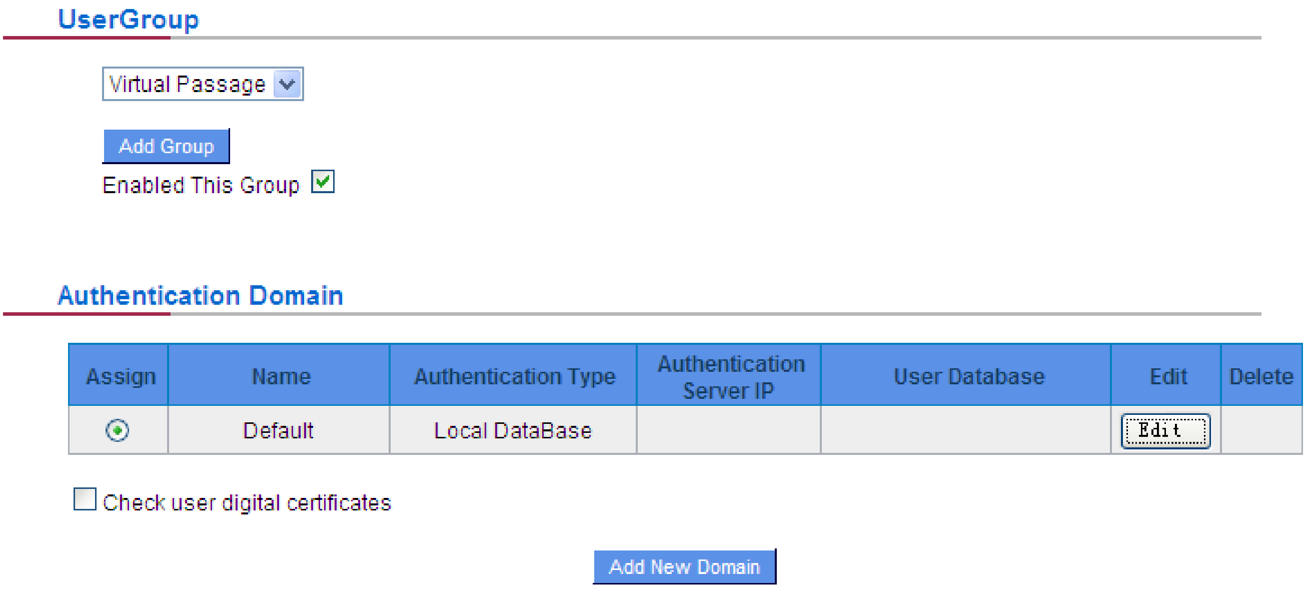
One Click

SSL VPN provides one-click setting. With fewest configurations, all users can use SSL tunnels to access an open internal resource. While in "All Users" group, the authentication server settings support the current enterprise authentication server. So all users, after being identified via the authentication server, will be directed to the portal and can use the full range of enterprise resources. For Authentication server settings, see step one below: Domain Management.

If you don't want all users to access the full range of available resources, go to "All Users" group settings to disable or modify settings in sequential order according to the following steps.

If you want to use the one-click function, after you have added new authentication servers, complete the setup by assigning the All Users group authentication server to the newly created authentication server.

Note: All of the users in this authentication server can link to the web portal and access all of the enterprise resources pre-determined by administrators. Administrators do not need to define settings for step 2 (User management) and step 3 (Service resources management).



UserGroup

Virtual Passage

Enabled This Group ☑

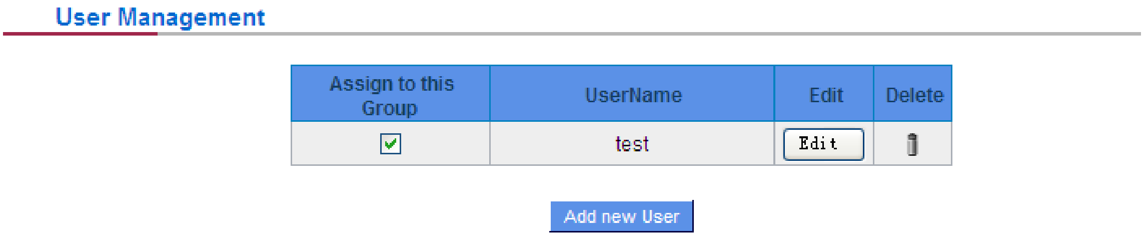
Authentication Domain

Assign	Name	Authentication Type	Authentication Server IP	User Database	Edit	Delete
●	Default	Local DataBase			Edit	

□ Check user digital certificates

Step 2: User Management

User Management determines who belong to this group and have the right to use the resources. Newly added users will appear on the user list; click on "Assign to this Group" column to designate a user to this group. If "Domain Management" is set to "Customize User Database" and when the user list does not have a suitable user, click "Add New User" to create a new one.



User Management

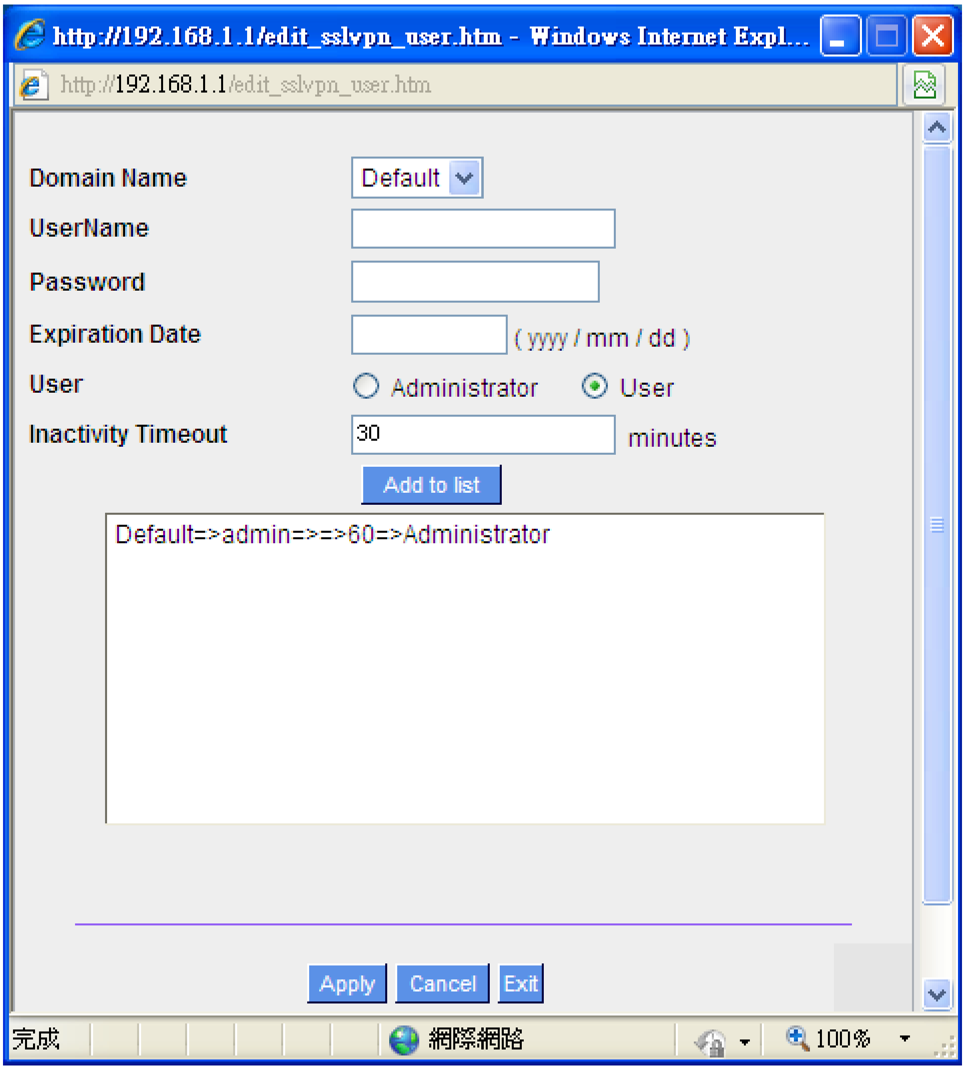
Assign to this Group	UserName	Edit	Delete
☑	test	Edit	🗑

Item	Description
Assign to this Group	Select a user from the user list to assign to this group. One user can be assigned to one group only.
User Name	Display customized user name. Please note: The built- in users of the authentication server database in Domain Management will not display on the user list.
Edit	User passwords (if Local Database), expiration dates, user classifications, and inactive timeouts can be edited or modified, but user authentication servers and user names cannot. If you want to modify a user name, first delete it, and then add a new modified user name.
Delete	Delete this user.

Add New User

Click on "Add new user" and the window below will pop up.

Please note: In addition to Local Database, user names and passwords must correspond to the selected authentication server's user names.


http://192.168.1.1/edit_sslvpn_user.htm - Windows Internet Expl...
http://192.168.1.1/edit_sslvpn_user.htm
Add to list
Apply
Cancel
Exit
完成
網際網路
100%

Domain Name: Default
UserName:
Password:
Expiration Date: (yyyy / mm / dd)
User: ○ Administrator ● User
Inactivity Timeout: 30 minutes

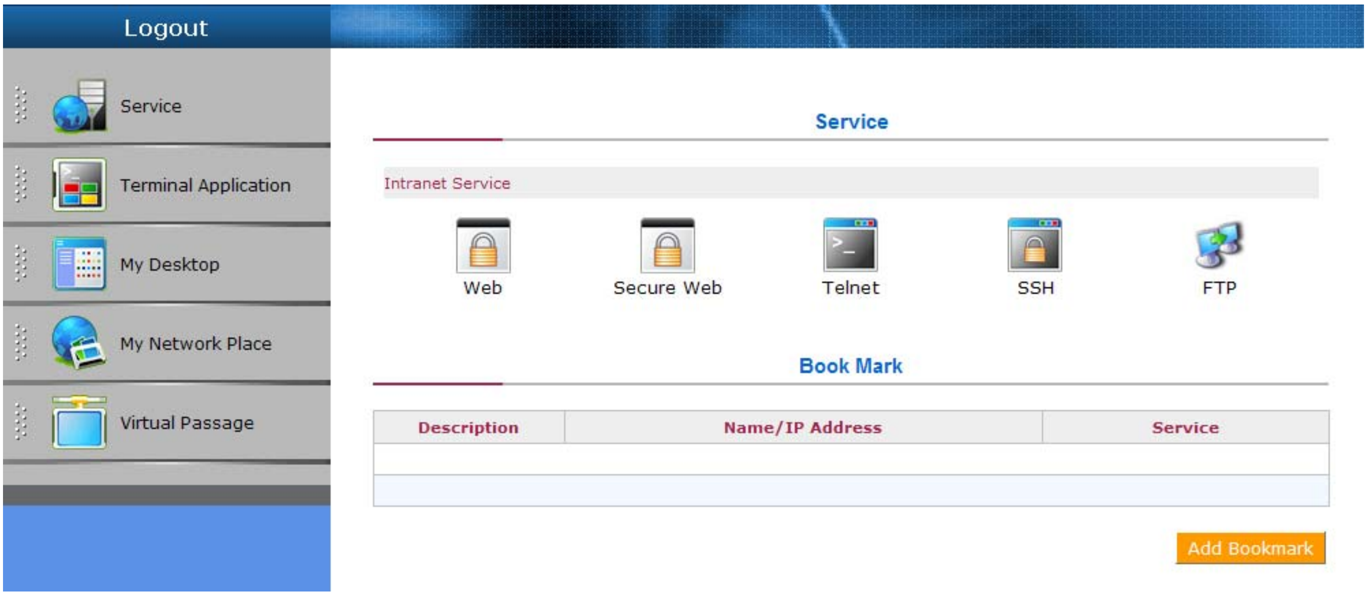
Default=>admin=>=>60=>Administrator

Item	Description
Domain Name	Display the authentication server name used by this group.
User Name	Enter authentication server's user name.
Password	For Local Database, enter user passwords. Passwords do not need to be entered if Local Database is not used.
Expiration Date (yyyy/mm/dd)	Enter users' permitted time limit. For example, if the expiration date is set to November 1, 2007, then the user will be denied beginning on November 2, 2007 at 12: 00 AM.
User Type	If set to "Administrator", the user will login on the router management UI. If set to "U user", the user will login on the web portal. Please note: Only Local Database users can be set as "Administrator"; external authentication server users can only be "Users" and cannot login on the router

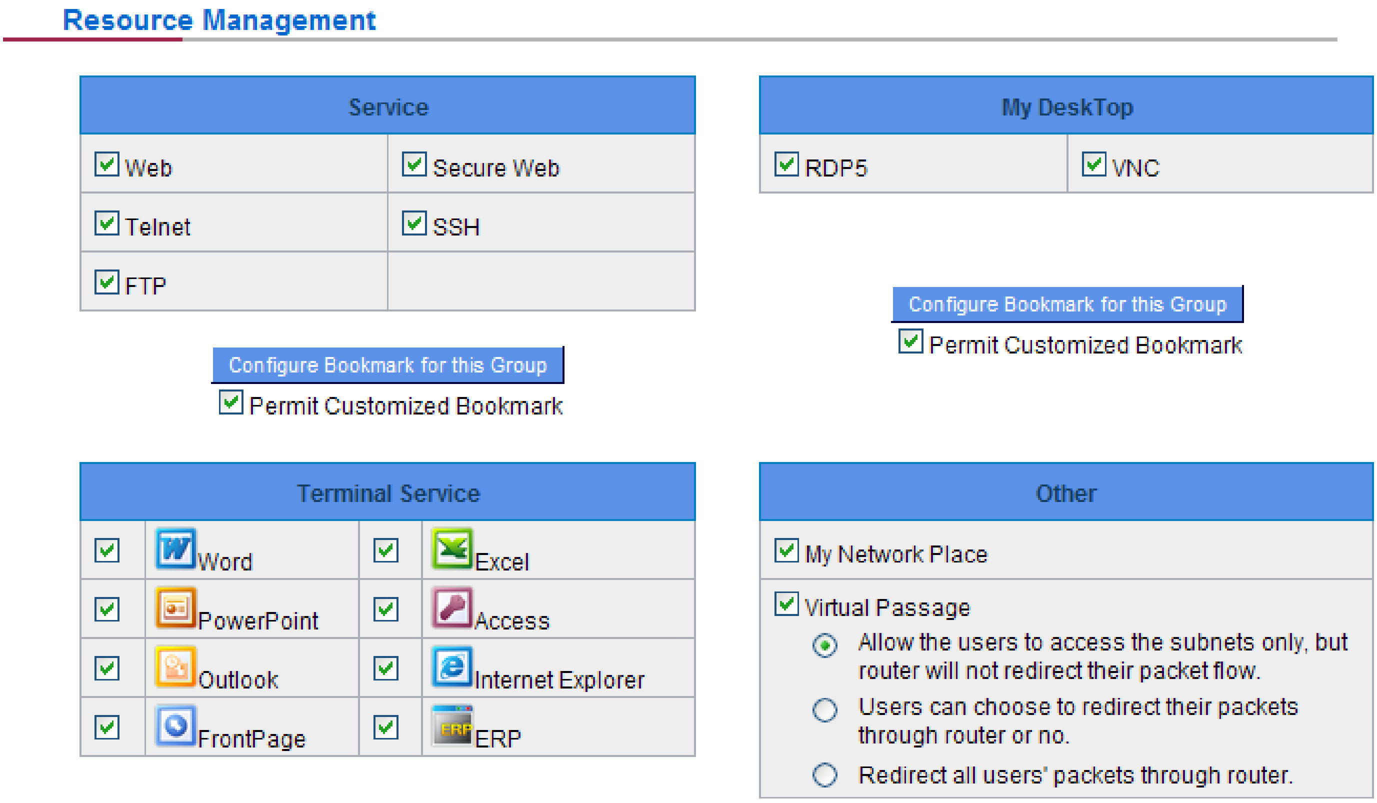
	management UI.
Inactivity timeout	Even though a user has logged in via the web portal, he/she will be forced to logout (timeout) due to inactivity after 10 minutes. If a user logs into the web portal to access enterprise resources using a SSL in an unsafe environment, a shorter timeout time is recommended to mitigate risk if the user is logged in but inactive.
Add to List	After completing the above settings, click on "add to list" to add newly created user settings to the corresponding list.
Apply	After complete settings, click on the “**Apply**” tab to save.
Cancel	Click on the “**Cancel**” tab to cancel all unsaved settings.
Exit	Click on the “**Exit**” tab to close the “add new user” window.

Step 3: Service Resource Management:

Service resource management settings determine which enterprise resources a group's users can use. The checked resources will be the icons which are available to the users after they have logged on to the web portal. If users are not allowed to enter resource addresses or names, administrators can opt to not activate that resource and bookmark the limits of users' access to resources. For example, if a company has multiple FTP servers internally, and when FTP service is activated, then a group's users can connect through the web portal and enter the FTP servers if they want to access. If an administrator has not activated FTP service, but has only bookmarked one FTP, then the group's users can only access the bookmarked FTP server.



Description	Name/IP Address	Service



Resource Management

Service	
☑ Web	☑ Secure Web
☑ Telnet	☑ SSH
☑ FTP	

Configure Bookmark for this Group

☑ Permit Customized Bookmark

My DeskTop	
☑ RDP5	☑ VNC

Configure Bookmark for this Group

☑ Permit Customized Bookmark

Terminal Service			
☑	Word	☑	Excel
☑	PowerPoint	☑	Access
☑	Outlook	☑	Internet Explorer
☑	FrontPage	☑	ERP

Other

☑ My Network Place

☑ Virtual Passage

- ● Allow the users to access the subnets only, but router will not redirect their packet flow.
- ○ Users can choose to redirect their packets through router or no.
- ○ Redirect all users' packets through router.

Default values for each built-in user groups are shown in the following table.

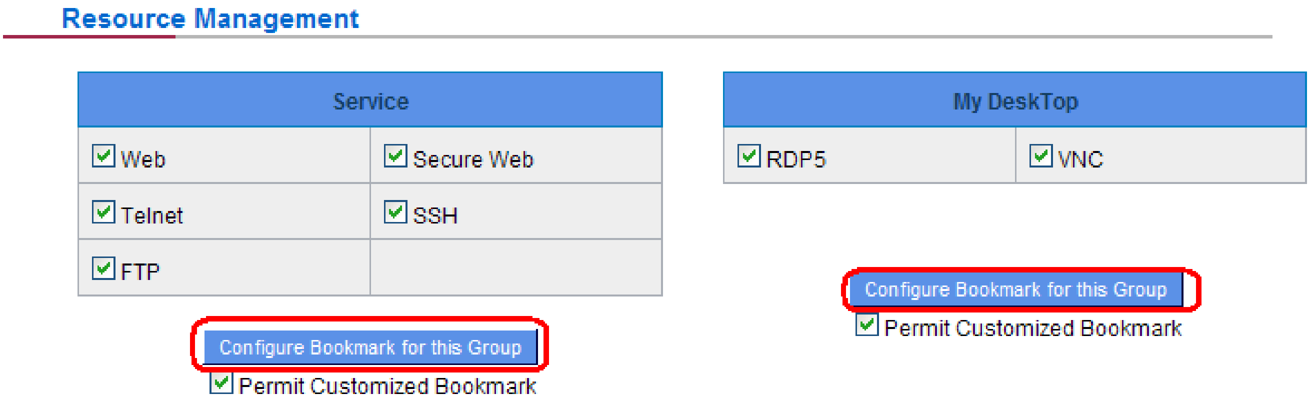
Group name	**All Users**	**Supervisor**	**Mobile User**	**Branch Staff**
Resource name				
Internet Services				
Telnet	✓			
SSH	✓			
FTP	✓	✓	✓	✓
Microsoft Terminal Services				
Word	✓	✓	✓	
Excel	✓	✓	✓	
Power Point	✓	✓	✓	
Access	✓	✓	✓	
Outlook	✓	✓	✓	
IE	✓			
FrontPage	✓			
ERP	✓	✓	✓	✓
Remote Desktop				
RDP5	✓		✓	
VNC	✓			
My Network Place	✓	✓		

Virtual Passage	✓	✓		

Configure Bookmark for this Group

Services (Telnet, SSH, FTP) and remote desktop services (RDP5, VNC) can use group established bookmarks. Users are not required to remember or set a server name or IP address.

Administrators can see all configured bookmarks here, which will display on a user web portal. Users are not required to remember or set a server name or IP address; they can click to use the administrator pre-configured resources.



Resource Management

Service	
☑ Web	☑ Secure Web
☑ Telnet	☑ SSH
☑ FTP	

Configure Bookmark for this Group

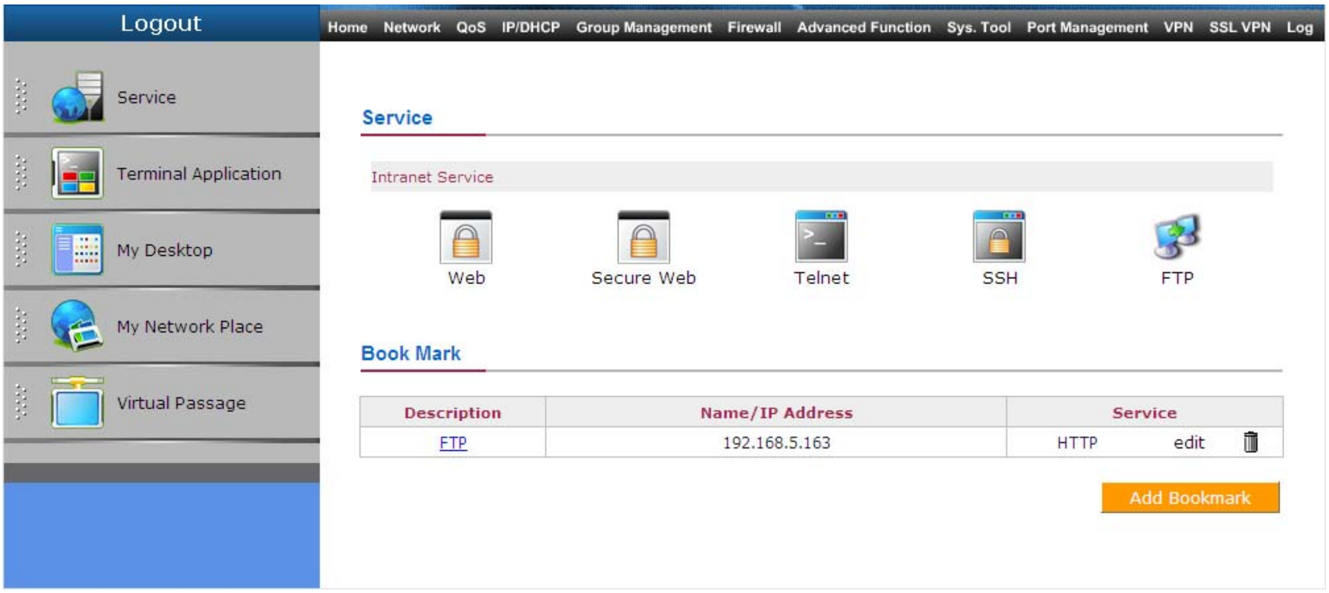
☑ Permit Customized Bookmark

My DeskTop	
☑ RDP5	☑ VNC

Configure Bookmark for this Group

☑ Permit Customized Bookmark

Administrators can see all configured bookmarks here, which will display on a user web portal. Users are not required to remember or set a server name or IP address; they can click to use the administrator pre-configured resources.


Logout
Home Network QoS IP/DHCP Group Management Firewall Advanced Function Sys. Tool Port Management VPN SSL VPN Log
Service
Terminal Application
My Desktop
My Network Place
Virtual Passage

Service

Intranet Service

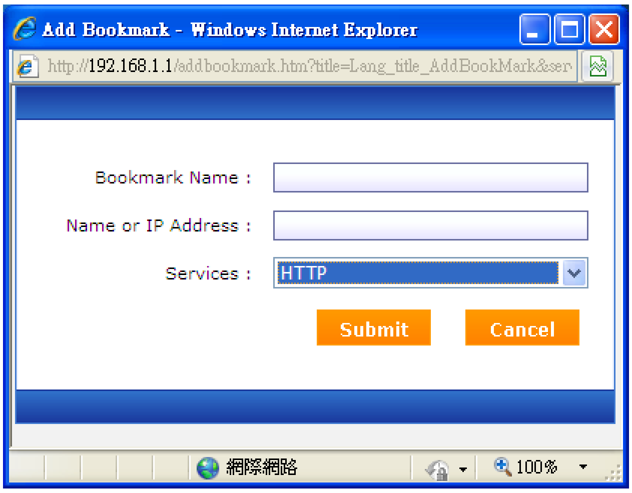
Web
Secure Web
Telnet
SSH
FTP

Book Mark

Description	Name/IP Address	Service	
FTP	192.168.5.163	HTTP	edit

Add Bookmark

Bookmark configured for this group



Add Bookmark - Windows Internet Explorer

http://192.168.1.1/addbookmark.htm?title=Lang_title_AddBookMark&ser

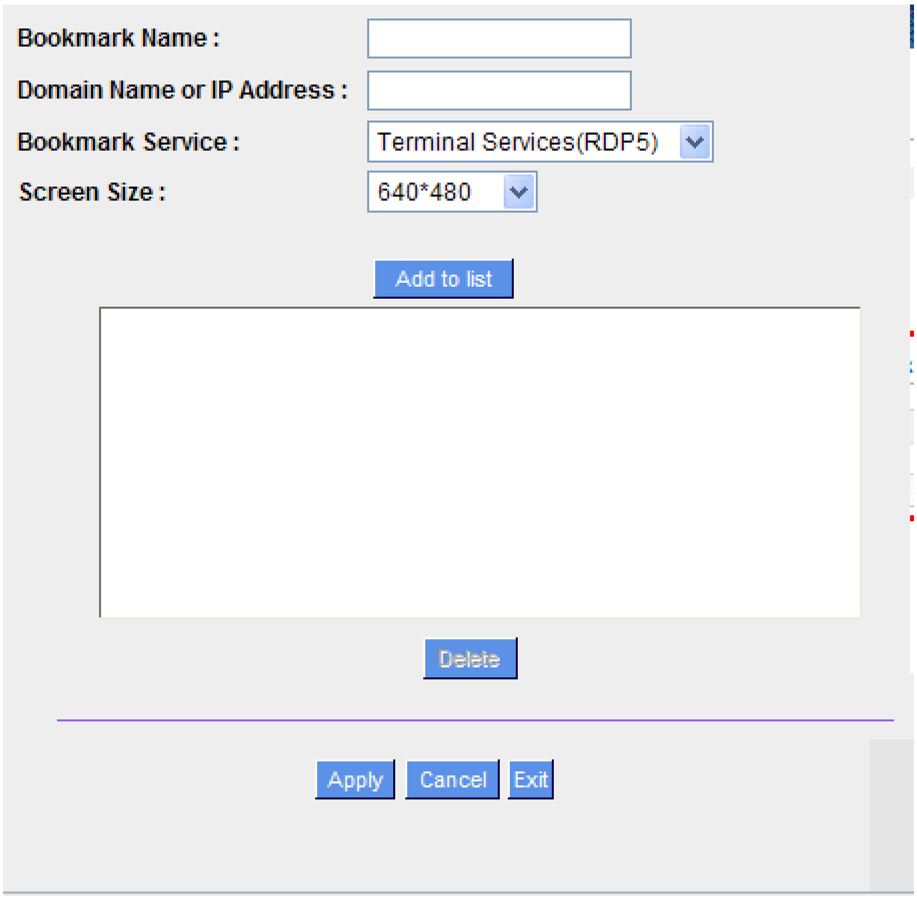
Bookmark Name :

Name or IP Address :

Services : HTTP

Item	Description
Bookmark Name	Enter the service resource name; this name will appear on the user's web portal as the service name.
Name or IP address	Enter the service name or IP address.
Service	Select a service from the drop down menu below, for example: Telnet/SSH/FTP.
Apply	After completing the previous steps, click on the "Add to List" tab to add the bookmark setting into the list.
Cancel	Click on the "**Cancel**" tab to cancel all unsaved settings.

Bookmark configured for this group: Remote desktop service



Bookmark Name :

Domain Name or IP Address :

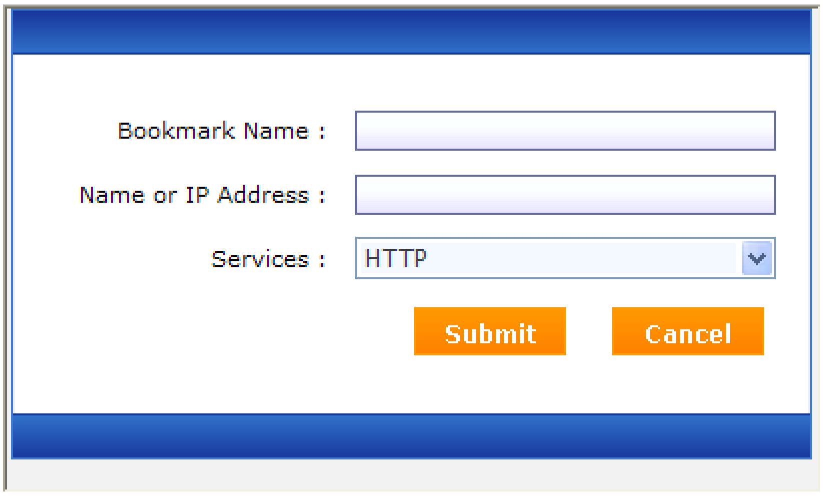
Bookmark Service : Terminal Services(RDP5)

Screen Size : 640*480

Item	Description
Bookmark Name	Enter the service resource name; this name will appear on the user's web portal as the service name.
Name or IP address	Enter the service name or IP address.
Service	Select remote desktop service RDP5/VNC from the drop down menu.
Screen Size	Configure user remote desktop screen display dimensions: 680x480, 800x600, 1027x768 or full-screen
Add to List	After completing the previous steps, click on the "Add to List" tab to add the bookmark setting into the list.
Apply	After complete settings, click on the "**Apply**" tab to save.
Cancel	Click on the "**Cancel**" tab to cancel all unsaved settings.
Exit	Click on the "**Exit**" tab to close the window.

Permit Customized Bookmarks

If an administrator activates "Permit Customized Bookmarks", then users should click "Add Bookmark" to configure a service name or IP address to use that resource.



Bookmark Name :

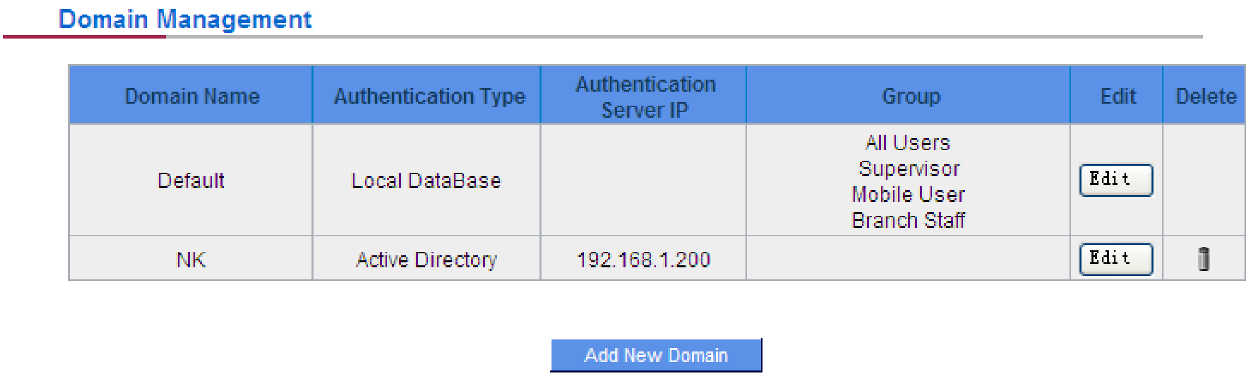
Name or IP Address :

Services : HTTP

11.4 Domain Management

In addition to selecting 8.3 "Group Management", SSL VPN can also provide authentication to display Domain Management. All authentication services will be shown in the Domain Management list. Groups using authentication services will be displayed according to the authentication server name.

Group / Step	All User Group	Supervisor Group	Mobile User	Branch Staff Group
Step 1: **Domain Management**				
Step 2: **User Management**				
Step 3: **Service Resource Management:**				



Domain Management

Domain Name	Authentication Type	Authentication Server IP	Group	Edit	Delete
Default	Local DataBase		All Users Supervisor Mobile User Branch Staff	Edit	
NK	Active Directory	192.168.1.200		Edit	🗑

Item	Description
Domain Name	All newly added authentication services will be displayed on the Domain Management list.

Authentication Type	Authentication service types are displayed by authentication server name, including: Local Database, Radius- PAP/ CHAP/ MSCHAP/ MSCHAPV2, NT-Domain, Active Directory and LDAP.
Authentication Server IP	Display configured external authentication server IP addresses.
Group	Display authentication server group names.
Edit	Click on the "**Edit**" tab to select an authentication server IP address and edit authentication domain names.
Delete	Click on the "clear" tab to clear the selected authentication server.

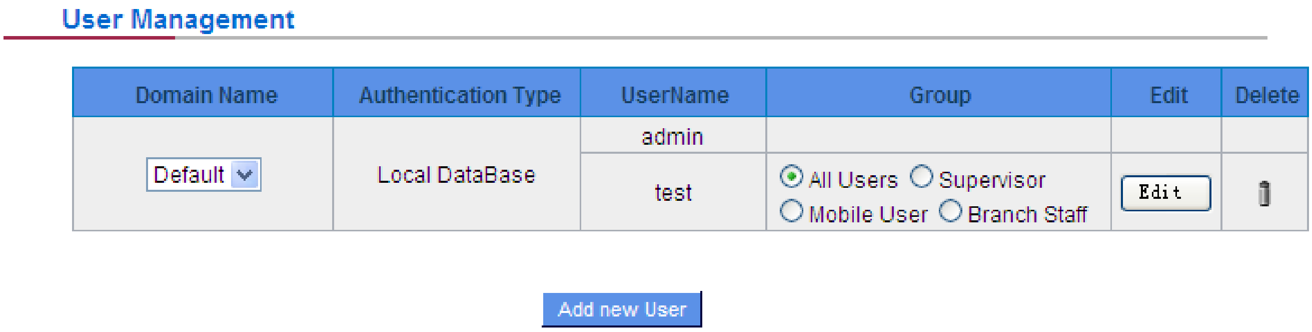
Add New Domain

See 11.3 "Group Management".

11.5 User Management

In addition to selecting 12.3 Group Management to configure group settings, SSL VPN can also provide inter-group user management. On the user management list, each authentication server will display all self-defined users that can be appointed to groups.

Group **Step**	**All User Group**	**Supervisor Group**	**Mobile User**	**Branch Staff Group**
Step 1: **Domain Management**				
Step 2: **User Management**				
Step 3: **Service Resource Management:**				



User Management

Domain Name	Authentication Type	UserName	Group	Edit	Delete
Default ▾	Local DataBase	admin			
		test	● All Users ○ Supervisor ○ Mobile User ○ Branch Staff	Edit	🗑

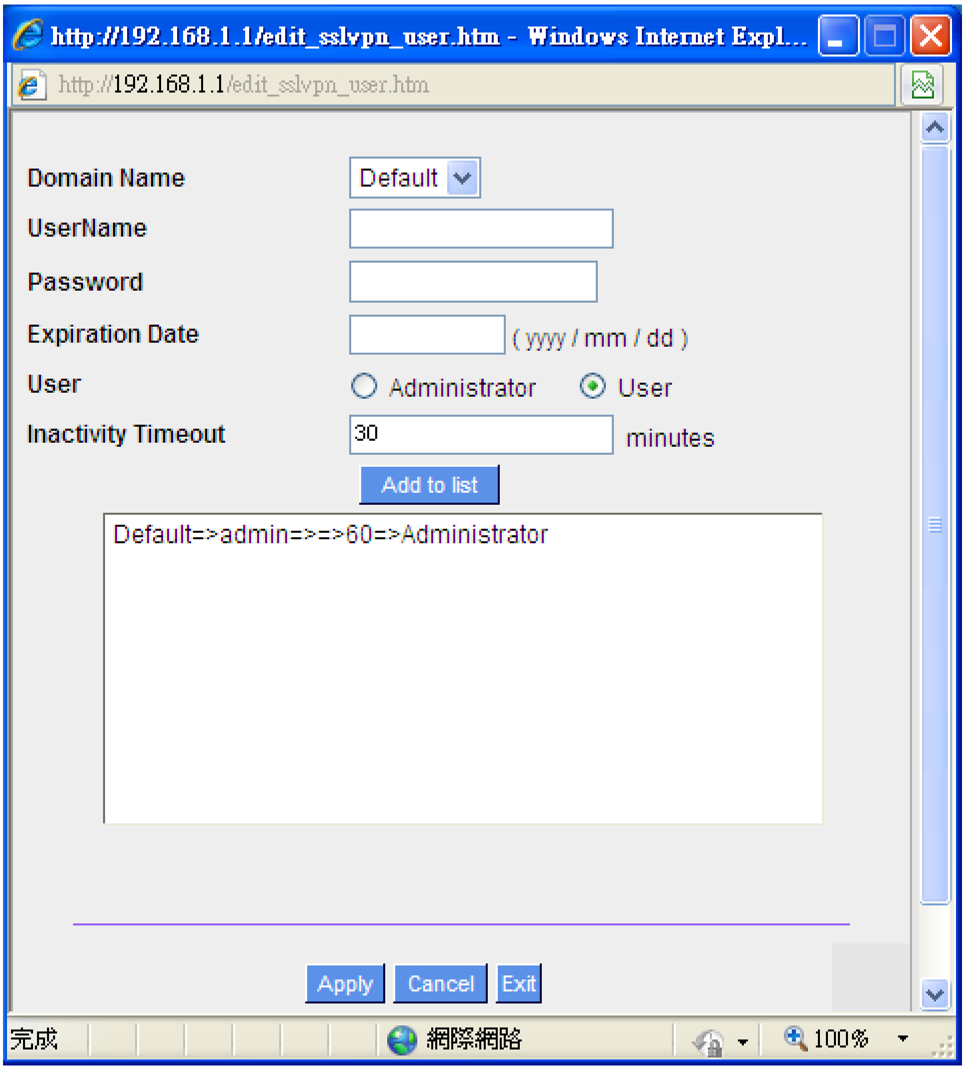
Item	**Description**
Domain Name	Select an authentication server to perform user management on from the drop down menu.
Authentication	Displays the name of the authentication server type and also shows default is Local

Type	Database.
User Name	Displays authentication server's self-defined user names.
Group	Displays which group the user belongs to; from here you can modify user groups.
Edit	User passwords (if Local Database), expiration dates, user classifications, and inactive timeouts can be edited or modified, but user authentication servers and user names cannot. If you want to modify a user name, first delete it, and then add a new user name. You can also select an authentication server to edit IP address and domain name.
Delete	Click on the "Delete" tab to delete selected users.

Add New User

Click on "Add New User" and then the window below will pop up.

Please note: In addition to the local database, user names and passwords must correspond to the selected authentication server's user names.


http://192.168.1.1/edit_sslvpn_user.htm - Windows Internet Expl...
http://192.168.1.1/edit_sslvpn_user.htm

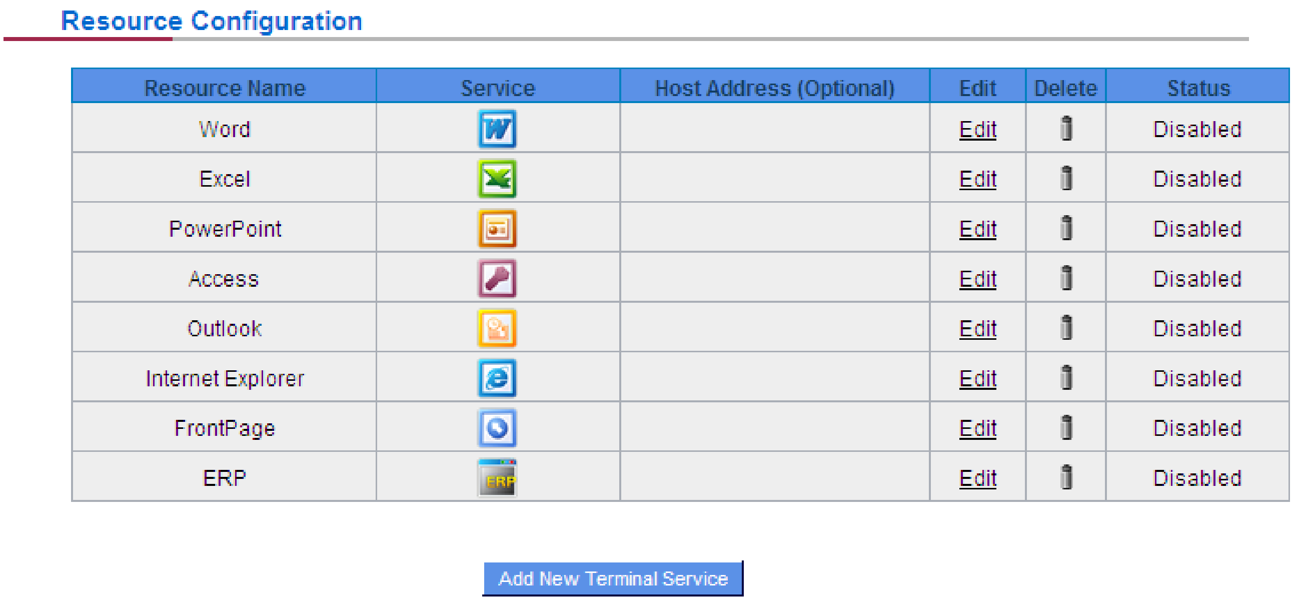
Domain Name: Default
UserName:
Password:
Expiration Date: (yyyy / mm / dd)
User: ○ Administrator ● User
Inactivity Timeout: 30 minutes

Default=>admin=>=>60=>Administrator

Apply
Cancel
Exit
完成
網際網路
100%

Item	Description
Domain Name	Displays the authentication server name.
User Name	Enter authentication server's user names.
Password	For Local Database, enter user passwords. Passwords do not need to be entered if Local Database is not used.
Expiration Date (yyyy/mm/dd)	Enter users' permitted time limit. For example, if the expiration date is set to November 1, 2007, then the user will be denied beginning on November 2, 2007 at 12: 00 AM.
User Type	If set to "Administrator", the user will login on the router management UI. If set to "User", the user will login on the web portal. Please note: Only Local Database users can be set as "Administrator", external authentication server users can only be "User" and cannot login on the router management UI.
Inactive timeout	Even though a user has logged in via the web portal, he/she will be forced to logout (timeout) due to inactivity after 10 minutes. If a user logs into the web portal to access enterprise resources using a SSL in an unsafe environment, a shorter timeout time is recommended to mitigate risk if the user is logged in but inactive.
Add to List	After completing the above settings, click on "Add to List" to add newly created user settings to the corresponding list.
Apply	After settings are complete, click on the "**Apply**" tab to save.
Cancel	Click on the "**Cancel**" tab to cancel all unsaved settings.
Exit	Click on the "**Exit**" tab to close the window.

11.6 Service Resource Management

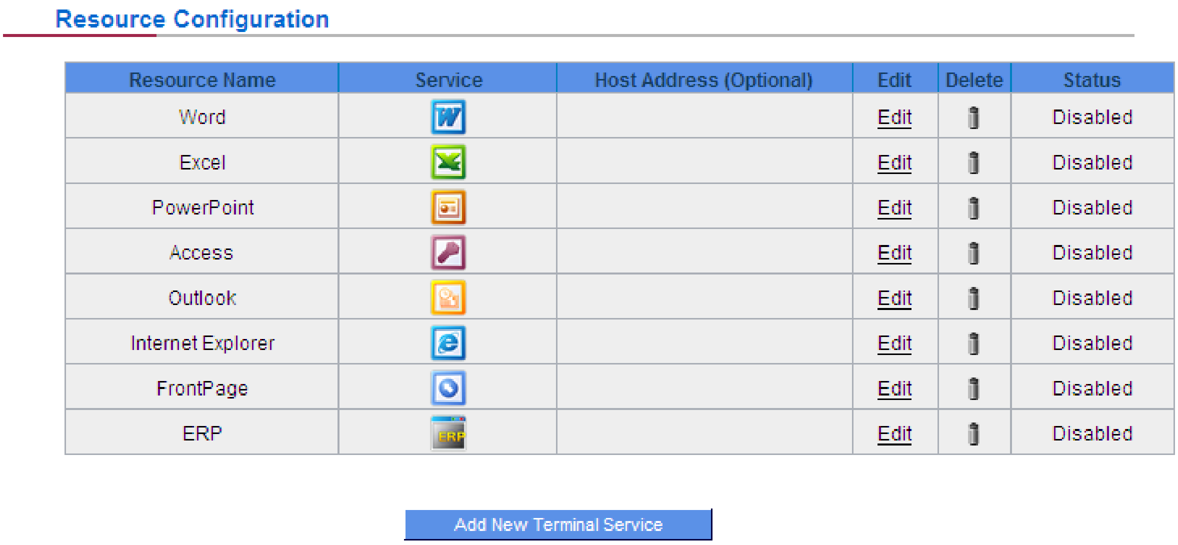


Resource Configuration

Resource Name	Service	Host Address (Optional)	Edit	Delete	Status
Word	W		Edit	🗑	Disabled
Excel	X		Edit	🗑	Disabled
PowerPoint			Edit	🗑	Disabled
Access			Edit	🗑	Disabled
Outlook			Edit	🗑	Disabled
Internet Explorer	e		Edit	🗑	Disabled
FrontPage			Edit	🗑	Disabled
ERP	ERP		Edit	🗑	Disabled

11.6.1 Resource Configuration

SSL VPN supports common Microsoft terminal services (including Word, Excel, PowerPoint, Access, Outlook, IE, FrontPage, and ERP). Administrators can also click on the "**Add New Terminal Service**" tab to add additional terminal services.



Resource Configuration

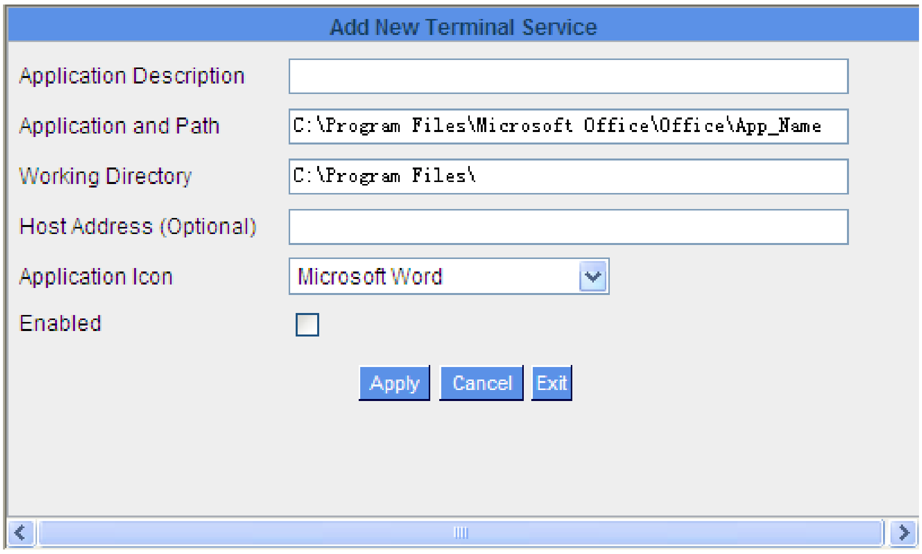
Resource Name	Service	Host Address (Optional)	Edit	Delete	Status
Word	W		Edit	🗑	Disabled
Excel	X		Edit	🗑	Disabled
PowerPoint			Edit	🗑	Disabled
Access			Edit	🗑	Disabled
Outlook			Edit	🗑	Disabled
Internet Explorer	e		Edit	🗑	Disabled
FrontPage			Edit	🗑	Disabled
ERP	ERP		Edit	🗑	Disabled

Item	Description
Resource Name	Display resource name, including SSL VPN supported terminal services like Word, Excel, PowerPoint, Access, Outlook, IE, FrontPage, and ERP.
Service	Display different service icons, which will show on a user's web portal.
Host Address	Display terminal server address.
Edit	Provides selected resource application program paths, execution paths, server

	addresses, and application program image editing. SSL VPN supports built-in application program paths c: \program files\Microsoft office\office\windword.exe. If you have installed Microsoft terminal services that have a different server path, modification will be required. Microsoft terminal service is "Disabled" by default. Once Microsoft terminal service server is set up and configured, activate it to avoid limited services for group users.
Delete	If there is no need to support terminal services, click on the delete icon to delete the resource.
Status	Displays server resource status as Enabled or Disabled.

Add New Terminal Server

If an enterprise has multiple internal terminal servers, click on the "Add New Terminal Service" tab to add a new terminal service.



Add New Terminal Service

Application Description:

Application and Path: C:\Program Files\Microsoft Office\Office\App_Name

Working Directory: C:\Program Files\

Host Address (Optional):

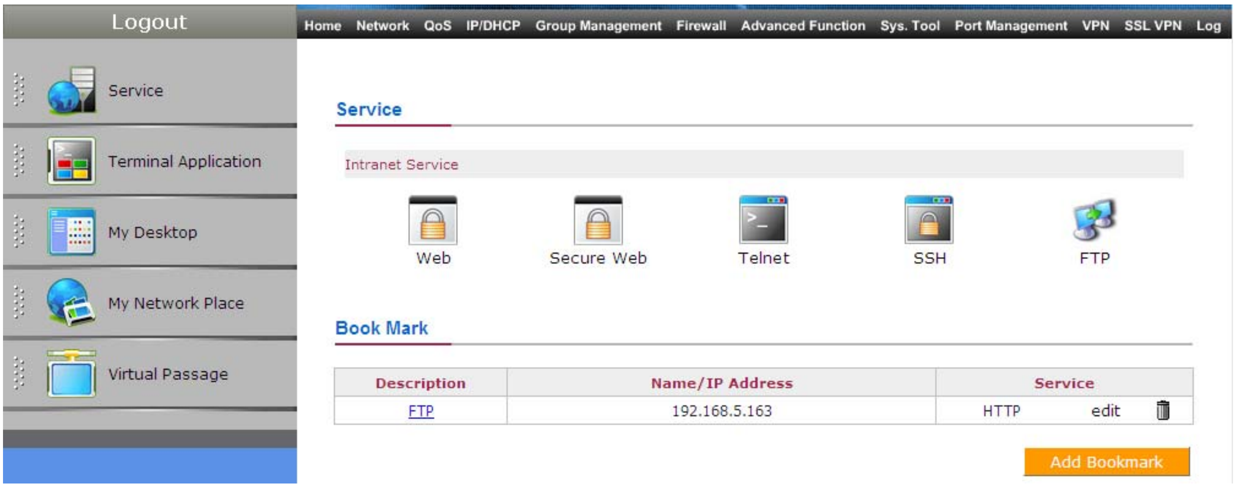
Application Icon: Microsoft Word

Enabled ☐

Item	**Description**
Application Description	Import an application name.
Application and Path	Set installation path this of application server.
Working Directory	Set application working directory.
Host Address	Set server address.
Application Icon	Select the server icon. In addition to built-in icons, there are also commonly used icons.
Enable	Check to activate this service.

11.7 Link to Portal

If user management settings have the user type set to "Administrator", the user will login on the router management UI. For login to the web portal, click "Link to Portal".



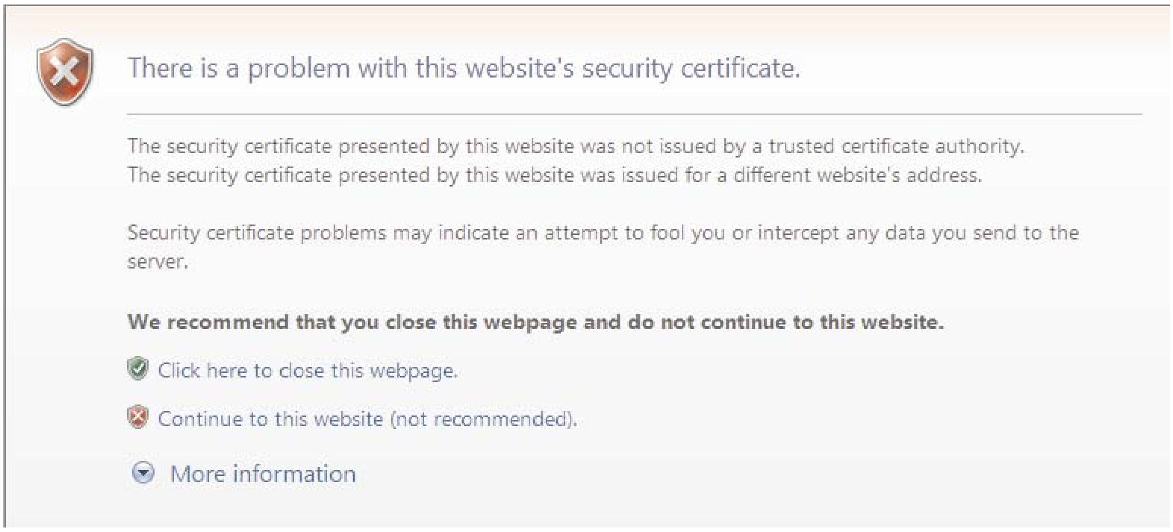
Description	Name/IP Address	Service	
FTP	192.168.5.163	HTTP	edit

11.8 Certificate Management

In short, SSL Certificate is an authentication between web browser and host. A comprehensive certificate includes corporation name, web site name, users account, digital key and validity date of certificate. Web browser will request the web site to show digital certificate when the web browser requests to use SSL mode (https://). If web browser decides to accept the digital certificate, all data between the web site and browser will use certificate digital-key encryption to avoid hacker to access the data.

SSL certificate includes public-key and private-key. Public-key is used to encrypt data while the private-key is used to decrypt. When the web browser connects to SSL network (http://), SSL protocol will verifies server and client identities and creates a encryption method with public key. Then, the SSL will start a security process to protect the privacy and data integrity.

Generally, if users do not import a legal authentication/authorization SSL certificate verified through third party, web page will display as below figure to warm that users have not getting SSL certificate by legal authorized third party agent.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

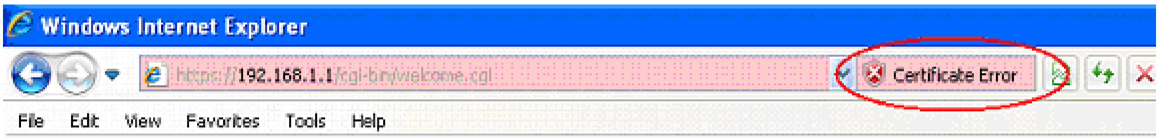
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

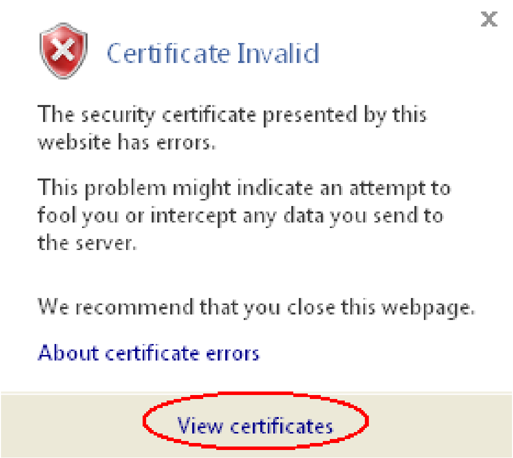
Click here to close this webpage.

Continue to this website (not recommended).

More information



Windows Internet Explorer
https://192.168.1.1/cgi-bin/welcome.cgi
Certificate Error
File
Edit
View
Favorites
Tools
Help



Certificate Invalid

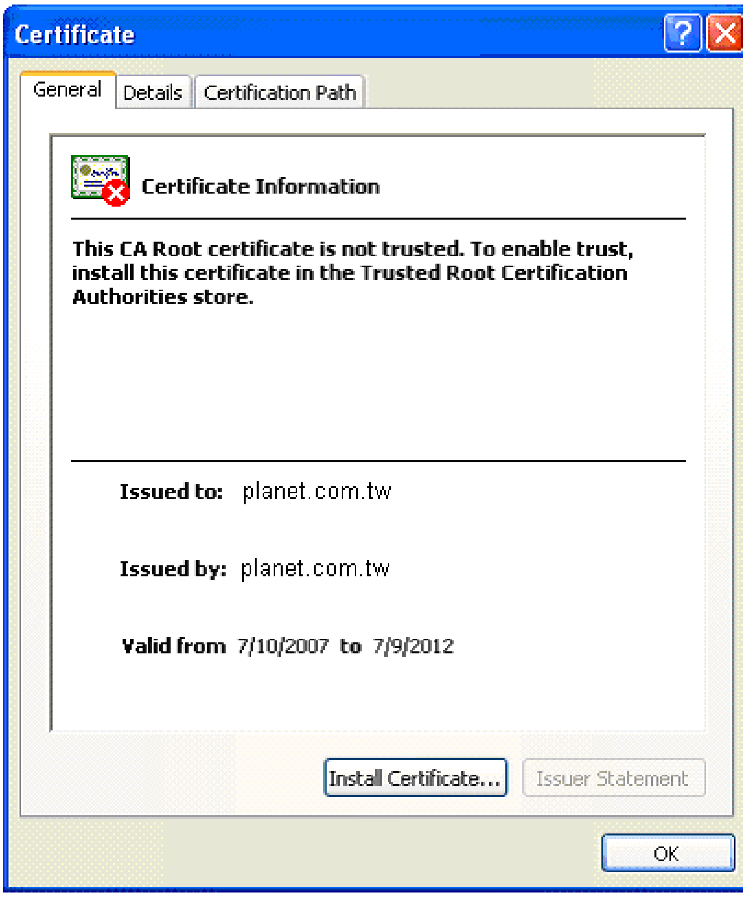
The security certificate presented by this website has errors.

This problem might indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates


Certificate

Certificate Information

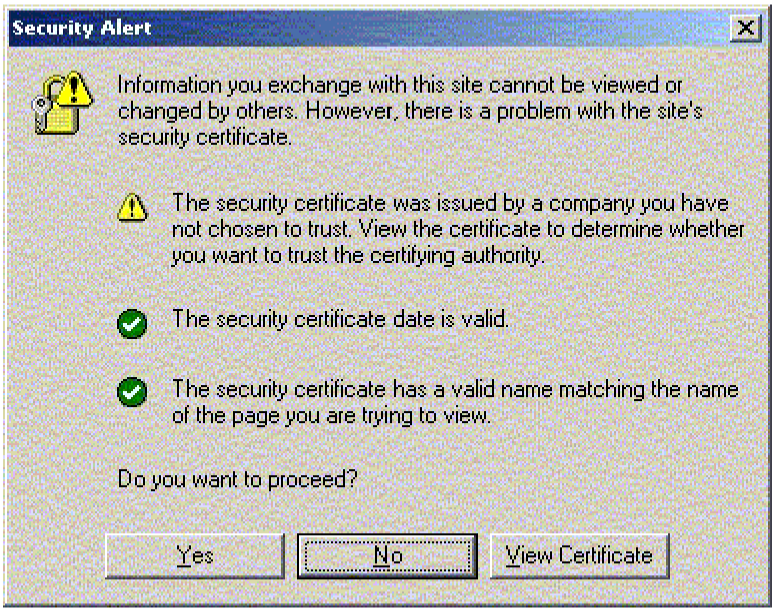
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: planet.com.tw

Issued by: planet.com.tw

Valid from 7/10/2007 to 7/9/2012

The browser older than IE8.0 may display as below figure.


Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

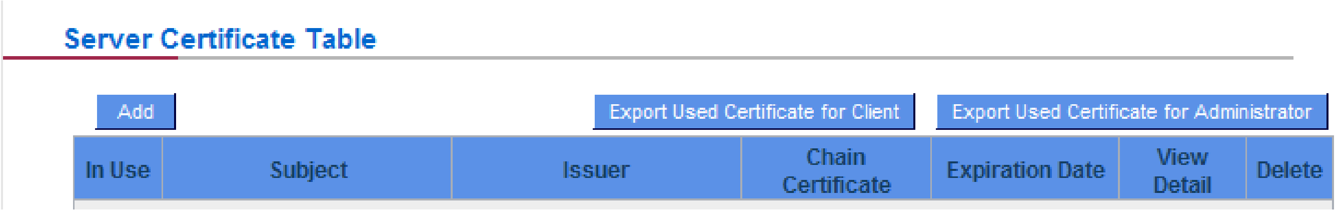
⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Please note that these warning messages won't influence the operation and usage of the SSL VPN. But if you want to apply an integrity SSL certificate from a third party organization, you need contact these third party organizations(for example: VeriSign) and follow their procedures to apply a integrity SSL certificate for your business.



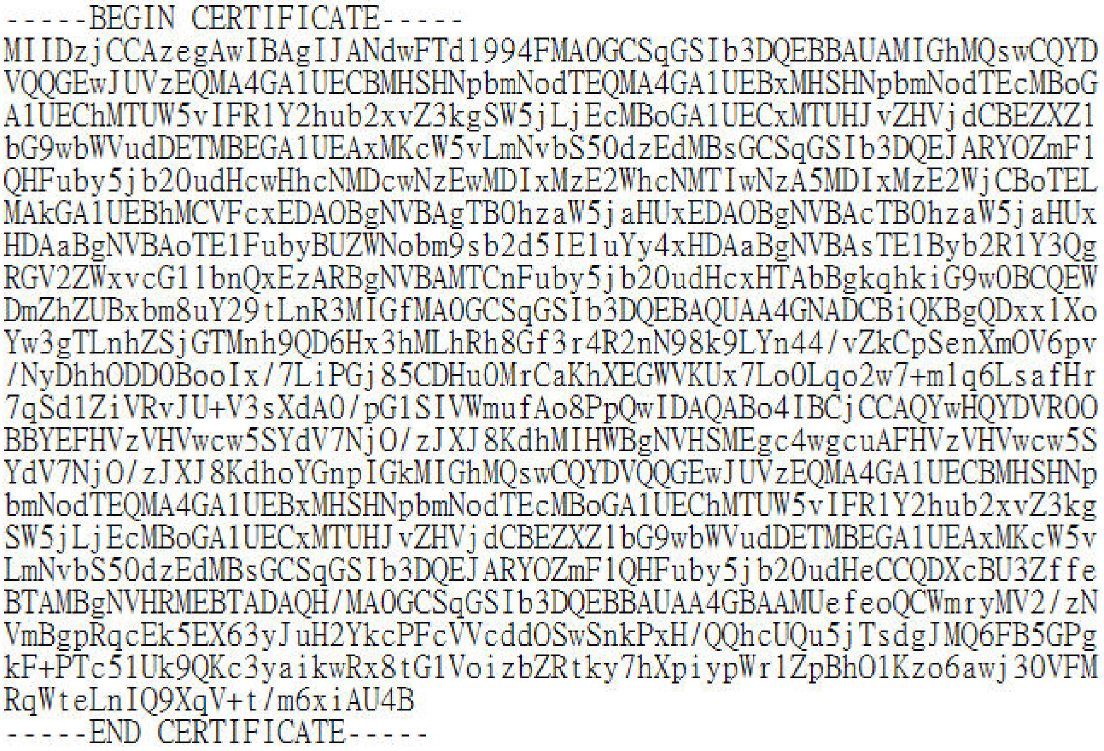
Server Certificate Table

Add
Export Used Certificate for Client
Export Used Certificate for Administrator

In Use	Subject	Issuer	Chain Certificate	Expiration Date	View Detail	Delete

SSL certificate import:

Generally, SSL certificate format looks like the diagram below, and it indicates a .PEM file format which is available in the Planet System. Users only need to copy all the letters (including the “Begin” and “End”) into the notepad file and save to .PEM file. Then, users can import this .PEM file into Planet System. Press the “**Add**” tab to import certificate.



```
-----BEGIN CERTIFICATE-----
MIIDzjCCAzegAwIBAgIJANdwFTd1994FMA0GCSqGSIb3DQEBBAUAMIGhMQswCQYD
VQQGEwJUVzEQMA4GA1UECBMHSHNpbmNodTEQMA4GA1UEBxMHSHNpbmNodTEcMBoG
A1UEChMTUW5vIFR1Y2hub2xvZ3kgSW5jLjEcMBoGA1UECxMTUHJvZHVjdCBEZXZ1
bG9wbWVudDETMBEGA1UEAxMKcW5vLmNvbS50dzEdMBsGCSqGSIb3DQEJARYOZmF1
QHFuby5jb20udHcwHhcNMDcwNzEwMDIxMzE2WhcNMTIwNzA5MDIxMzE2WjCBoTEL
MAkGA1UEBhMCVFcxEDAOBgNVBAgTB0hzaW5jaHUxEDAOBgNVBAcTB0hzaW5jaHUx
HDAaBgNVBAoTE1FubyBUZWNobm9sb2d5IE1uYy4xHDAaBgNVBAsTE1Byb2R1Y3Qg
RGV2ZWxvcG11bnQxEzARBgNVBAMTCnFuby5jb20udHcxHTAbBgkqhkiG9w0BCQEW
DmZhZUBxbm8uY29tLnR3MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDxx1Xo
Yw3gTLnhZSjGTMnh9QD6Hx3hMLhRh8Gf3r4R2nN98k9LYn44/vZkCpSenXmOV6pv
/NyDhhODD0BooIx/7LiPGj85CDHu0MrCaKhXEGWVKUx7Lo0Lqo2w7+m1q6LsafHr
7qSd1ZiVRvJU+V3sXdA0/pG1SIVWmufAo8PpQwIDAQABo4IBCjCCAQYwHQYDVR0O
BBYEFHVzVHVwcw5SYdV7NjO/zJXJ8KdhMIHWBgNVHSMEgc4wgcuAFHVzVHVwcw5S
YdV7NjO/zJXJ8KdhoYGnpIGkMIGhMQswCQYDVQQGEwJUVzEQMA4GA1UECBMHSHNp
bmNodTEQMA4GA1UEBxMHSHNpbmNodTEcMBoGA1UEChMTUW5vIFR1Y2hub2xvZ3kg
SW5jLjEcMBoGA1UECxMTUHJvZHVjdCBEZXZ1bG9wbWVudDETMBEGA1UEAxMKcW5v
LmNvbS50dzEdMBsGCSqGSIb3DQEJARYOZmF1QHFuby5jb20udHeCCQDXcBU3Zffe
BTAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAAMUefeoQCWmryMV2/zN
VmBgpRqcEk5EX63yJuH2YkcPFcVVcdd0SwSnkPxH/QQhcUQu5jTsdgJMQ6FB5GPg
kF+PTc51Uk9QKc3yaikwRx8tG1VoizbZRtky7hXpiypWr1ZpBh01Kzo6awj30VFM
RqWteLnIQ9XqV+t/m6xiAU4B
-----END CERTIFICATE-----
```

If the SSL certificate is .CER file, users can translate file to .PEM file format by Windows build-in translation tool.

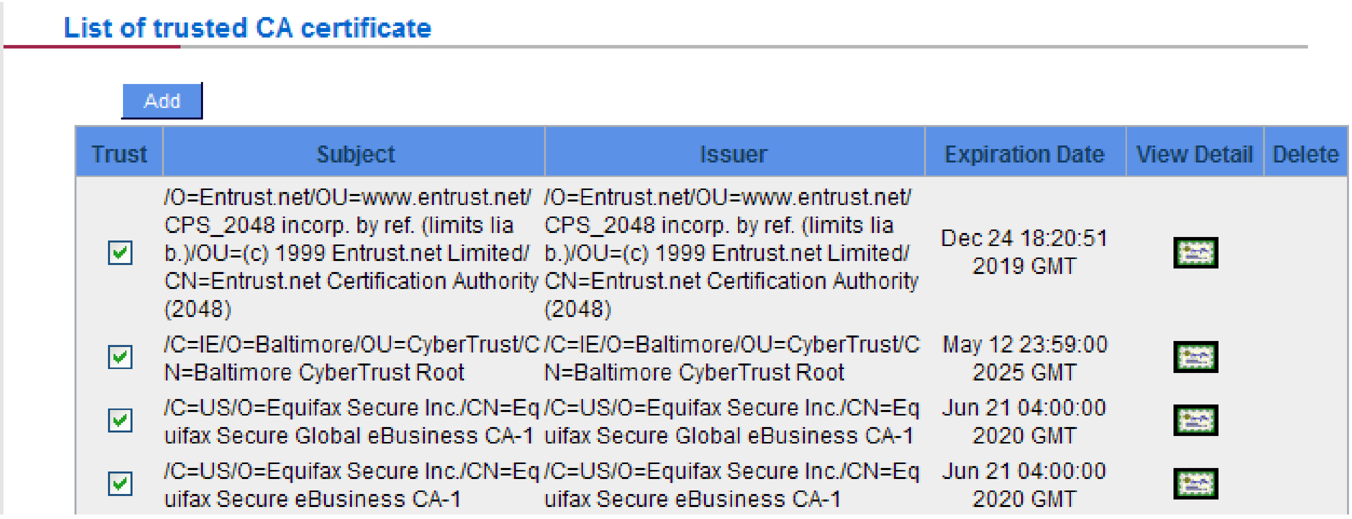
To export SSL certificate for administrator：

Administrators can not only export the completed SSL certificate from a SSL VPN Firewall Router, but also import the certificate to others SSL VPN Firewall Router. The file format is .PEM file. Please click to export.

To export SSL certificate for User：

Users can export the SSL certificate from PC (excluding private-key) and import to other PCs. The exported file format is .PEM file. Please click Export Used Certificate for Client to export.

To add CA certificate into trusted list：



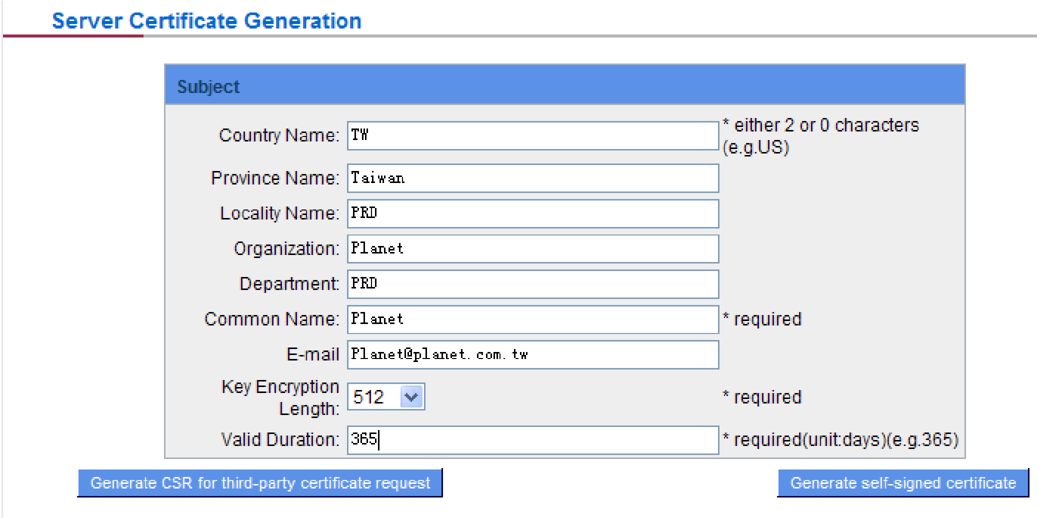
List of trusted CA certificate

Add

Trust	Subject	Issuer	Expiration Date	View Detail	Delete
☑	/O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)	/O=Entrust.net/OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.)/OU=(c) 1999 Entrust.net Limited/CN=Entrust.net Certification Authority (2048)	Dec 24 18:20:51 2019 GMT	▤	
☑	/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root	/C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	▤	
☑	/C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1	/C=US/O=Equifax Secure Inc./CN=Equifax Secure Global eBusiness CA-1	Jun 21 04:00:00 2020 GMT	▤	
☑	/C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1	/C=US/O=Equifax Secure Inc./CN=Equifax Secure eBusiness CA-1	Jun 21 04:00:00 2020 GMT	▤	

Users can also add CA certificate from trusted issuer. Please click the "**Add**" tab to add into list.

To Generate Certificate：



Server Certificate Generation

Subject

Country Name:	TW	* either 2 or 0 characters (e.g.US)
Province Name:	Taiwan	
Locality Name:	PRD	
Organization:	Planet	
Department:	PRD	
Common Name:	Planet	* required
E-mail	Planet@planet.com.tw	
Key Encryption Length:	512	* required
Valid Duration:	365	* required(unit:days)(e.g.365)

Generate CSR for third-party certificate request   Generate self-signed certificate

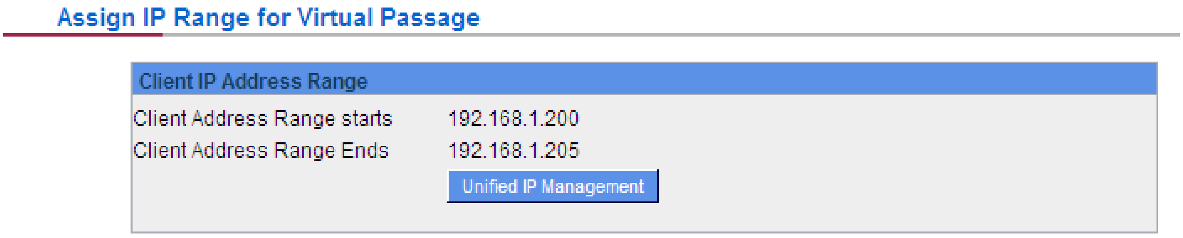
Users can generate CSR for third-party certificate request by clicking Generate CSR for third-party certificate request tab. The exported file format is .txt file. You can also generate a self-signed certificate. The exported file format will be .PEM file.

11.9 Advanced Settings

Advanced Settings can modify SSL connection ports & add SSL upgrades.

11.9.1 Assign IP Range for Virtual Passage

A virtual passage is a type of point-to-point SSL client connection. When remote users use a secure tunnel to connect, SSL VPN will establish a virtual web interface. For this reason, you will need to set SSL VPN's secure tunnel client address range so it does not conflict with your company's Internet DHCP IP. Default for 5 SSL users is 192.168.1.200 to 192.168.1.205.



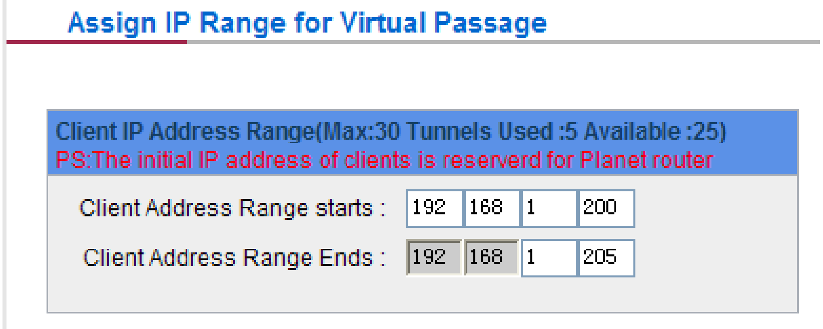
Assign IP Range for Virtual Passage

Client IP Address Range	
Client Address Range starts	192.168.1.200
Client Address Range Ends	192.168.1.205

Unified IP Management:

The Unified IP Management configuration window can set LAN IP range, DHCP IP range, SSL virtual passage IP range, and PPTP IP address range.

When the client uses SSL secure tunnel to connect to SSL VPN, SSL VPN will assign a LAN IP address to the user. You can use SSL VPN's supported SSL tunnels to adjust "client start addresses" and "client end addresses" to provide ample LAN IP the SSL secure tunnel clients. Ensure that the secure tunnel IP range doesn't conflict with the DHCP IP range or the PPTP secure tunnel IP range.



Assign IP Range for Virtual Passage

Client IP Address Range(Max:30 Tunnels Used :5 Available :25)

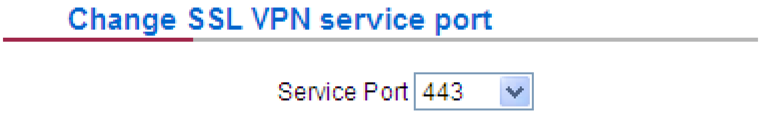
PS:The initial IP address of clients is reserverd for Planet router

Client Address Range starts : 192 168 1 200

Client Address Range Ends : 192 168 1 205

11.9.2 Change SSL VPN service port

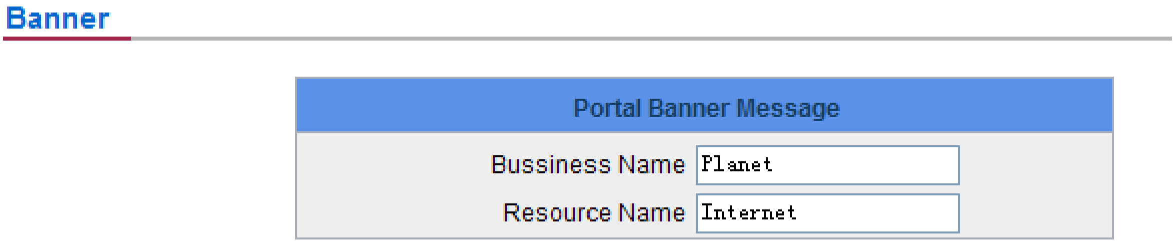
The SSL default port is 443. If port 443 is being used by another internal application, you can use the SSL VPN’s service port drop down menu to select a different one (10443, 20443). Remind: If you change a port other than the default 443, when a client connects to the SSL VPN, the port number will have to be entered after the address.


Change SSL VPN service port

Service Port: 443

11.9.3 Banner

Set the headings for users’ web portal, including enterprise and resource names.

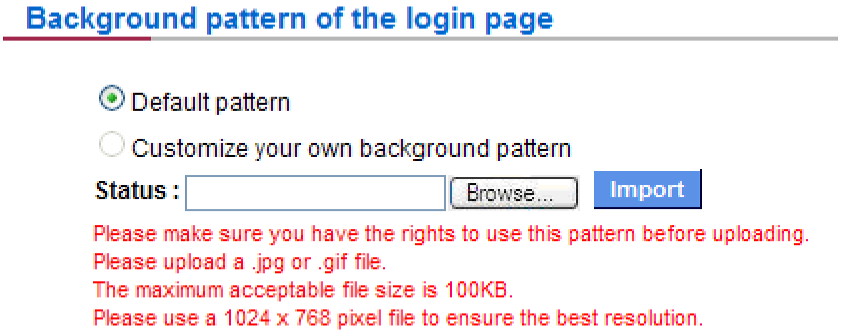

Banner

Portal Banner Message

Bussiness Name: Planet

Resource Name: Internet

11.9.4 Background pattern of the login page


Background pattern of the login page

● Default pattern

○ Customize your own background pattern

Status :

Please make sure you have the rights to use this pattern before uploading.
Please upload a .jpg or .gif file.
The maximum acceptable file size is 100KB.
Please use a 1024 x 768 pixel file to ensure the best resolution.

Administrator can choose to use customize pattern for login page.The file format should be .jpg or .gif, and the size should not be larger than 100KB. Please use a 1024 x 768 pixel picture to ensure the best resolution.

Chapter 12: Advanced Function

This chapter will introduce to you the advance router settings In the advance settings, you can:

1. Setup DMZ servers forwarding to WAN, for example, the Web or FTP servers.

2. Setup static routing entries or dynamic routing protocol.

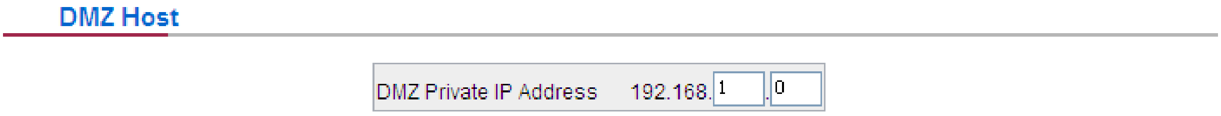
3. Setup one to one NAT function to mapping public IP address and private IP address.

4. Setup dynamic DNS service.

5. Setup MAC address in interfaces.

12.1 DMZ Host/ Port Range Forwarding

12.1.1 DMZ Host



DMZ Private IP Address 192.168.1.0

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:

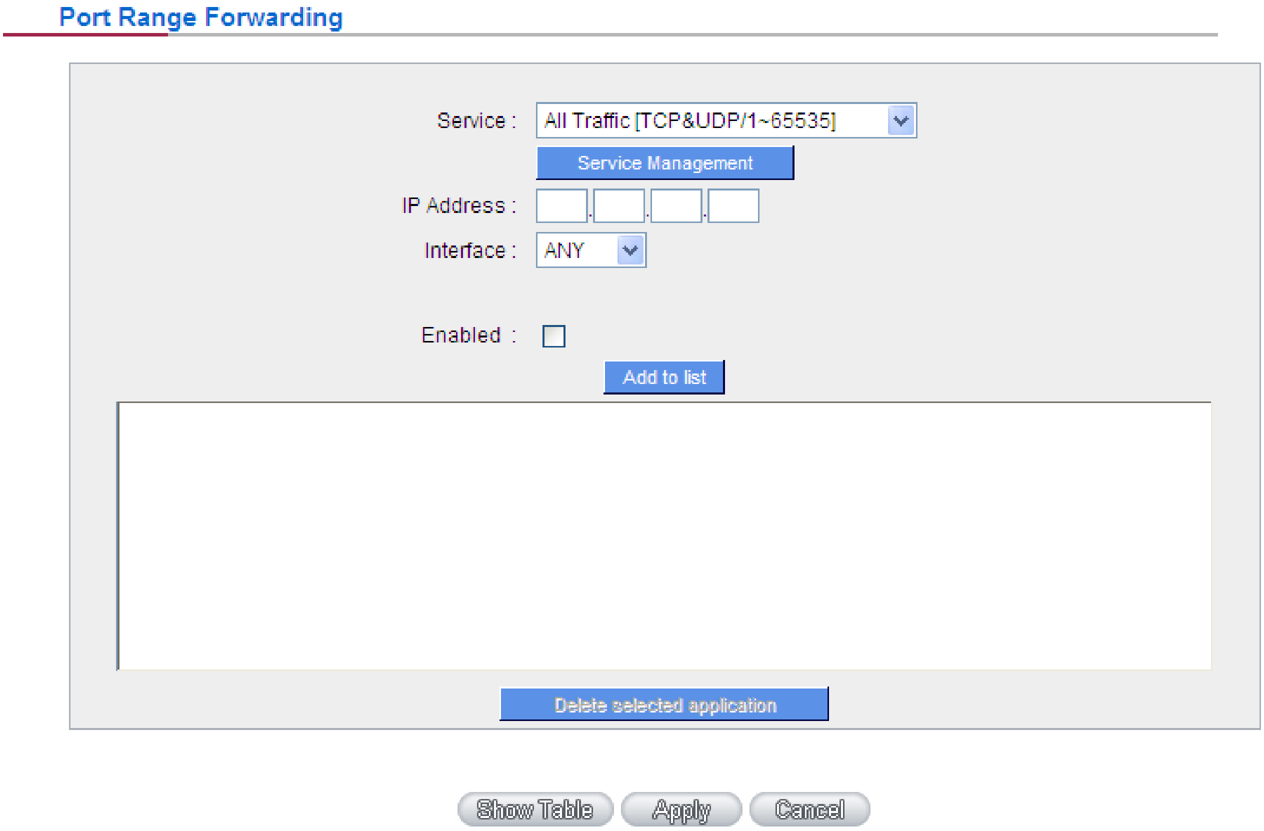
If the "DMZ Host" function is selected, to cancel this function, users must input "0" in the following "DMZ Private IP". This function will then be closed. After the changes are completed, click "Apply" to save the network configuration modification, or click "Cancel" to leave without making any changes.

12.1.2 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 : . . .

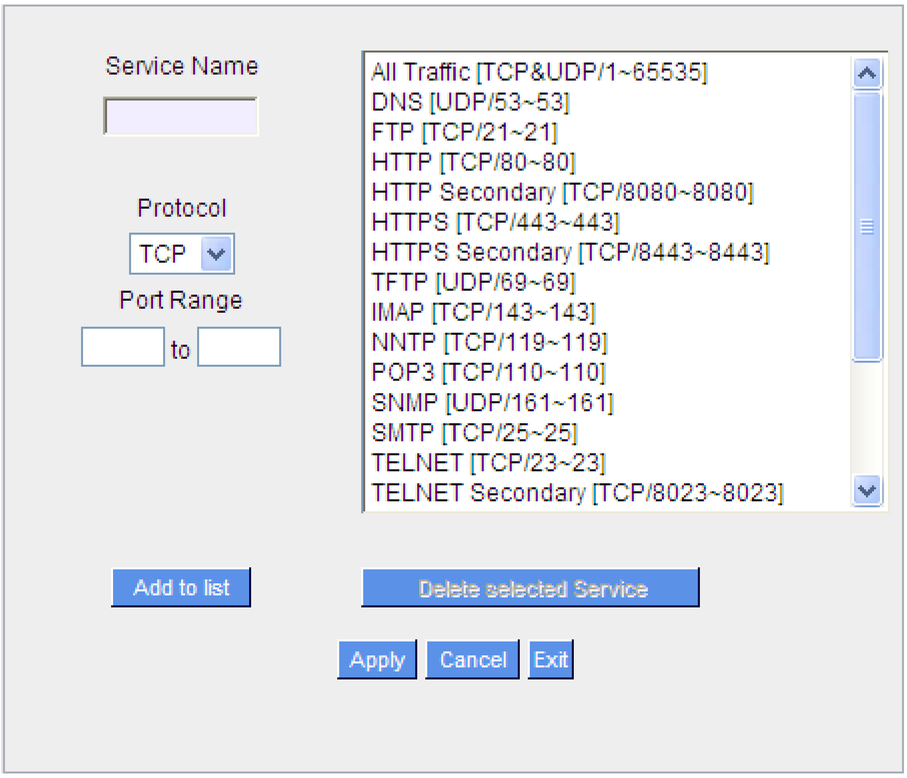
Interface : ANY

Enabled : □

Item	Description
Service	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.
IP Address	Input the virtual host IP address.
Interface	Select the WAN port.
Enabled	Activate this function.
Service Management	Add or remove service ports from the list of service ports.
Add to list	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:



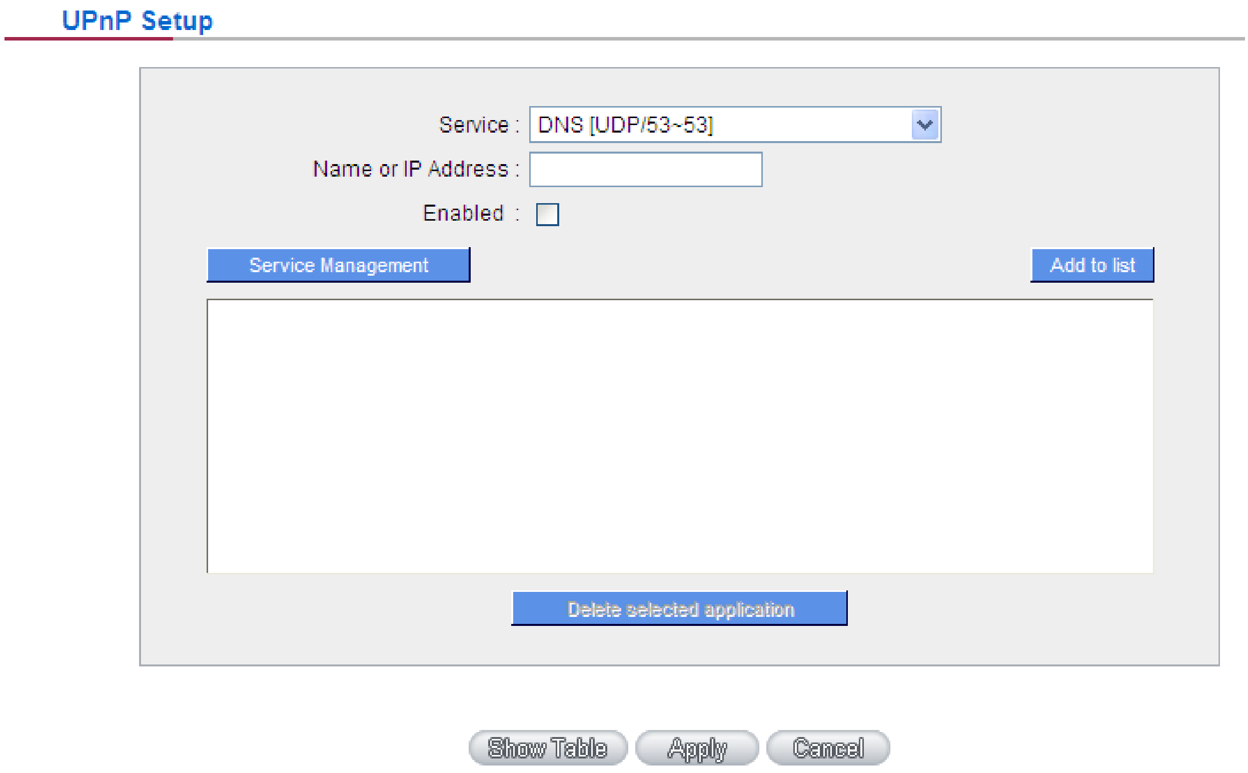
All Traffic [TCP&UDP/1~65535]
DNS [UDP/53~53]
FTP [TCP/21~21]
HTTP [TCP/80~80]
HTTP Secondary [TCP/8080~8080]
HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]

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

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

12.2 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

Service : DNS [UDP/53~53]

Name or IP Address :

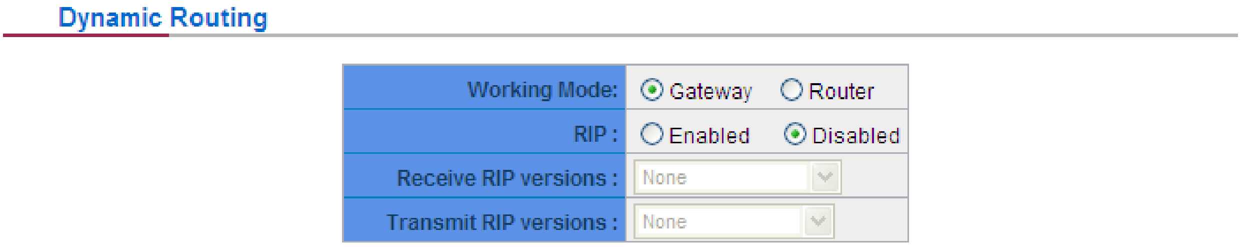
Enabled : □

Item	Description
Service Port	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.
Host Name or IP Address	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.
Enabled	Activate this function.
Service Port Management	Add or remove service ports from the management list.

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

12.3 Routing

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

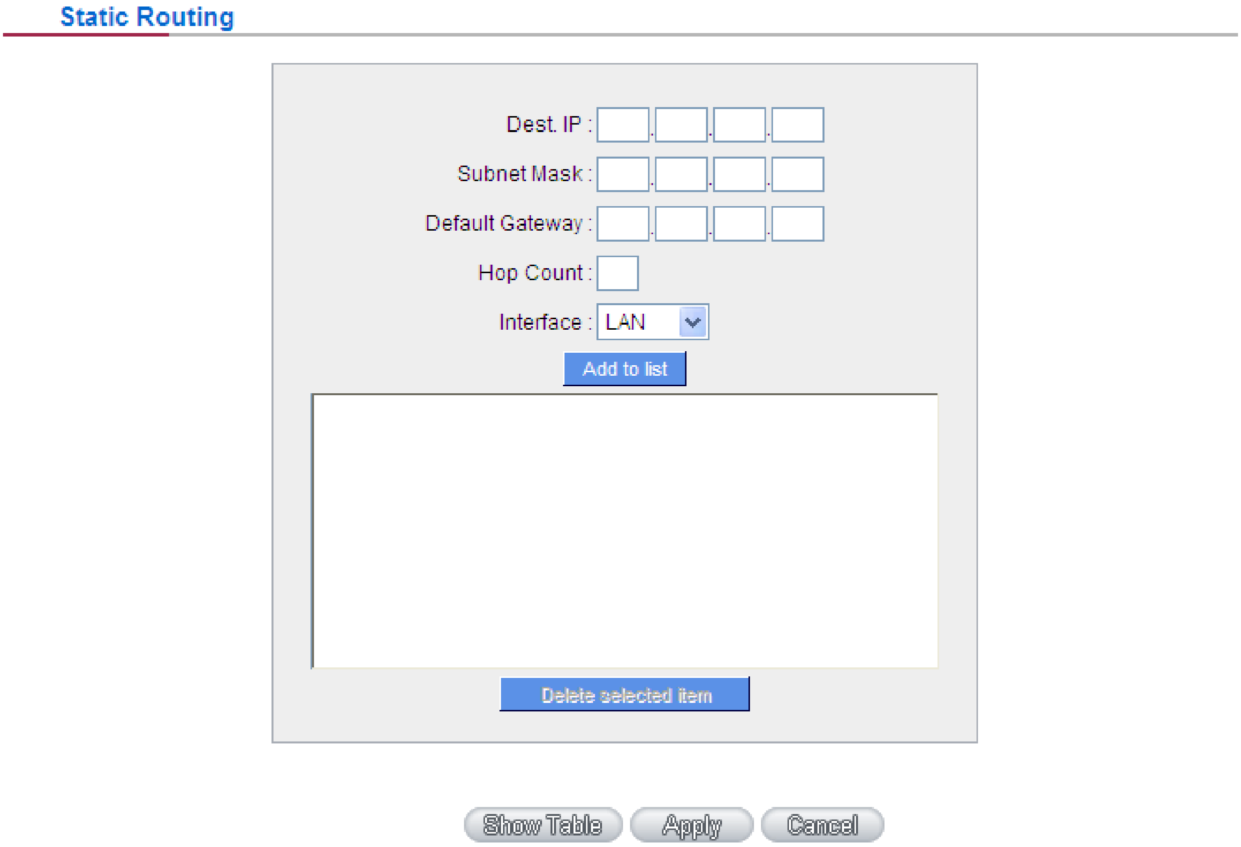


Working Mode: ● Gateway ○ Router

RIP : ○ Enabled ● Disabled

Receive RIP versions : None

Transmit RIP versions : None

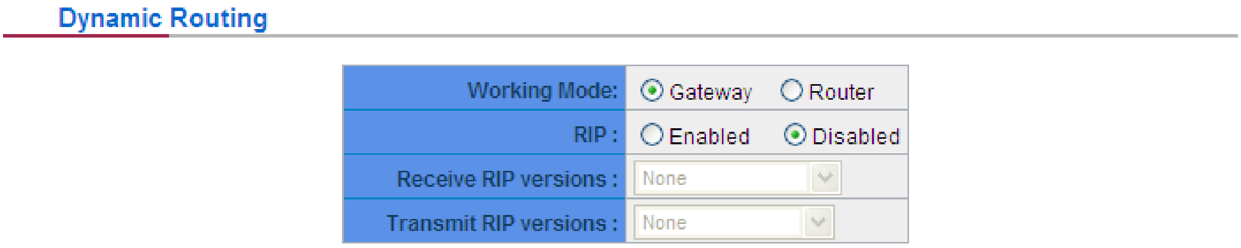


Interface : LAN

12.3.1 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.



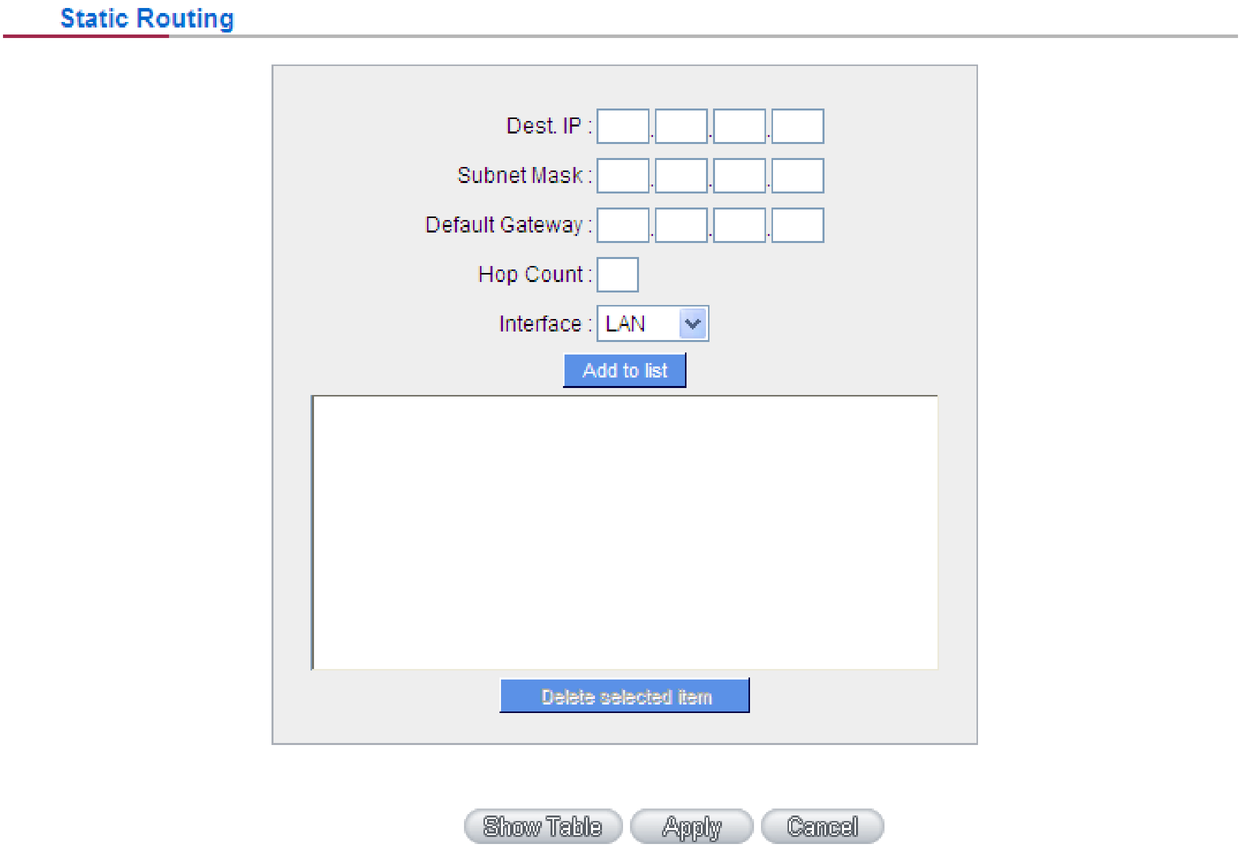
Dynamic Routing

Working Mode:	● Gateway ○ Router
RIP :	○ Enabled ● Disabled
Receive RIP versions :	None
Transmit RIP versions :	None

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

12.3.2 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
Dest. IP **Subnet Mask**	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.
Gateway	The default gateway location of the network node which is to be routed.
Hop Count	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.)
Interface	This is to select "WAN port" or "LAN port" for network connection location.
Add to List	Add the routing rule into the list.
Delete Selected Item	Remove the selected routing rule from the list.
Show Table	Show current routing table.
Apply	Click **"Apply"** to save the network configuration modification
Cancel	Click **"Cancel"** to leave without making any changes.

12.4 One to One NAT

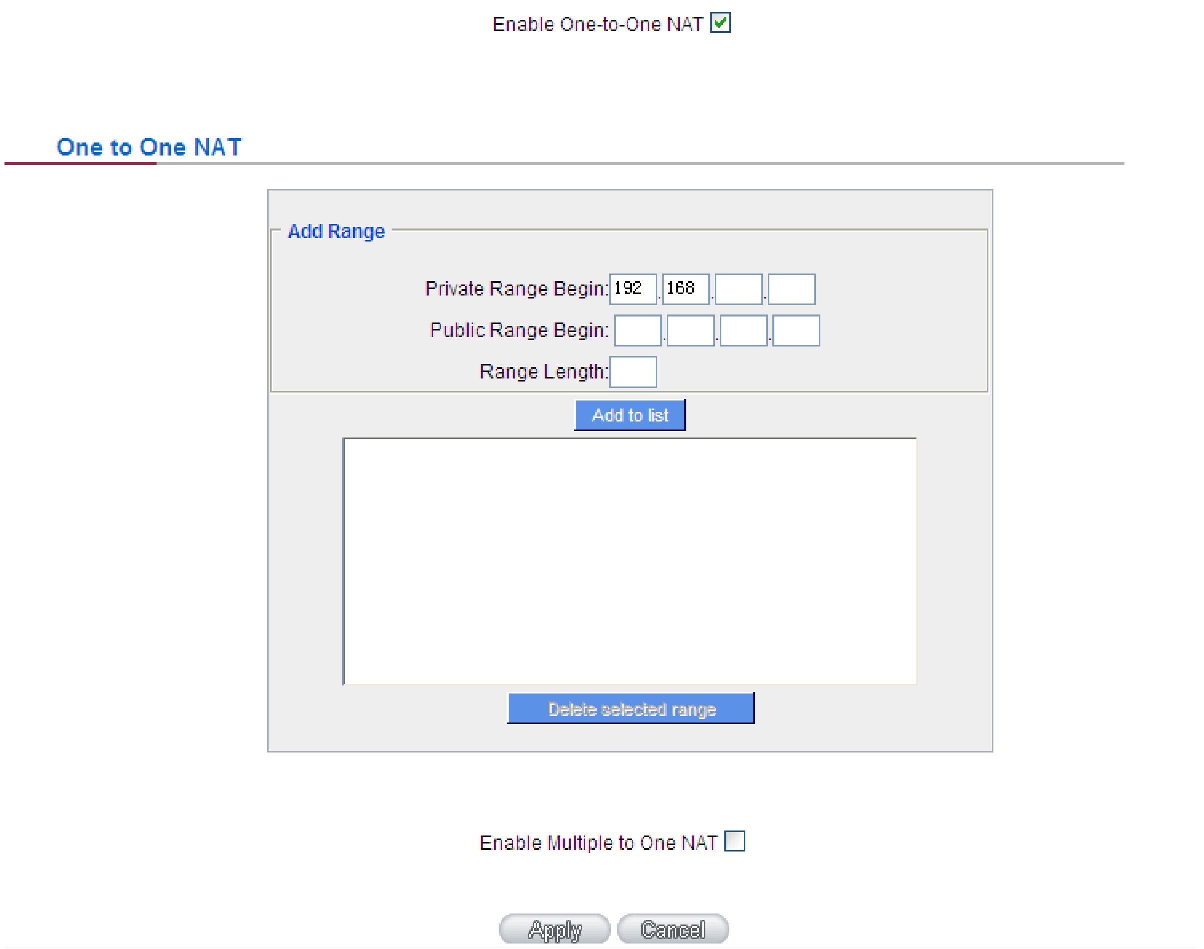
As both the device and ATU-R need only one actual IP, if ISP issued more than one actual IP (such as eight ADSL static IP addresses or more), users can map the remaining real IP addresses to the intranet PC virtual IP addresses. These PCs use private IP addresses in the Intranet, but after having One 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: 192 . 168 . .

Public Range Begin: . . .

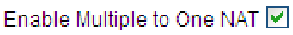
Range Length:

Enable Multiple to One NAT □

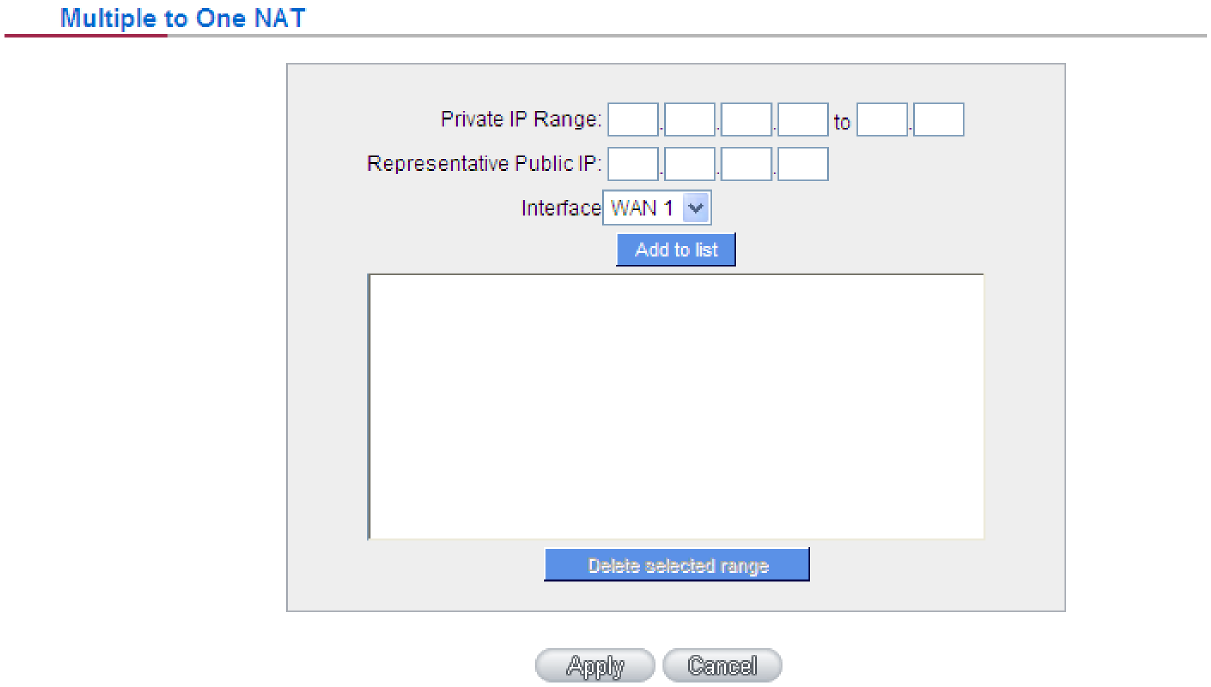
Item	Description
Enabled One to One NAT	To activate or close the One-to-One NAT function. (Check to activate the function).
Private IP Range Begin	Input the Private IP address for the Intranet One-to-One NAT function.
Public IP Range Begin	Input the Public IP address for the Internet One-to-One NAT function.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

✍ **Attention**	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. 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.

Multiple to One NAT



Enable Multiple to One NAT ☑



Multiple to One NAT

Private IP Range: . . . to .

Representative Public IP: . . .

Interface WAN 1

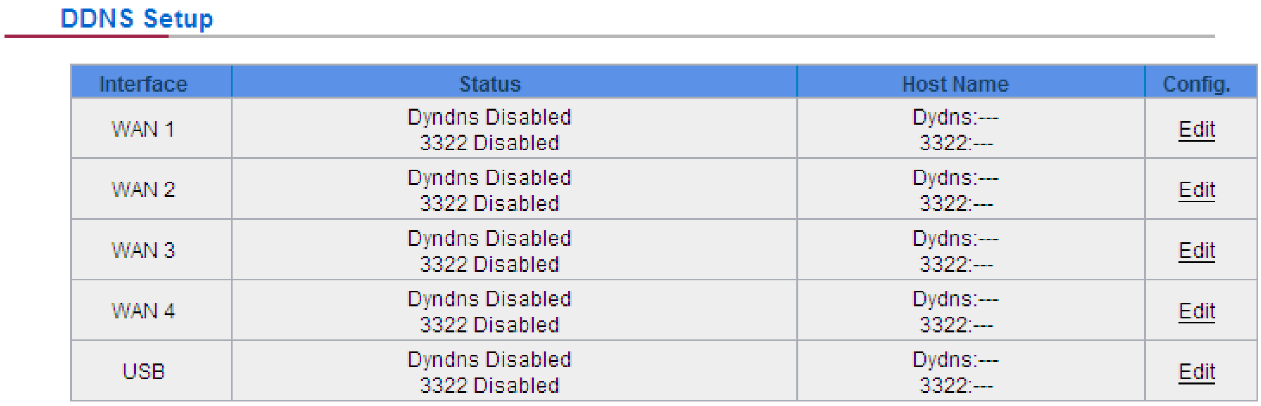
Item	Description
Enable Multiple to One NAT	Click to enable multiple to one NAT function.
Private IP Range	Input intranet IPs for NAT mapping.
Respective Public IP	Input the respective public IP addresses. This should go along with the following interface selection. If the IP address is not within the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

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

12.5 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.

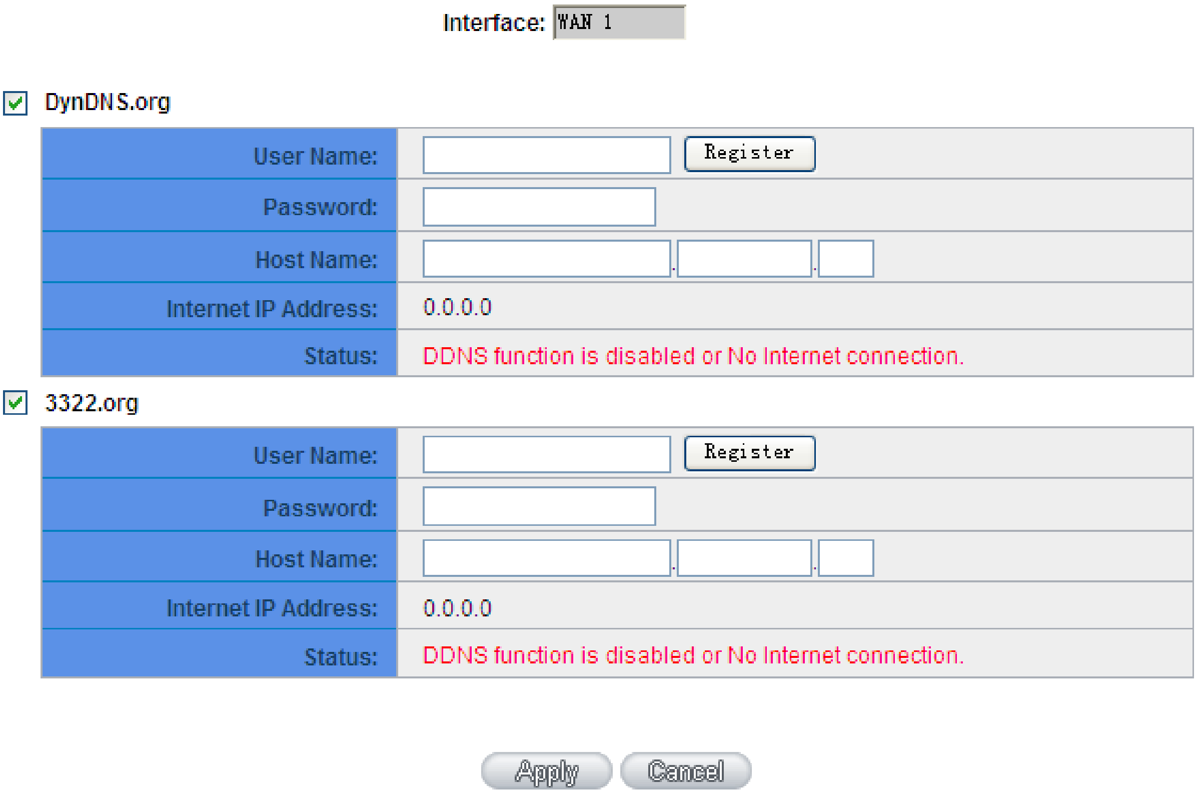
Also, in order to solve the issue that DDNS server is not stable, the device can update the dynamic IP address with different services at the same time.



DDNS Setup

Interface	Status	Host Name	Config.
WAN 1	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
WAN 2	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
WAN 3	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
WAN 4	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit
USB	Dyndns Disabled 3322 Disabled	Dydns:--- 3322:---	Edit

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:	Register
Password:	
Host Name:	. .
Internet IP Address:	0.0.0.0
Status:	DDNS function is disabled or No Internet connection.

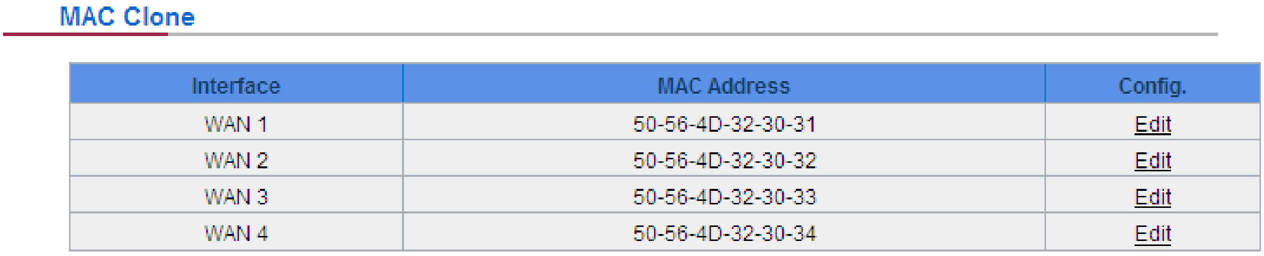
☑ 3322.org

User Name:	Register
Password:	
Host Name:	. .
Internet IP Address:	0.0.0.0
Status:	DDNS function is disabled or No Internet connection.

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

12.6 MAC Clone

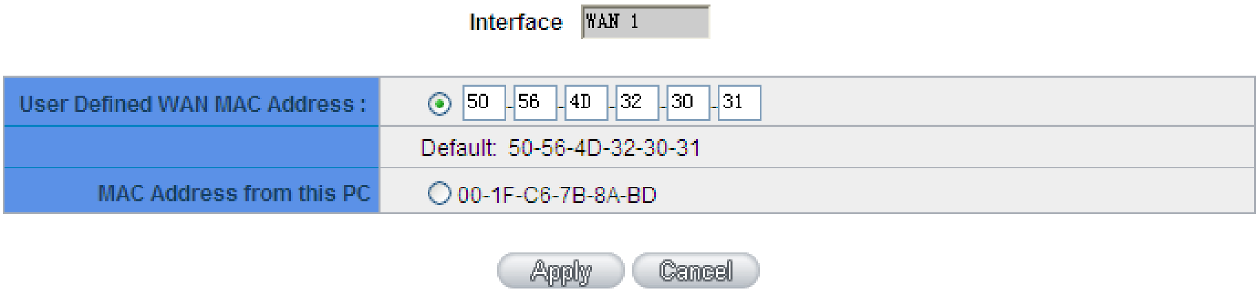
Some ISP will request for a fixed MAC address (network card physical address) for distributing IP address, which is mostly suitable for cable mode users. Users can input the network card physical address (MAC address: 00-xx-xx-xx-xx-xx) here. The device will adopt this MAC address when requesting IP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



MAC Clone

Interface	MAC Address	Config.
WAN 1	50-56-4D-32-30-31	Edit
WAN 2	50-56-4D-32-30-32	Edit
WAN 3	50-56-4D-32-30-33	Edit
WAN 4	50-56-4D-32-30-34	Edit

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 :	● 50 - 56 - 4D - 32 - 30 - 31
	Default: 50-56-4D-32-30-31
MAC Address from this PC	○ 00-1F-C6-7B-8A-BD

Chapter 13: System Tool

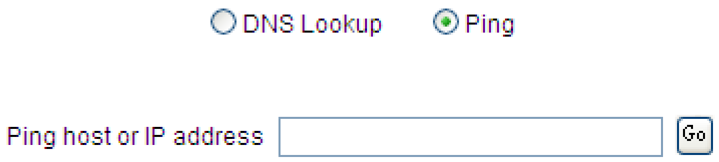
System Tool

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.

13.1 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).

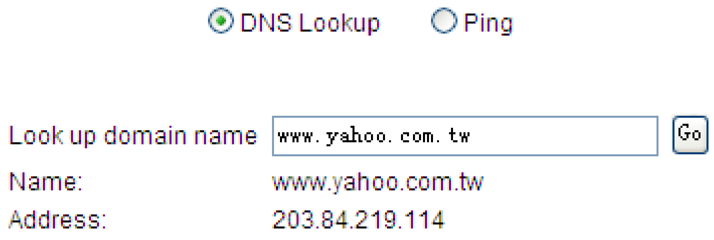


○ DNS Lookup ● Ping

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.



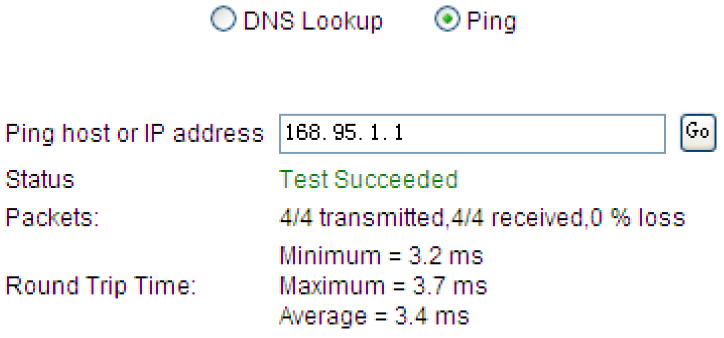
● DNS Lookup ○ Ping

Look up domain name: www.yahoo.com.tw

Name: www.yahoo.com.tw

Address: 203.84.219.114

Ping



○ DNS Lookup ● Ping

Ping host or IP address: 168.95.1.1

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

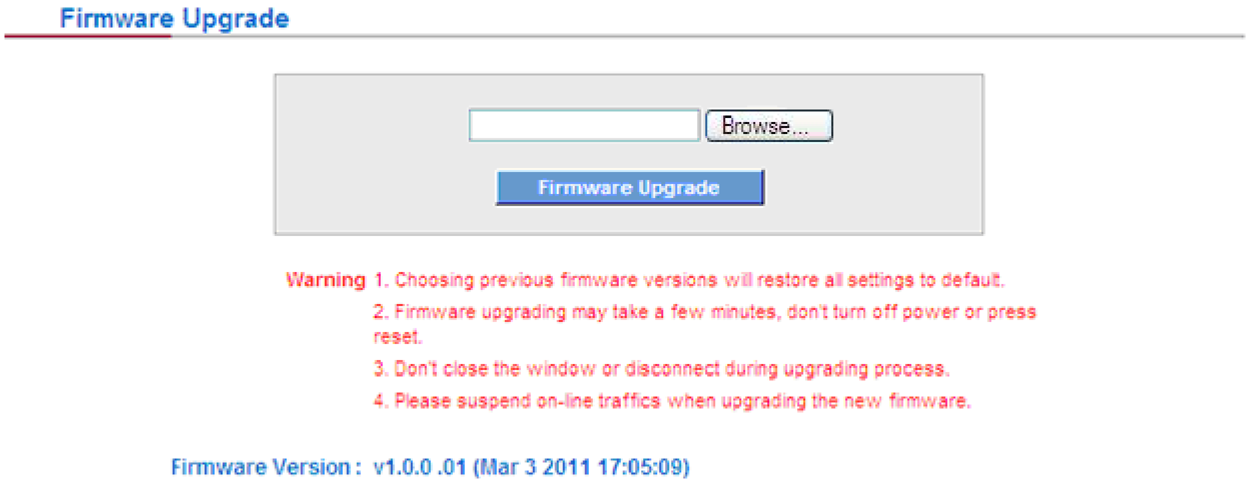
This item informs users of the status quo of the outbound session and allows the user to know the existence of computers online.

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.

13.2 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.

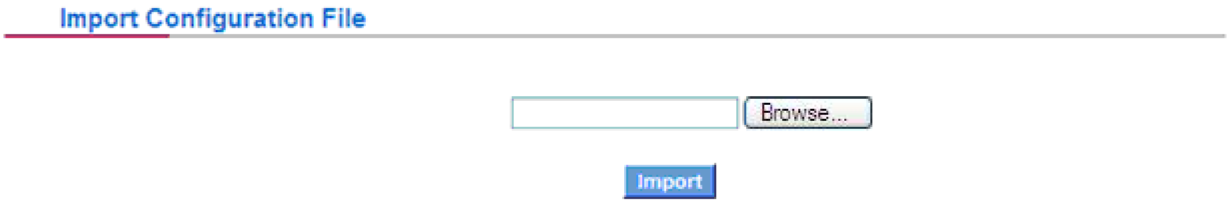
✍ **Attention**	Please read the warning before firmware upgrade. Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.

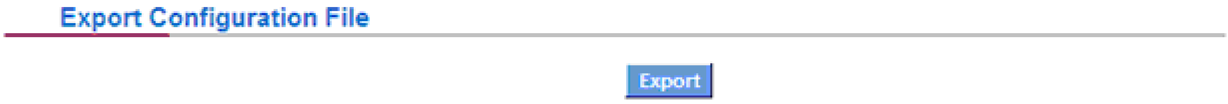


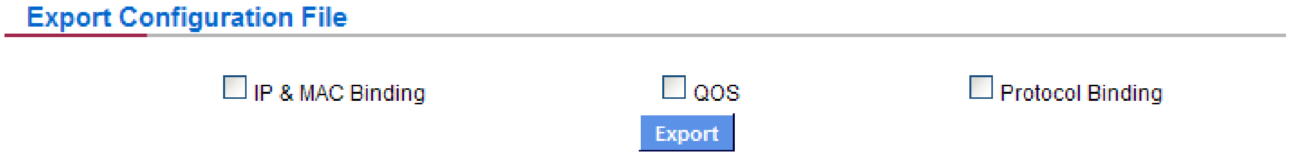
Warning 1. Choosing previous firmware versions will restore all settings to default.
2. Firmware upgrading may take a few minutes, don't turn off power or press reset.
3. Don't close the window or disconnect during upgrading process.
4. Please suspend on-line traffics when upgrading the new firmware.

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

13.3 Configuration Backup







Import Configuration File

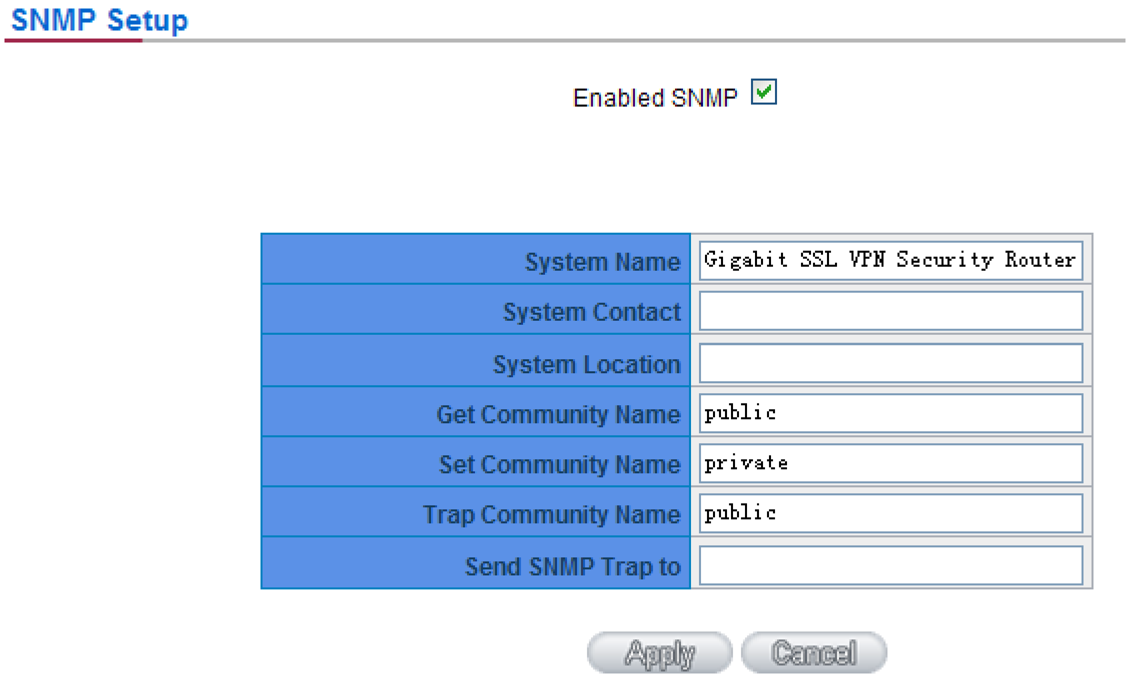
This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click **"Import"** to **import** the file.

Export Configuration File

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

13.4 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

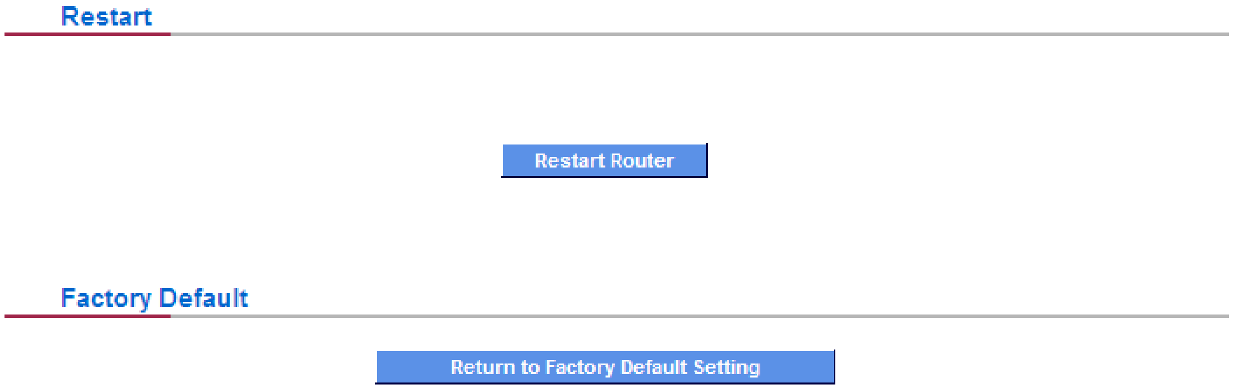
Enabled SNMP ☑

System Name	Gigabit SSL VPN Security Router
System Contact	
System Location	
Get Community Name	public
Set Community Name	private
Trap Community Name	public
Send SNMP Trap to	

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

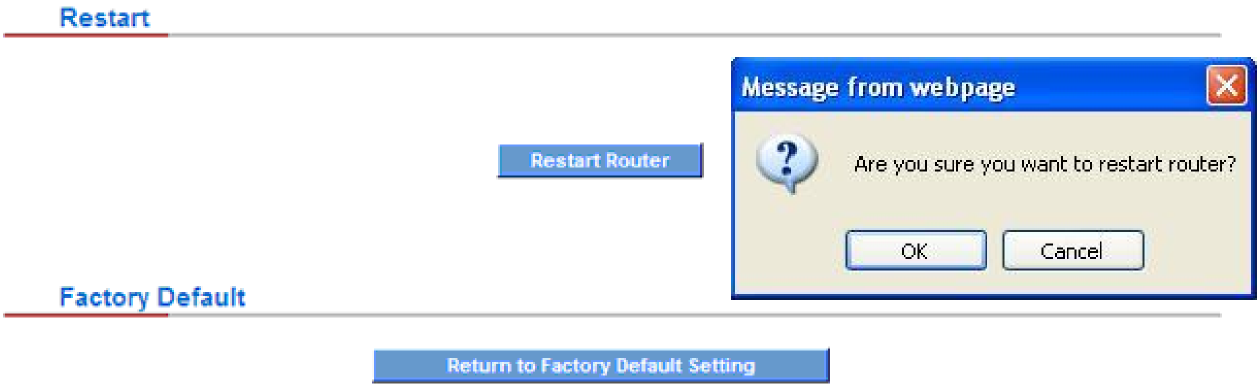
13.5 System Recover

Users can restart the device with System Recover button.



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.



Are you sure you want to restart router?

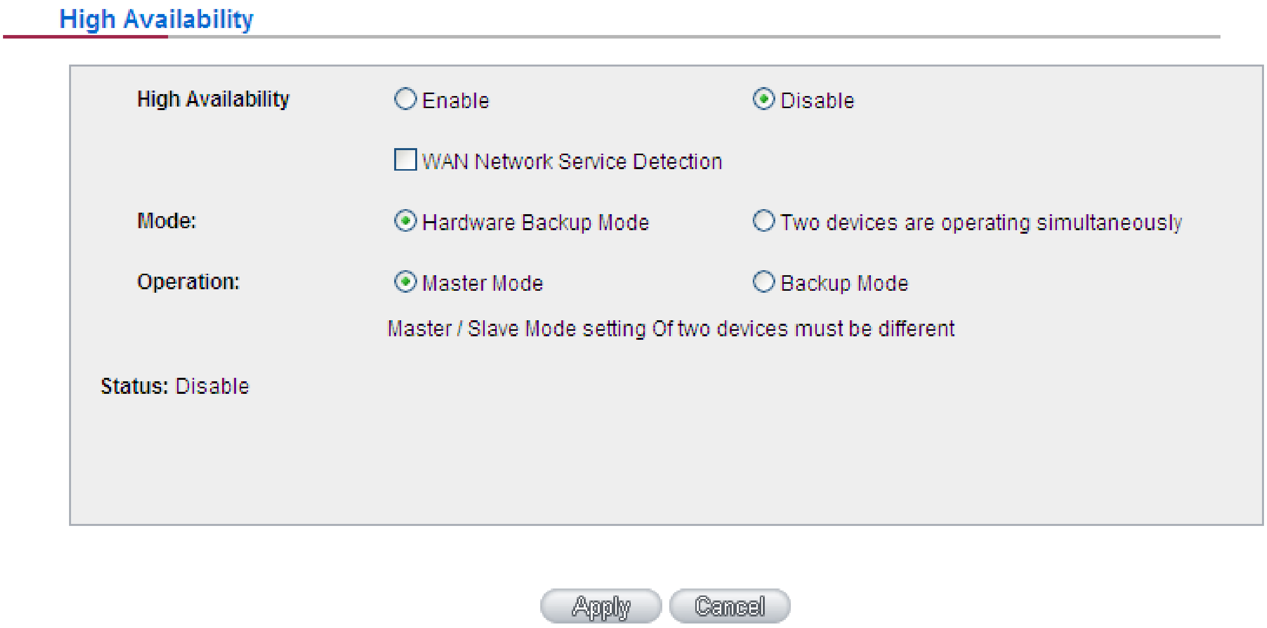
Return to Factory Default Setting

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)

13.6 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 ○ Enable ● Disable

□ WAN Network Service Detection

Mode: ● Hardware Backup Mode ○ Two devices are operating simultaneously

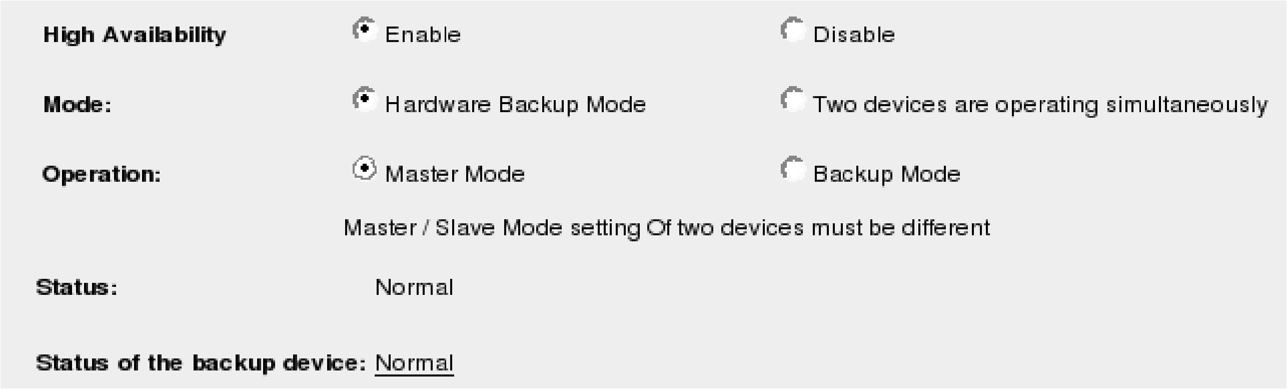
Operation: ● Master Mode ○ Backup Mode

Master / Slave Mode setting Of two devices must be different

Status: Disable

Item	Description
High Availability	**Enable:** Activate HA function. **Disable:** Disable HA function.
Mode	**(1) Hardware Backup Mode** 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. **(2) Two devices are operating simultaneously** 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.

Following is the description of the two different modes.



High Availability ● Enable ○ Disable

Mode: ● Hardware Backup Mode ○ Two devices are operating simultaneously

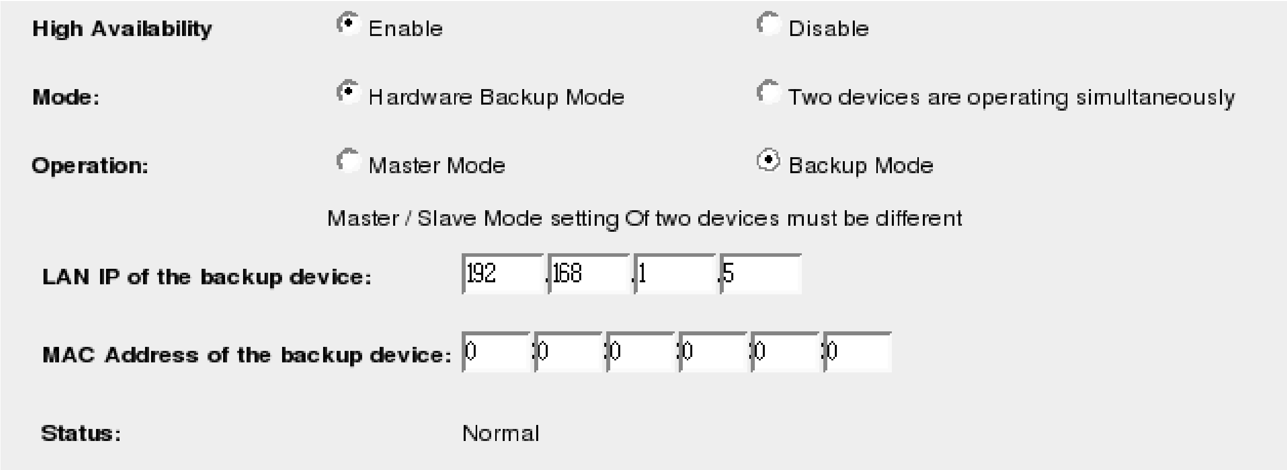
Operation: ● Master Mode ○ Backup Mode

Master / Slave Mode setting Of two devices must be different

Status: Normal

Status of the backup device: Normal

Item	Description
Operation-Master Mode	Indicates the master device will operate for all outbound links. When the master device fails transmitting, the backup device will take over.
Status	"Status- Normal" indicates the device operates well.
Status of the backup device	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.



High Availability ● Enable ○ Disable

Mode: ● Hardware Backup Mode ○ Two devices are operating simultaneously

Operation: ○ Master Mode ● Backup Mode

Master / Slave Mode setting Of two devices must be different

LAN IP of the backup device: 192 . 168 . 1 . 5

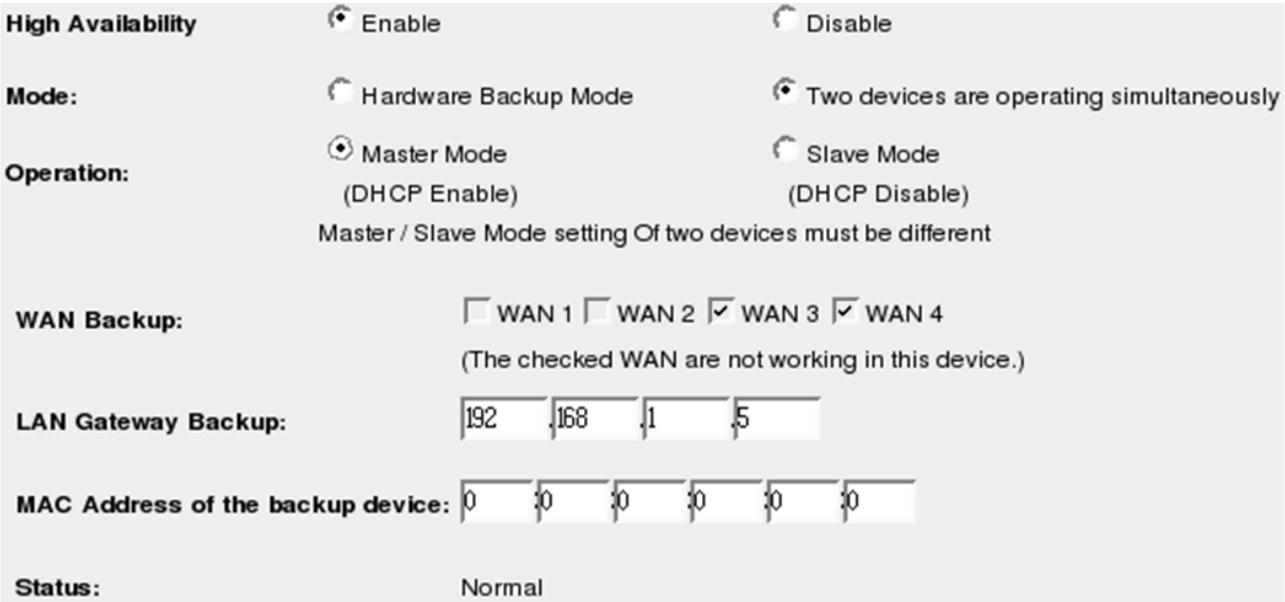
MAC Address of the backup device: 0 : 0 : 0 : 0 : 0 : 0

Status: Normal

Item	Description
Operation-Backup Mode	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.
LAN IP of the backup device	Input LAN IP of Master mode, which is backed up.
MAC Address of the backup device	Input Master device MAC address, which is backed up.
Status	"Status- Normal" indicates the status is idle. Master device operates normally. "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.

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

(The checked WAN are not working in this device.)

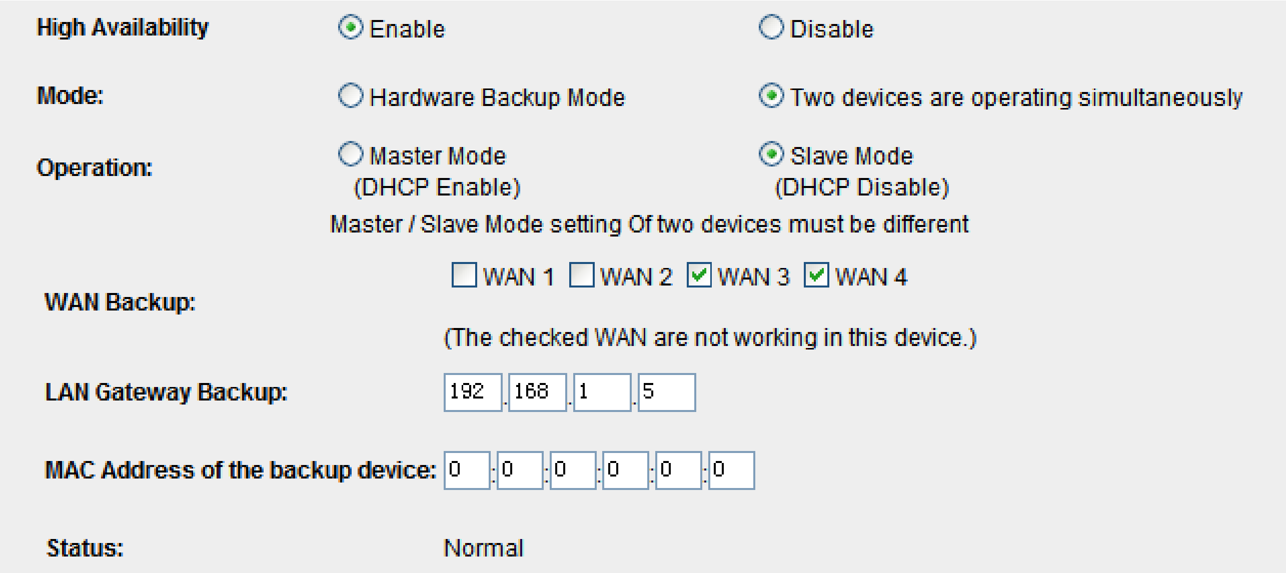
LAN Gateway Backup: 192 . 168 . 1 . 5

MAC Address of the backup device: 0 : 0 : 0 : 0 : 0 : 0

Status: Normal

Item	Description
Operation-Master Mode	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.
WAN Backup (The Checked WANs are not working in this device.)	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.
LAN Gateway Backup	Input LAN IP of Slave device. The IP should be different from LAN IP of Master device.
MAC Address of the	Input LAN MAC of Slave device. It should be different from LAN MAC of Master

backup device	device.
Status	"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: 192 . 168 . 1 . 5

MAC Address of the backup device: 0 : 0 : 0 : 0 : 0 : 0

Status: Normal

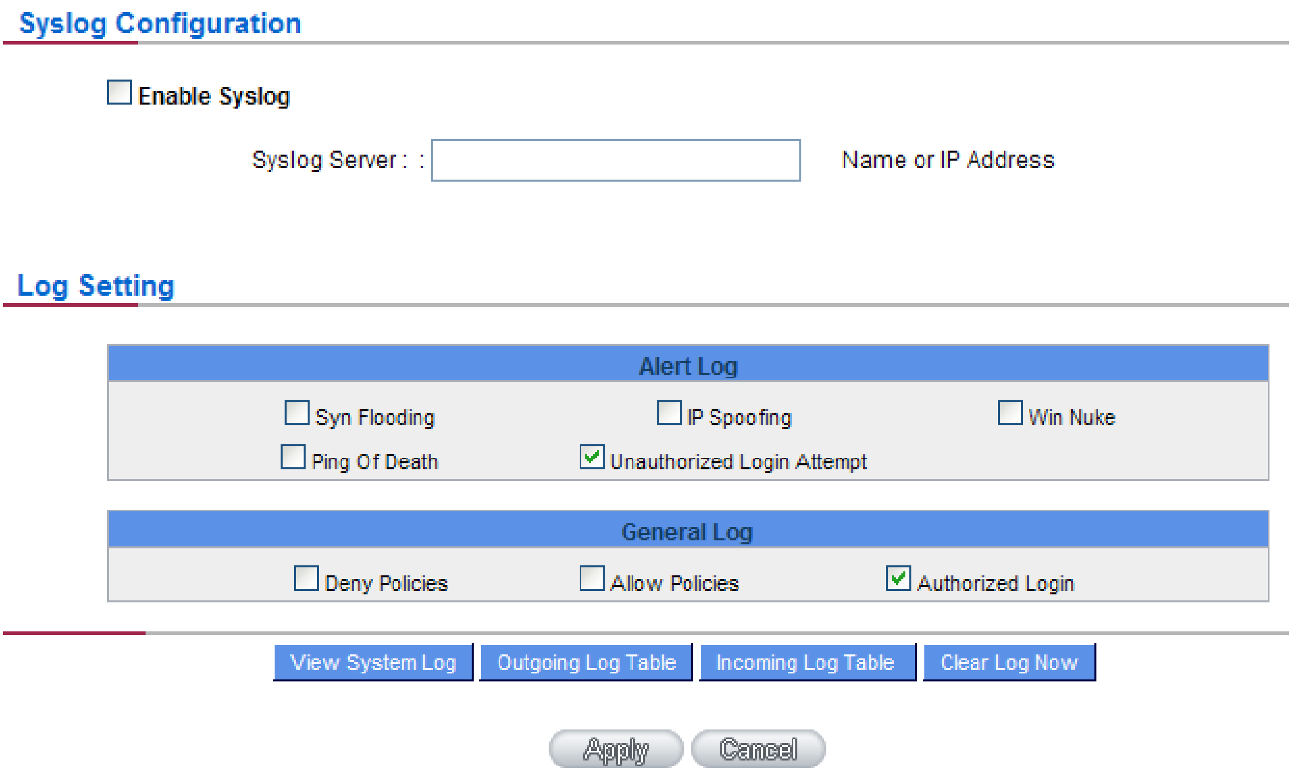
Item	Description
Operation-Slave Mode	Although working with master device, Backup device's DHCP server is disabled. LAN users need to transmit traffic through the WAN on Slave device. You should add LAN IP of Slave device into Master device DHCP server default gateway, which is DHCP server IP address. 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, Salve device should be in the same subnet, ex. 192.168.1.2.
WAN Backup (The Checked WANs are not working in this device.)	The checked WANs will works 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.
LAN Gateway Backup	Input the LAN IP of Master device. It should be different from Slave device's IP. (Must be in the same subnet.)
MAC Address of the backup device	Input the LAN MAC of Master device. It should be different from Salve device's LAN MAC.
Status	"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 14. 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.

14.1 System Log

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



Syslog Configuration

□ Enable Syslog

Syslog Server : : [   ] Name or IP Address

Log Setting

Alert Log

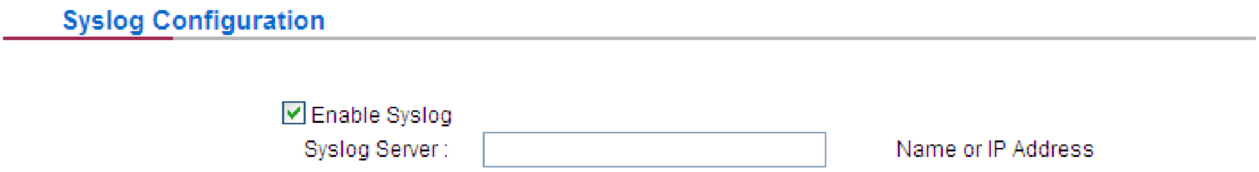
□ Syn Flooding □ IP Spoofing □ Win Nuke

□ Ping Of Death ☑ Unauthorized Login Attempt

General Log

□ Deny Policies □ Allow Policies ☑ Authorized Login

System Log



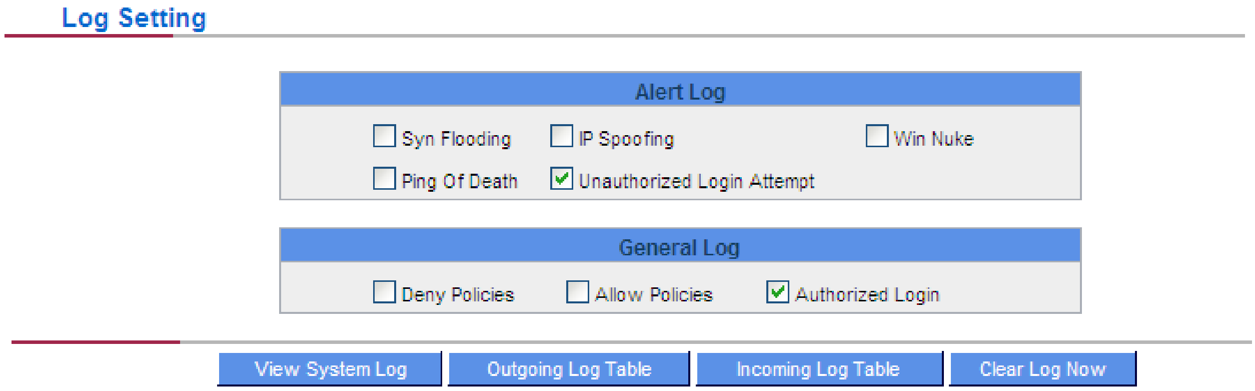
Syslog Configuration

☑ Enable Syslog

Syslog Server : [   ] Name or IP Address

Item	Description
Enabled	If this option is selected, the System Log feature will be enabled.
Syslog Server	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

□ Syn Flooding □ IP Spoofing □ Win Nuke

□ Ping Of Death ☑ Unauthorized Login Attempt

General Log

□ Deny Policies □ Allow Policies ☑ Authorized Login

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
Syn Flooding	Bulky syn packet transmission in a short time causes the overload of the system storage of record in connection information.
IP Spoofing	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.
Win Nuke	Servers are attacked or trapped by the Trojan program.
Ping of Death	The system fails because the sent data exceeds the maximum packet that can be handled by the IP protocol.
Unauthorized Login	If intruders into the device are identified, the message will be sent to the system log.

General Log

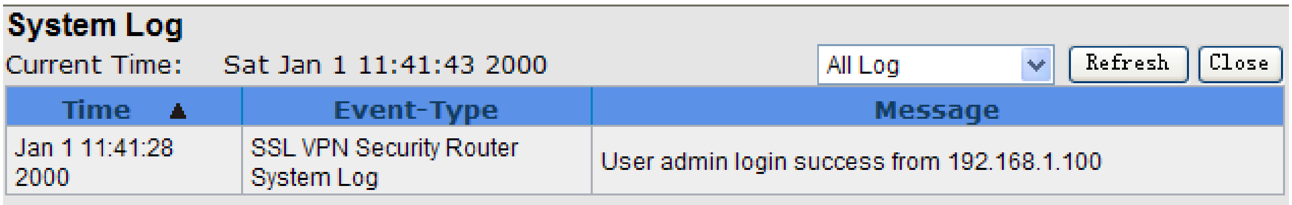
The device provides the following warning message. Click to activate the feature. System error message, blocked regulations, regulation of passage permission, system configuration change and registration verification.

Item	Description
Deny Policies	If remote users fail to enter the system because of the access rules; for instance, message will be recorded in the system log.
Allow Policies	If remote users enter the system because of compliance with access rules; for instance, message will be recorded in the system log.
Authorized Login	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

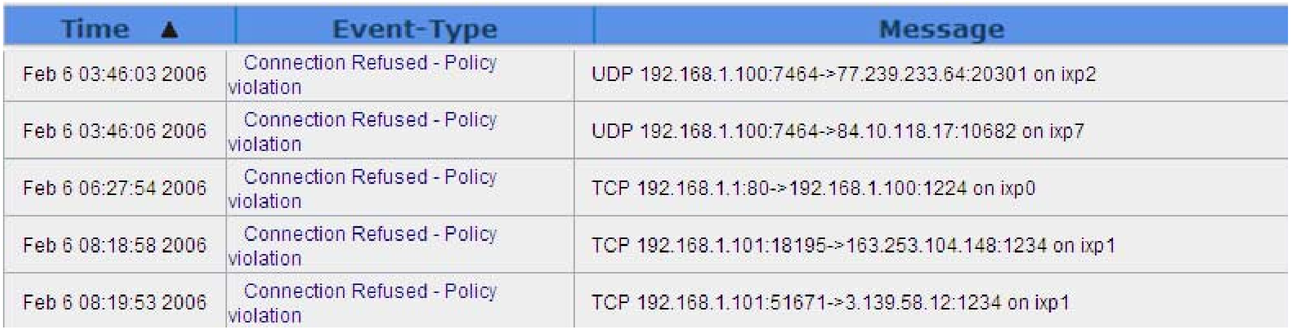
Current Time: Sat Jan 1 11:41:43 2000

All Log

Time ▲	Event-Type	Message
Jan 1 11:41:28 2000	SSL VPN Security Router System Log	User admin login success from 192.168.1.100

Outgoing Packet Log

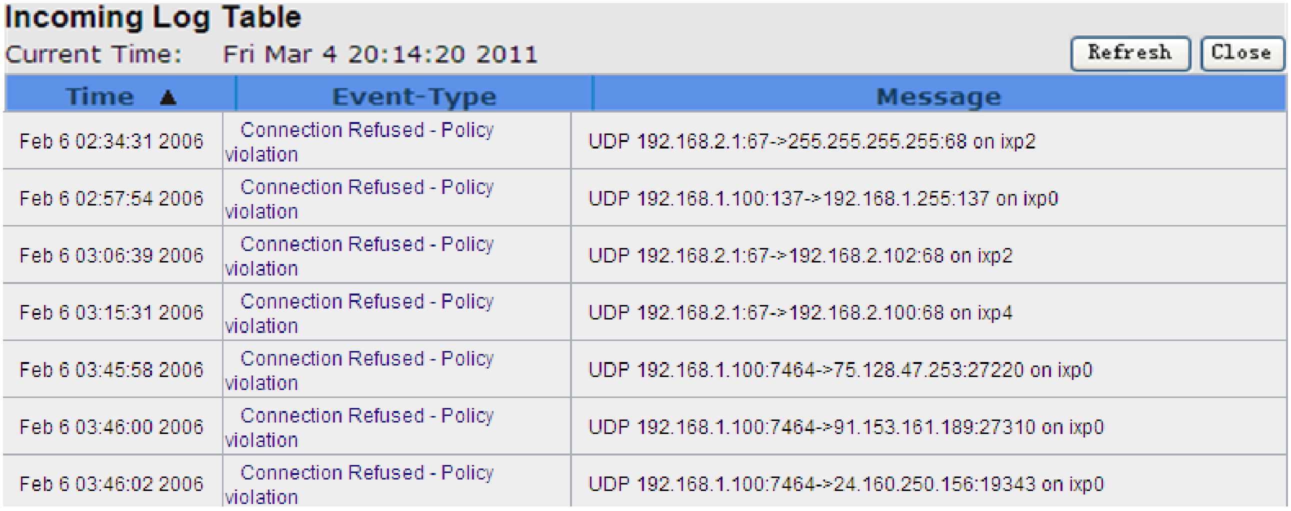
View system packet log which is sent out from the internal PC to the Internet. This log includes LAN IP, destination IP, and service port that is applied. It is illustrated as below.



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

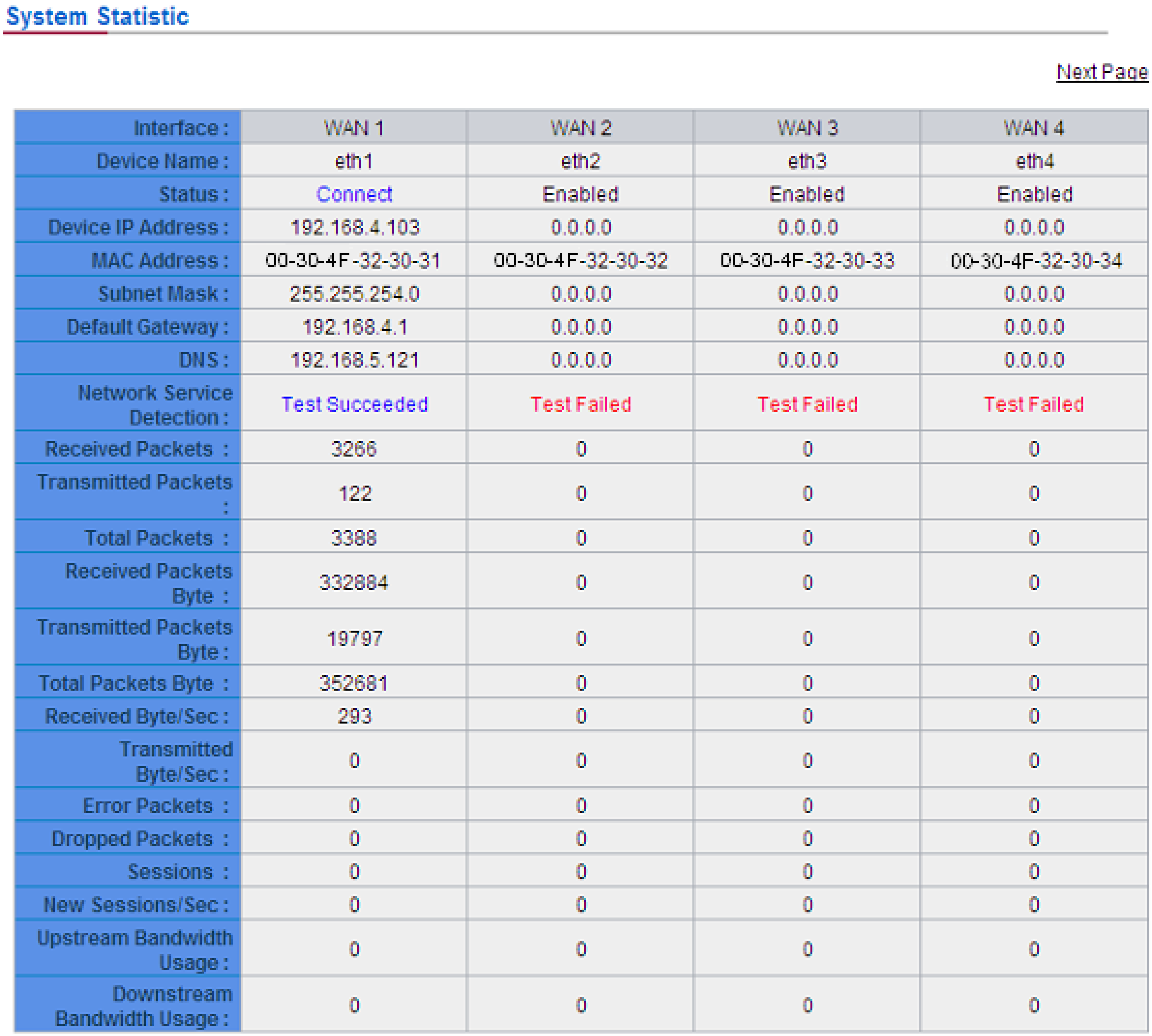
Time ▲	Event-Type	Message
Feb 6 02:34:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->255.255.255.255:68 on ixp2
Feb 6 02:57:54 2006	Connection Refused - Policy violation	UDP 192.168.1.100:137->192.168.1.255:137 on ixp0
Feb 6 03:06:39 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.102:68 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.

14.2 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 (%).



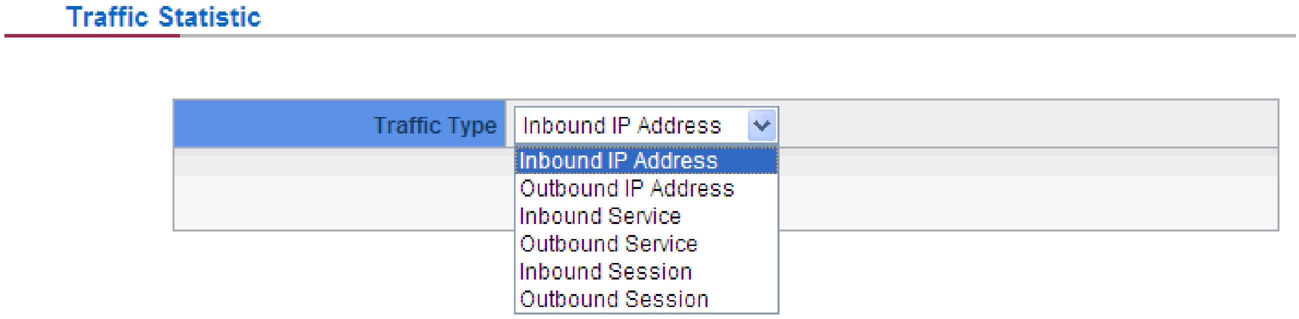
System Statistic

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 :	00-30-4F-32-30-31	00-30-4F-32-30-32	00-30-4F-32-30-33	00-30-4F-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

14.3 Traffic Statistic

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

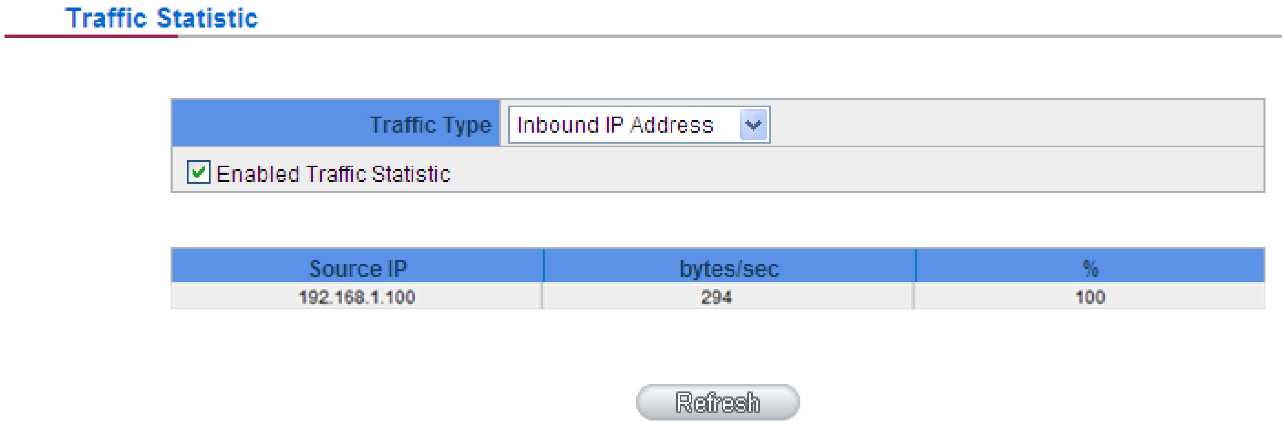


Traffic Statistic

Traffic Type: Inbound IP Address

By Inbound IP Address

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



Traffic Statistic

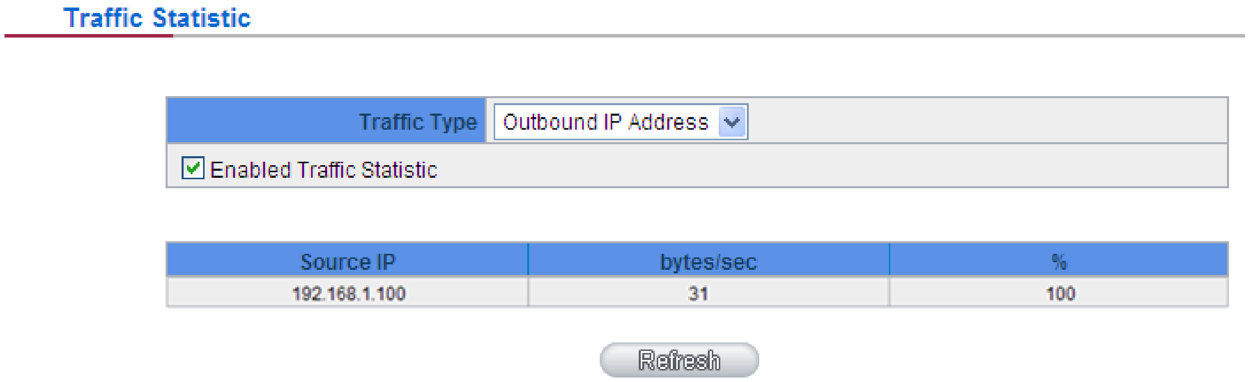
Traffic Type: Inbound IP Address

☑ Enabled Traffic Statistic

Source IP	bytes/sec	%
192.168.1.100	294	100

By outbound IP Address

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



Traffic Statistic

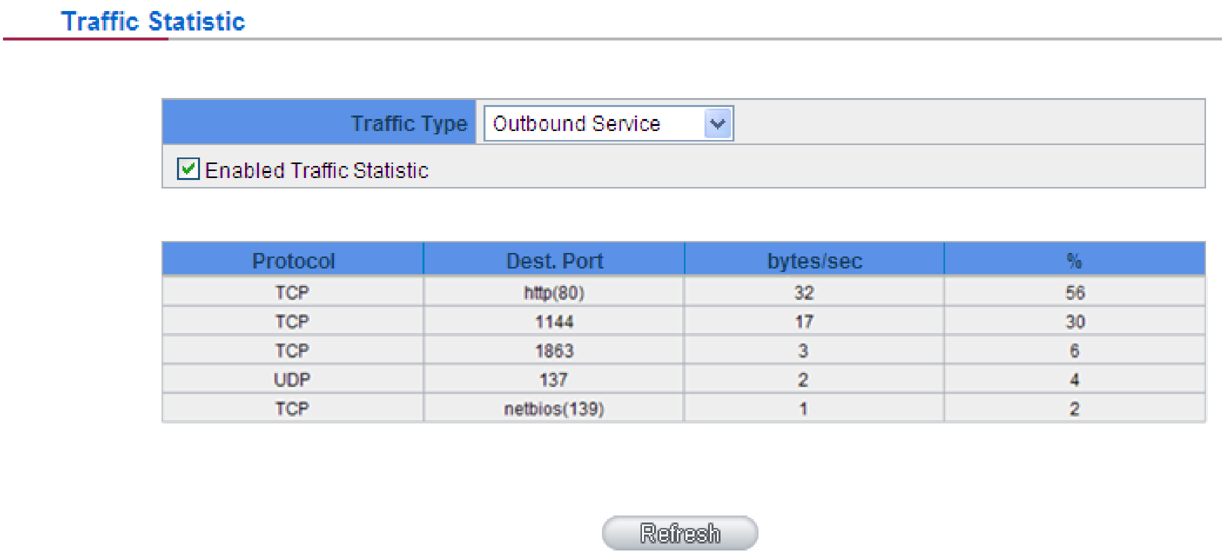
Traffic Type: Outbound IP Address

☑ Enabled Traffic Statistic

Source IP	bytes/sec	%
192.168.1.100	31	100

By Outbound Service

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



Traffic Statistic

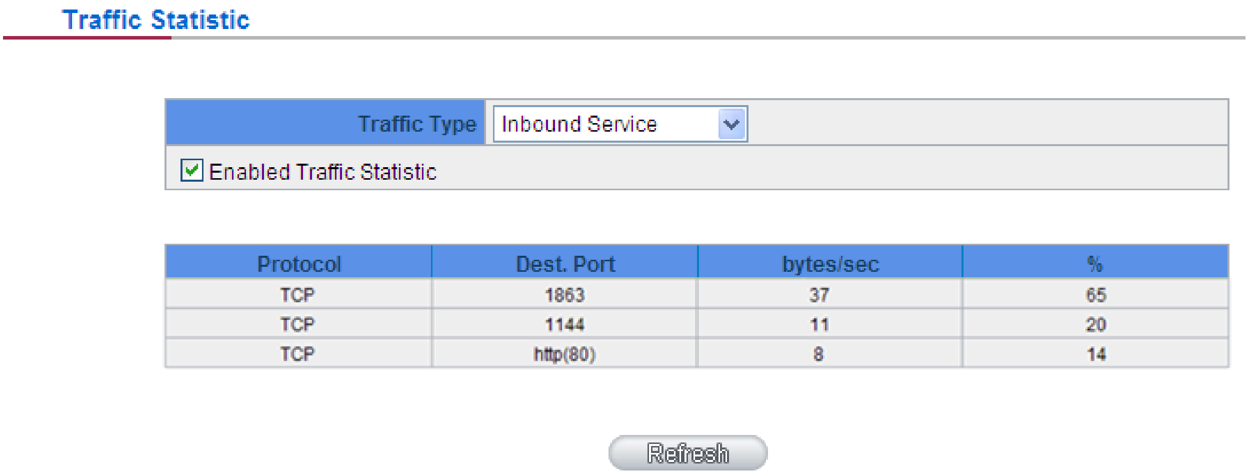
Traffic Type: Outbound Service

☑ 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 Service

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



Traffic Statistic

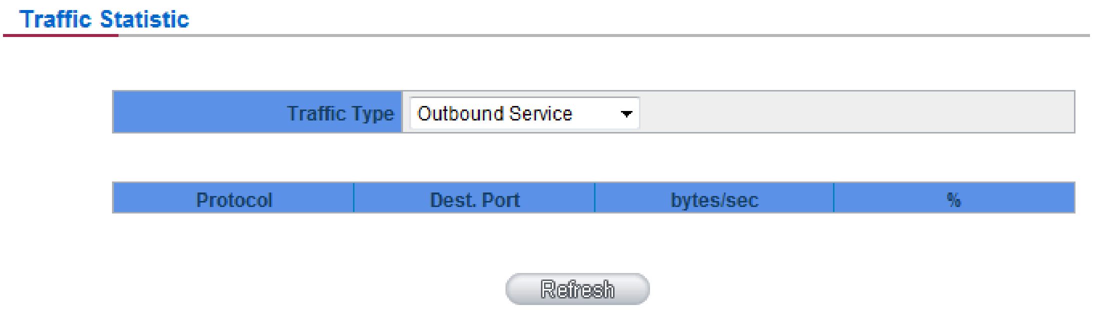
Traffic Type: Inbound Service

☑ 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.



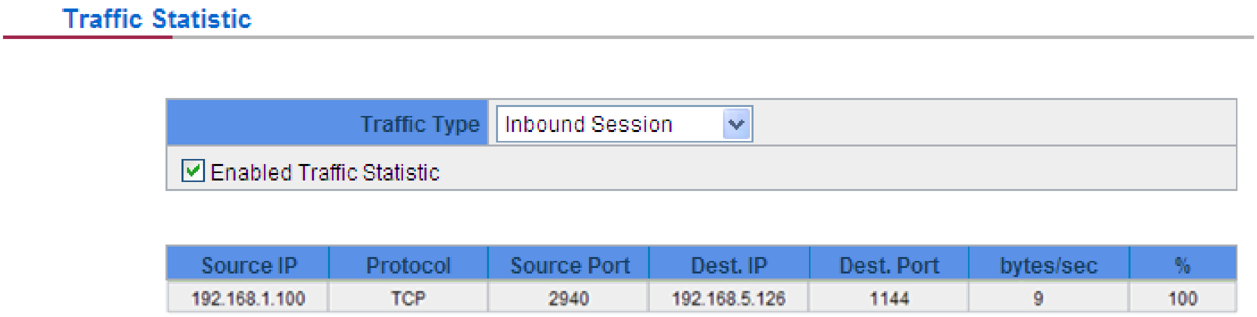
Traffic Statistic

Traffic Type: Outbound Service

Protocol	Dest. Port	bytes/sec	%

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.



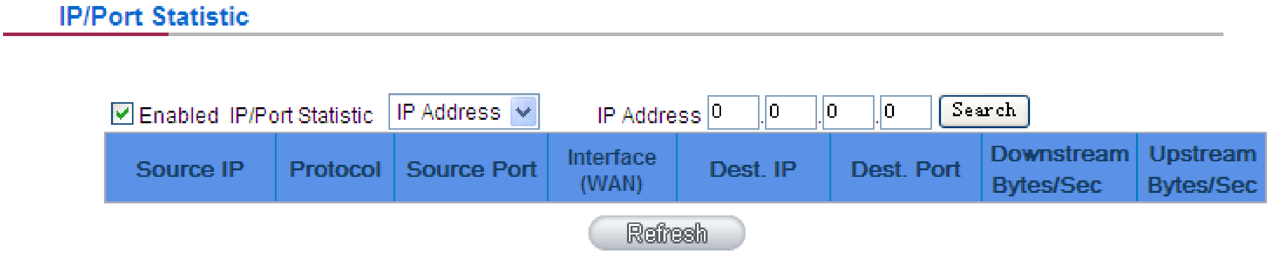
Traffic Statistic

Traffic Type	Inbound Session
☑ 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

14.4 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

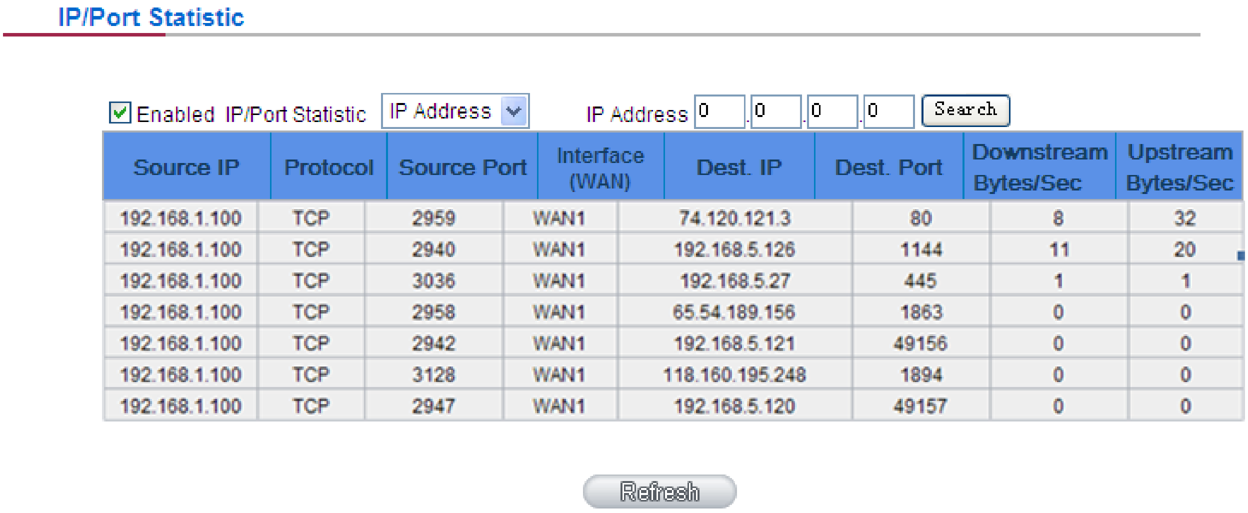
☑ Enabled IP/Port Statistic   IP Address   IP Address 0 . 0 . 0 . 0   Search

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

Refresh

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

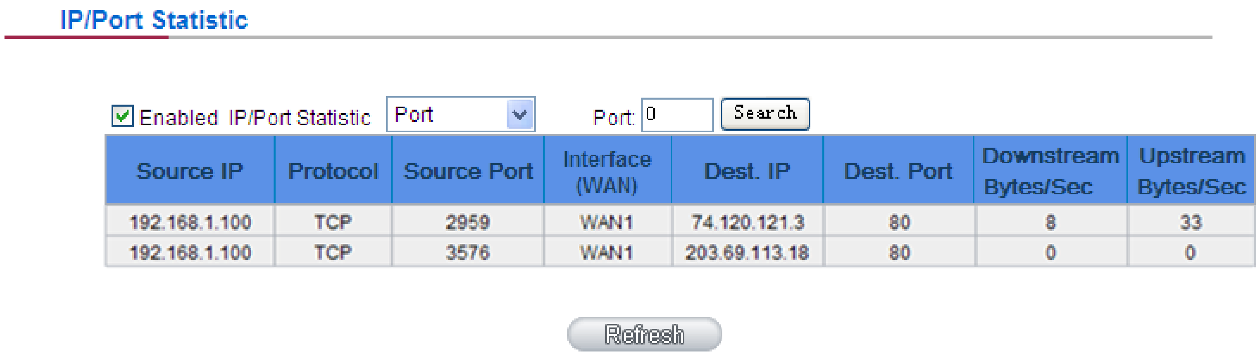
☑ Enabled IP/Port Statistic   IP Address   IP Address 0 . 0 . 0 . 0   Search

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	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

Refresh

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

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