your future life

2 WAN 4LAN
Medium Scale Multi-Wan QoS Router

Load Balancing, Bandwidth Management,
Network Security Management

English User's Manual

Index

1、Introduction

The device is a 2WAN / 4LAN Medium Scale Multi-WAN QoS Router. It can meet the needs of both small and medium-scale enterprises, internet cafes, etc.

It's an efficiently integrated new generation firewall device. The device has a high-efficiency Intel IXP 266MHz processor embedded. With high-speed SDRAM and Flash memory, the device brings users high-endurance and high networking efficiency.

One of the Dual-WAN ports is a configurable DMZ/WAN port, which supports DHCP fixed IP, PPPoE, bridge connecting mode, port binding, static routing, dynamic routing, NAT, one to one NAT, PAT, MAC Clone, as well as DDNS. As for the LAN port, it has 4 built-in 10/100 Base-T/TX Ethernets (RJ45). It supports Port Forwarding, Microsoft UPnP, Mirror Port, VLAN, Multi Subnet, and transparent bridge mode of internet IP. Internet IPs can also be used in intranet.

It supports two kinds of Load Balance mode, by IP and auto Load Balance. The device has strong bandwidth management capability. It also has built-in management fuction to block QQ, MSN, Skype, and figure out that the bandwidth is occupied by BT, Xunlei, P2P and video downloading. The device utilizes active detection technology SPI (Stateful Packet Inspection). The SPI firewall functions mainly within the network by dynamically inspecting each link. The SPI firewall also has a warning function for the application process; therefore, it can refuse links to non-standard communication protocols. With the function, we can prevent from Worm, ARP or any kind of attack efficiently.

With the Web-based UI which supports Chinese and English, the device supports remote management and it enables users easy to use. It also supports on-line firmware upgrade, Configuration backup, SNMP, Syslog, E-mail Alert and traffic statistic to fulfill users' demand.

You can log on to the Web site www.Qno.com.tw, and find technical support information on the appendix or contact with our technical support engineers. You can also get the newest Qno's product information and application examples from the web site.

2、Hardware Installation

2.1 Indicators on Front Panel

LED Status- Indicators on front panel

LED	Color	Indication
Power	Green	Green LED on: Power ON.
DIAG (Diagnostics)	Amber	Amber LED on: System self-test is running. Amber LED off: System self-test is completed successfully.
Link/ACT	Green	Green LED on: Ethernet connection is fine. Green LED blinking: Packets are transmitting through Ethernet port.
Speed	Amber	Amber LED on: Ethernet is running at 100Mbps. Amber LED off: Ethernet is running at 10Mbps.
WAN	Green	Green LED on: WAN port is designated. Green LED off: LAN port is designated.

Hardware Reset Button

Action	Description
Press Reset Button For 5 Secs	Warm Start DIAG indicator: Amber LED flashing slowly.
Press Reset Button Over 10 Secs	Factory Default DIAG indicator: Amber LED flashing quickly.

Replacing System Built-in Battery

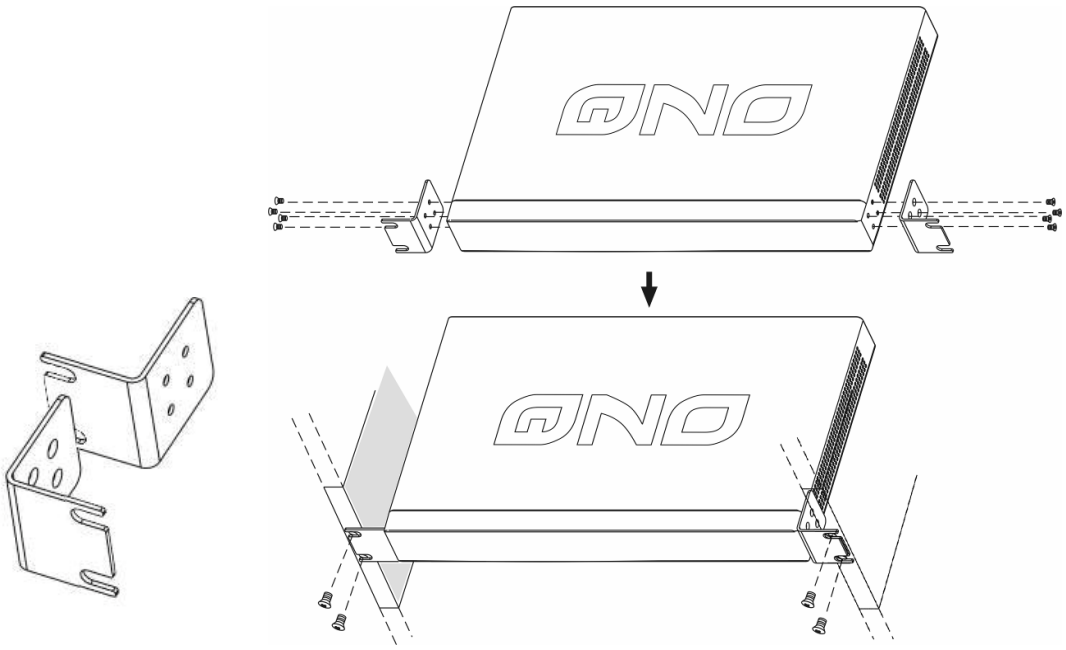
A system timing battery is built into the device. The lifespan of the battery is about 1~2 years. If the battery life is over or it can not be charged, the device will not be able to record time correctly, nor synchronize with internet NTP time server. Contact system supplier for information on how to replace the battery.

Attention!
Do not replace the battery yourself, otherwise irreparable damage to the product may be caused.

Installing the Device on a Standard 19” Rack

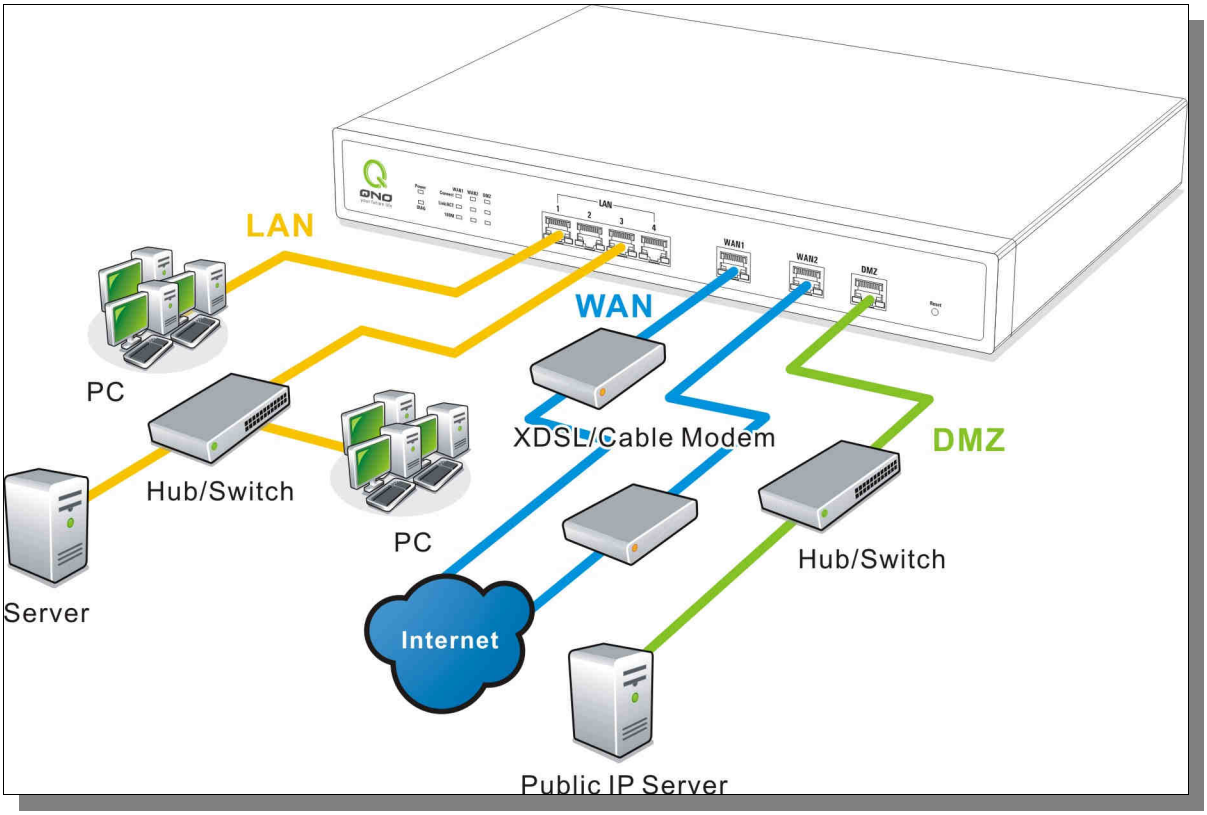
We suggest to either place the device on a desk or install it in a rack with attached brackets. Do not place other heavy objects together with the device on a rack. Overloading may cause the rack to fail, thus causing damage or danger.

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.



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.

2.2 Connecting This Device with Network



WAN Connection:

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

LAN Connection:

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

DMZ port:

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

3、Log In and Set Up

Input **User name** and **Password** (as per above image), and then click "OK". Both default user name and password are "**admin**". It is strongly recommended that the user changes the password.

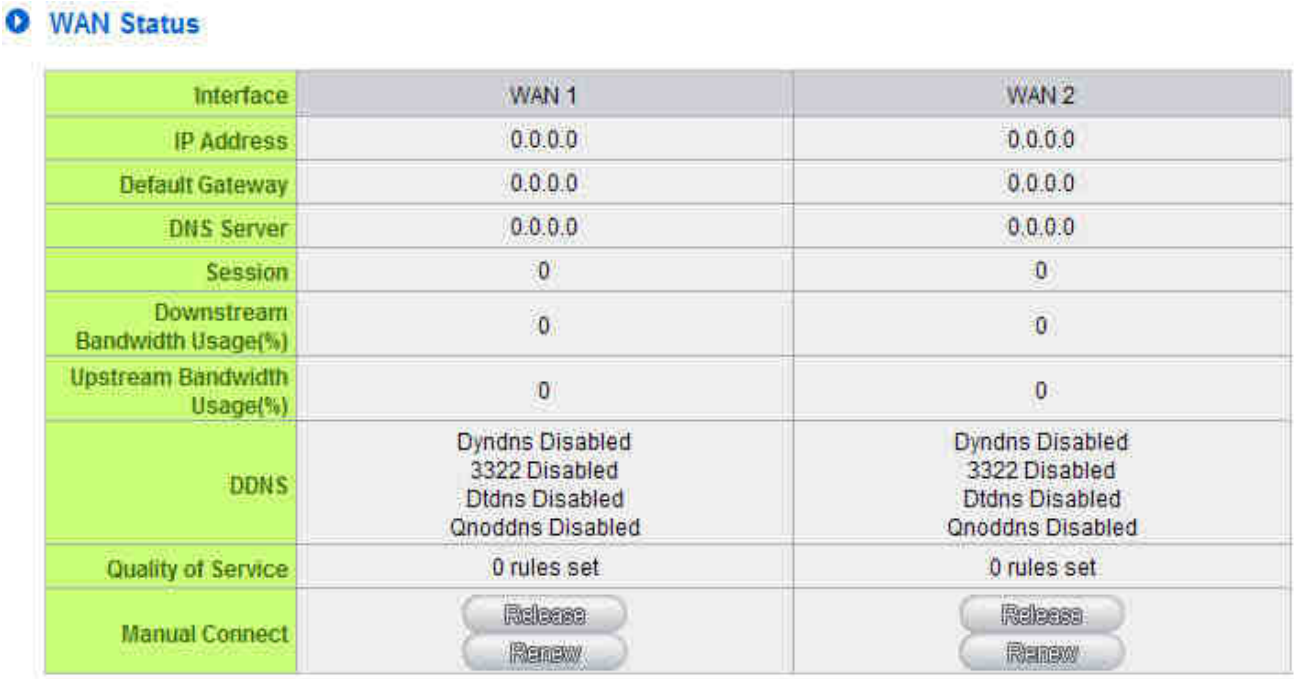
4、Basic Setting and Network Management

In this chapter, we are going to introduce the basic settings and management for WAN and LAN, and the advanced management function, as well as setting up the intranet through DHCP.

4.1 Home Page

In the Home page, all the device parameters and status are listed for users' reference. For detailed settings, click each parameter or status hyperlink below: the relevant set-up tab will be loaded for users to choose their management options. Three language versions, **Simplified Chinese**, **Traditional Chinese** and **English**, are offered in this page. Click the language version that suits you. The seleted tab will automatically change color to blue.

4.1.1 WAN Status



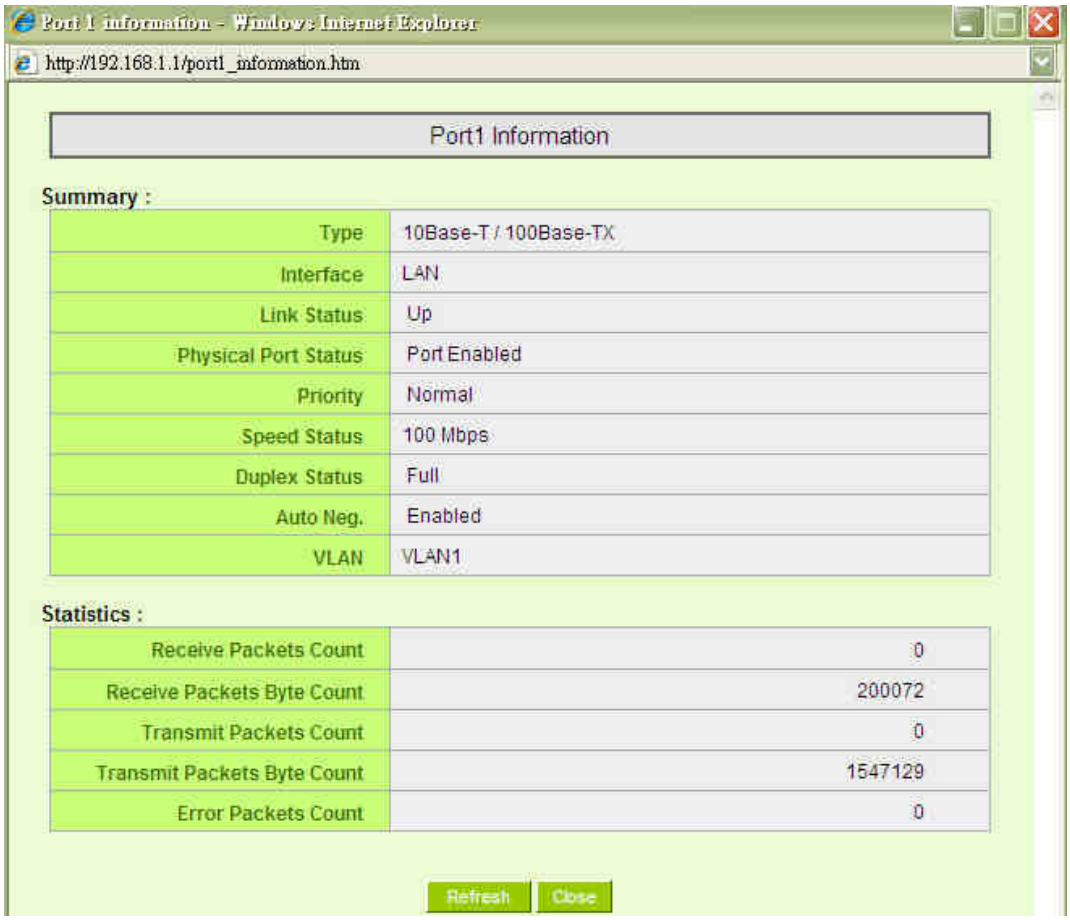
Interface	Specifies each WAN.
IP Address	Indicates the current IP configuration for each port.
Default Gateway	Indicates the current Gateway IP configuration. Click the hyperlink to enter and manage the configuration.
DNS Server	Indicates the current DNS IP configuration.
Session	Indicates the current session number of each WAN.

Downstream Bandwidth Usage(%)	Indicates the current downstream bandwidth usage of each WAN.
Upstream Bandwidth Usage(%)	Indicates the current upstream bandwidth usage of each WAN.
DDNS	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 IP configuration for DMZ port.

4.1.2 Physical Port Status

Physical Port Status

Port ID	1	2	3	4	Internet / DMZ	Internet
Interface	LAN				WAN 2	WAN 1
Status	Connect	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.

The current port setting status information will be shown in the Port Status Table. Examples: Network connection, port (on or off), priority (high or normal), connection speed (10Mbps or 100Mbps), duplex status (half-duplex or full duplex), and auto negotiation (Enabled or Disabled).

The status of the number of packets and Bytes receiving/transmitting as well as error percentage of packets and Bytes through respective ports, will be shown in each port status table (as above).

4.1.3 System Information

Device IP Address/ Subnet Mask

Identifies the current device IP address and subnet mask.

Working Mode

Indicates the current working 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.

4.1.4 Firewall Status

FirewallStatus

Firewall	Status
SPI (Stateful Packet Inspection)	On
DoS (Denial of Service)	On
Block WAN Request	Off
Prevent ARP Virus Attack	Off
Remote Management	Off
Access Rule	12 rules set

SPI (Stateful Packet Inspection):

Indicates whether SPI (Stateful Packet Inspection) is on or off. The default configuration is "Off".

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 number of activated access rules.

4.1.5 Log Setting Status

Syslog Server	Indicates if Syslog Server is Enabled or Disabled.
Email Alert	Indicates if Email Alert is Enabled or Disabled.

4.2 Password and Time

4.2.1 Password

This is an advanced management tool for the device. The default password of the host is "admin". Users can change the password after configuration has been completed. Remember to click "**Apply**" when the configuration data has been completed.

User Name:	The default is "admin".
Old Password:	Input the original password.
New User Name:	Input the new user name.
New Password:	Input the changed password.
Confirm New Password:	Input the new password again for verification.

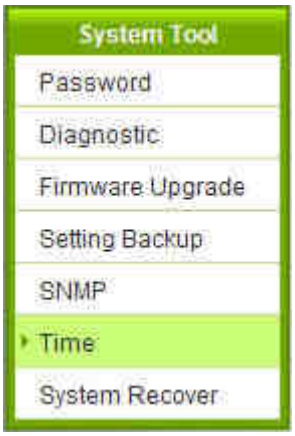
After the changes are completed, click **"Apply"** to save the configuration, or click

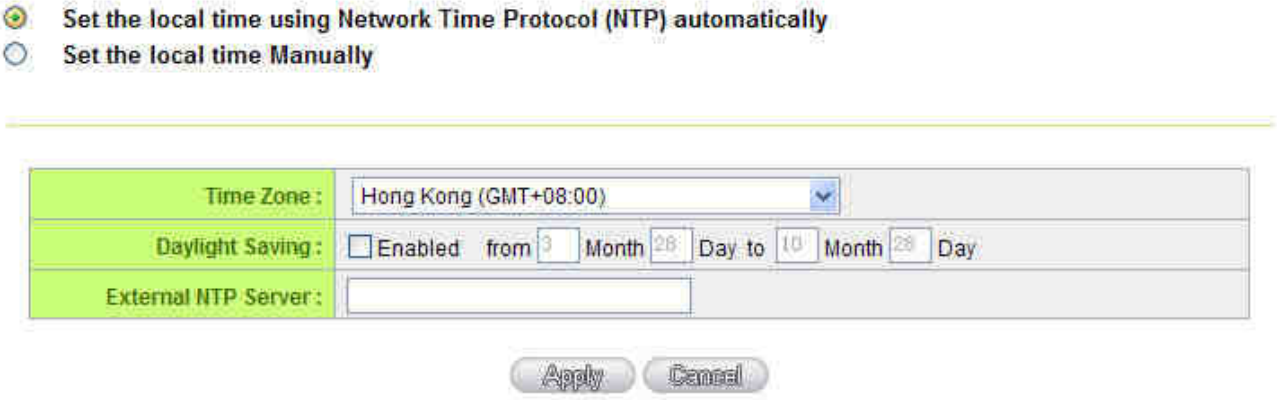
"Cancel" to leave without making any change.

4.2.2 Time

A function to calculate the correct time is available with the device. Users can either select the embedded NTP Server synchronization function or set up a time reference. This function enables users to 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.

Configuring Automatic Synchronize With NTP Function

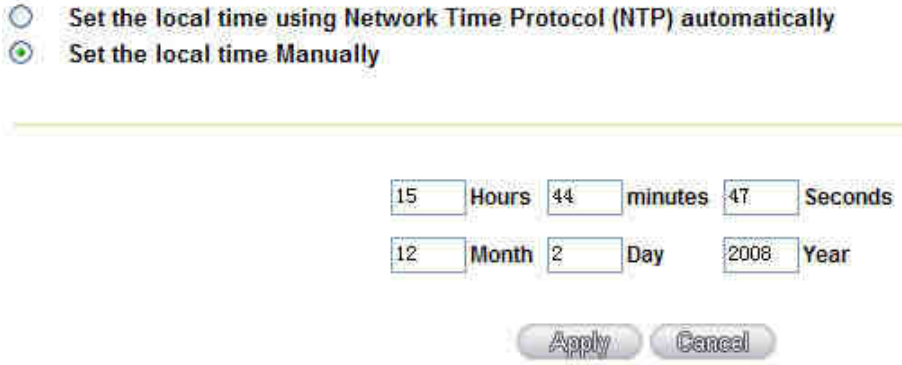




Select the time zone from the "**Time Zone**" pull-down option list. If there is **Daylight Saving Time** in the area, input it. The device will adjust the time for the Daylight Saving period automatically. If users have their own "**Time Server Address**", input the Server's IP address.

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

Input Date and Time Manually

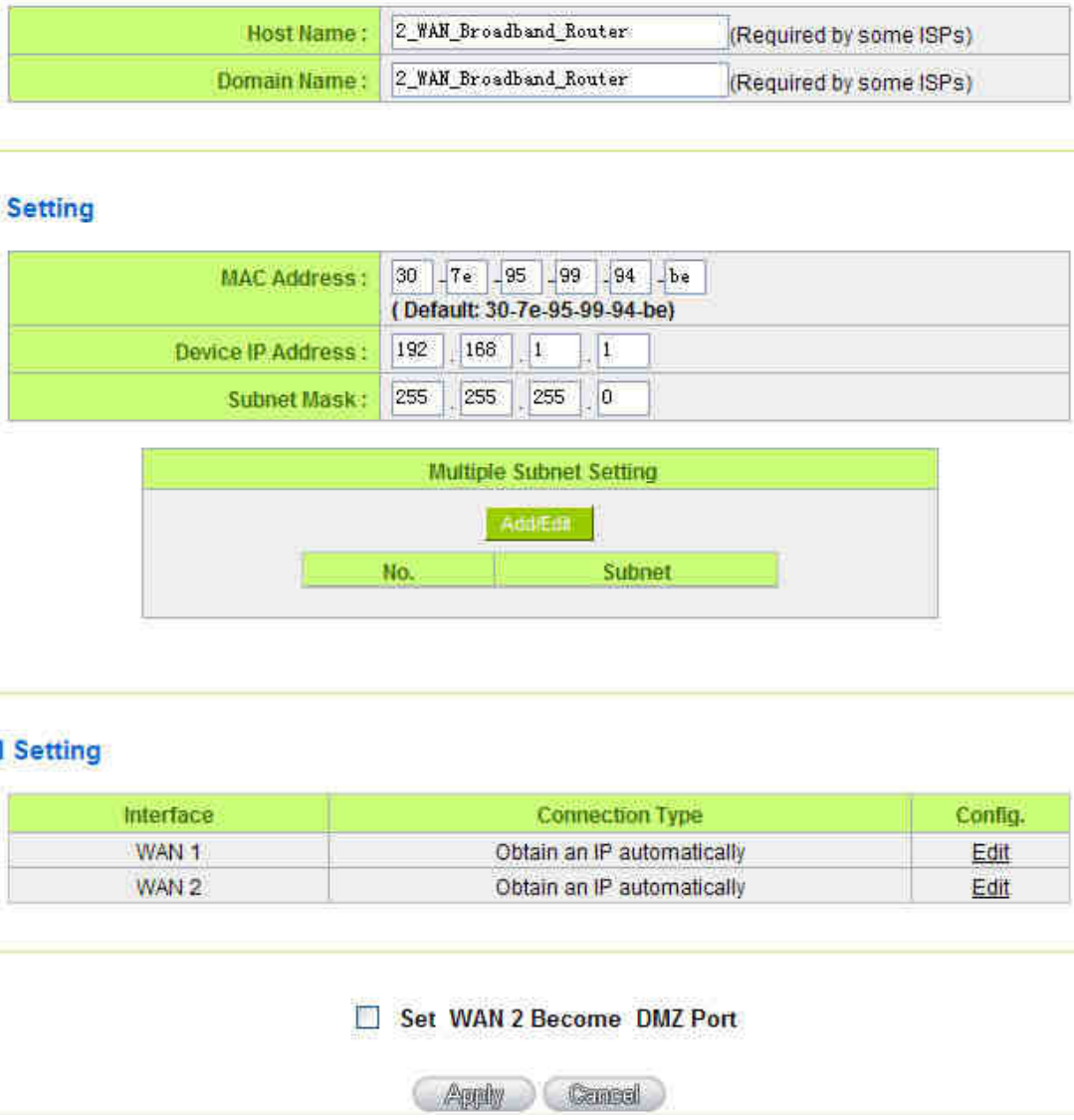


Input the correct date and time in the boxes.

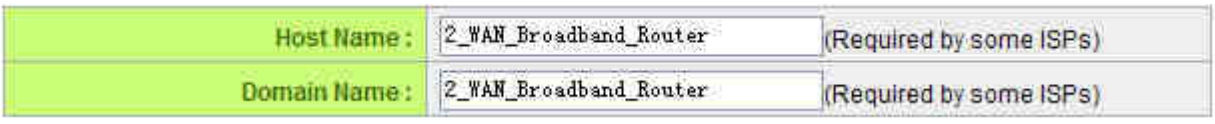
After the changes are completed, click "**Apply**" to save the configuration, or click "**Cancel**" to leave without making any changes.

5、Network

5.1 Network Connection



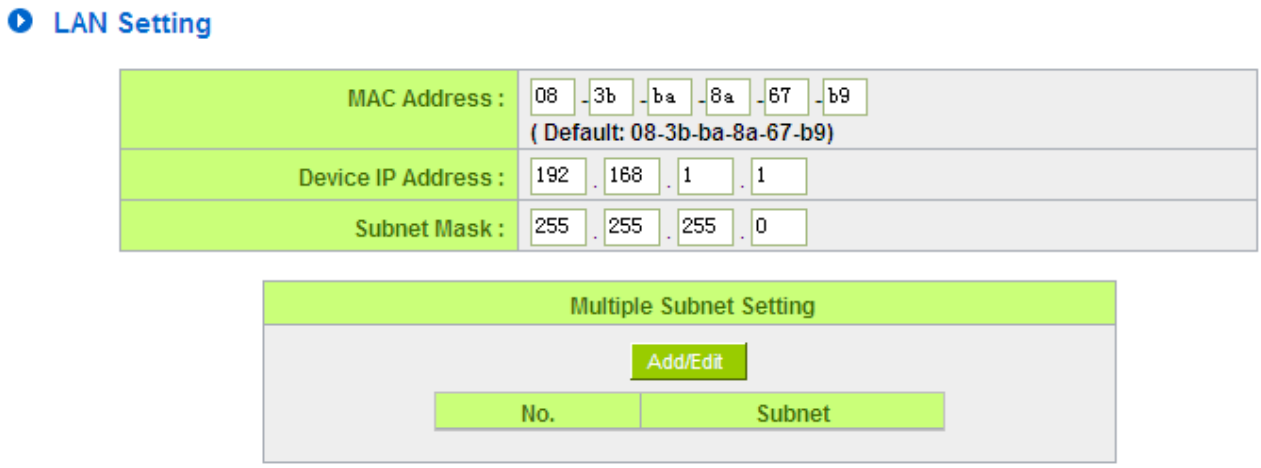
5.1.1 Host Name and Domain Name



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.

5.1.2 LAN Setting



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

In addition, the function of the MAC address is for the users' convenience. If a static ARP has been configured in the Intranet PC, it is not necessary to reconfigure the static IP for the original PC. All that is necessary is to modify the static ARP IP to map with the MAC.

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

Multiple Subnet Setting

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.

Click "**Add/Edit**" to enter the configuration page, as shown in the following figure. Input the hrespective IP addresses and subnet masks.

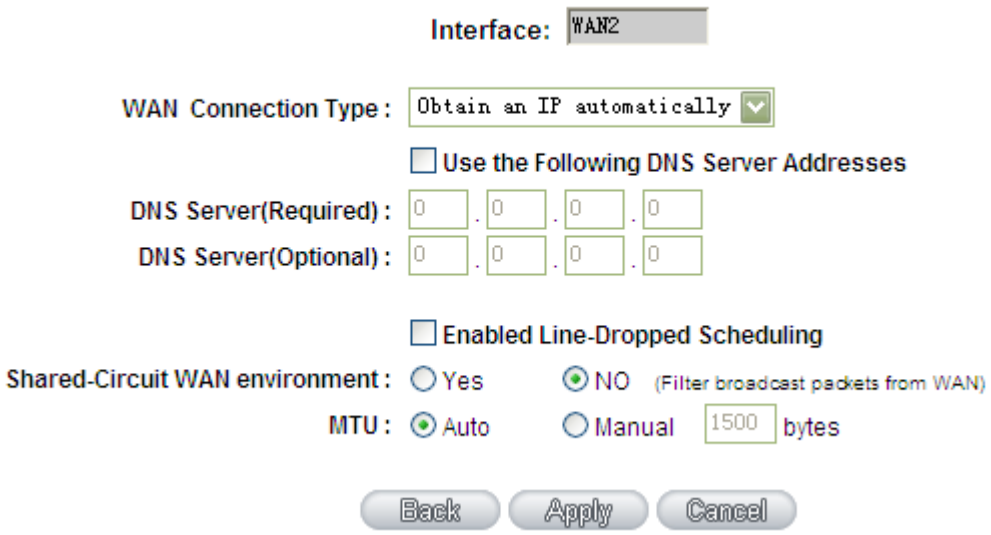
5.1.3 WAN Setting

Please choose how many WAN ports you prefer to use:	Select how many WANs to be configured. The default is four. User can change the number based on the needs.
Interface:	An indication of which port is connected.
Connection Type:	WAN configuration and internet connection status. This can be classified into five categories: ● Obtain an IP automatically ● Static IP connection ● PPPoE (Point-to-Point Protocol over Ethernet) ● PPTP (Point-to-Point Tunneling Protocol) ● Transparent Bridge
Config.:	A modification in an advanced configuration: Click **Edit** to enter the advanced configuration page.

WAN and the Internet Connection Configuration

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.



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 is two IP groups.
Enable Line-Dropped Scheduling:	The WAN interruption 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 interrupted from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN interruption, all the external connections that go through this WAN will be interrupted too. Only after the interrupted lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of interruptions, 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 interruption can be minimized.
Line-Dropped Period	Input the time rule for interruption of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be interrupted before the newly added connections should go through another WAN to connect with the Internet.
Shared- Circuit WAN environment	Choose whether this WAN share bandwidth with others from the same circuit or not

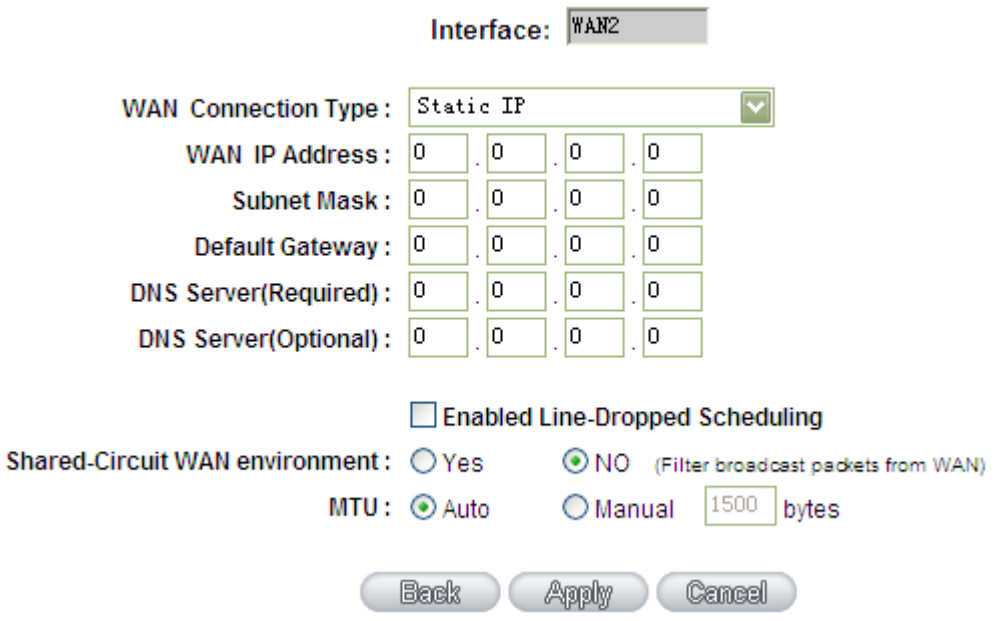
MTU	Input the packet maximum transmission unit of this WAN

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

Static IP

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

Attention: Even if ISP offers a static IP address, it might be an automatic mode to obtain a DHCP IP or to obtain a PPPoE dial-up IP. Although the IP address obtained will be the same each time, users still must select the correct connecting mode!



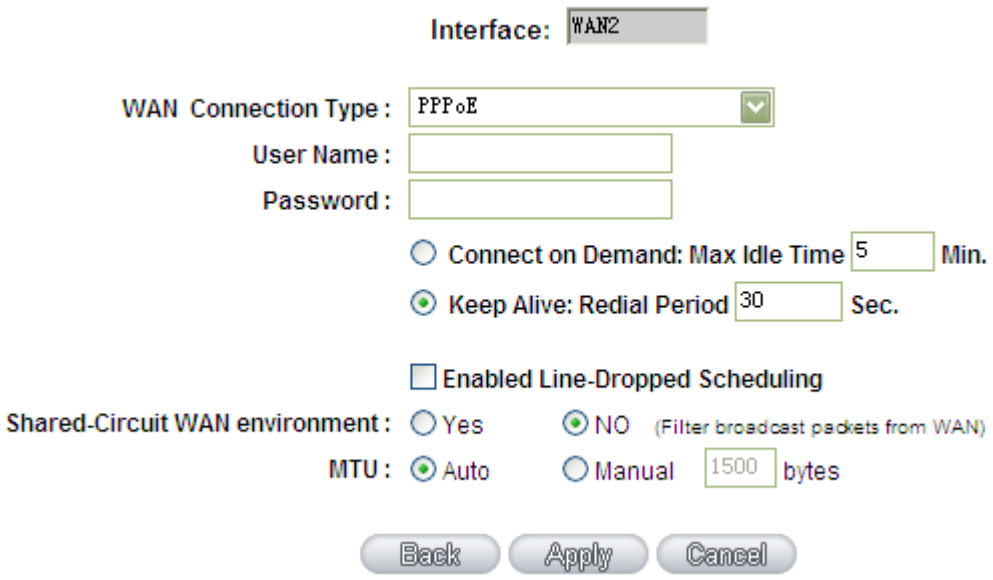
WAN IP address:	Input the available static IP address issued by ISP.
Subnet Mask:	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway:	Input the default gateway issued by 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 interruption 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 interrupted from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN interruption, all the external connections that go through this WAN will be interrupted too. Only after the interrupted lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of interruptions, 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 interruption can be minimized.
Line-Dropped Period	Input the time rule for the interruption of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be interrupted before the newly added connections should go through another WAN to connect with the Internet.
Shared- Circuit WAN environment	Choose whether this WAN share bandwidth with others from the same circuit or not
MTU	Input the packet maximum transmission unit of this WAN

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.



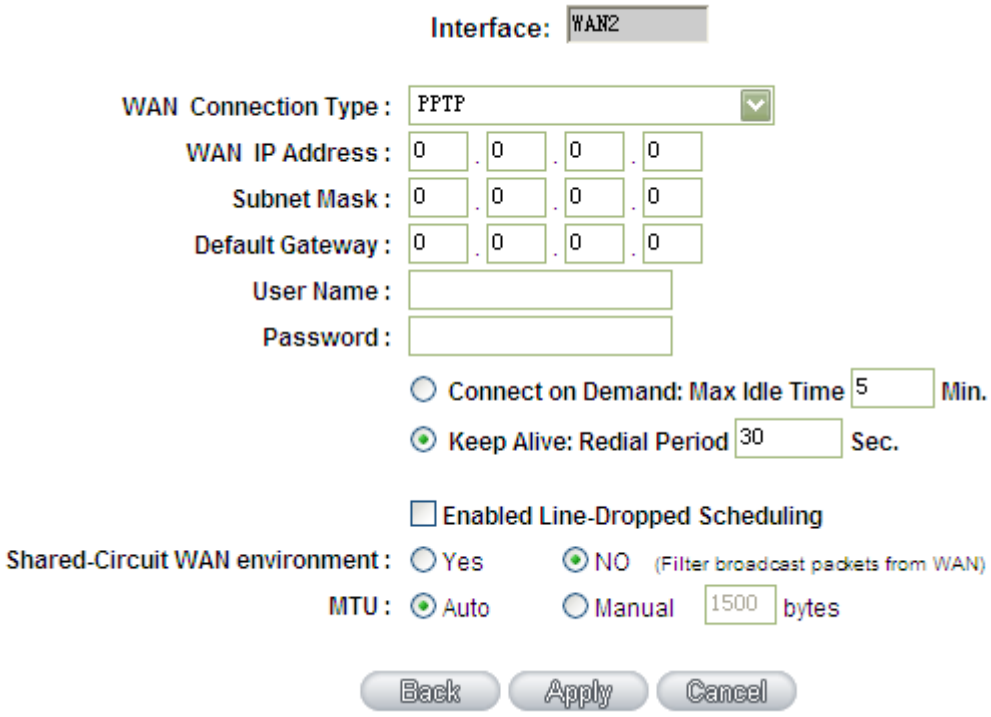
User Name:	Input the user name issued by ISP.
Password	Input the password issued by ISP.
Connect on Demand:	This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. 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 interrupted. It also enables a user to set up a time for redialing. The default is 30 seconds.
Enable Line-Dropped Scheduling	The WAN interruption 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 interrupted from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN interruption, all the external connections that go through this WAN will be interrupted too. Only after the interrupted lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of interruptions, users can activate this function to arrange new

	connections through another WAN to the Internet. In this way, the effect of any interruption can be minimized.
Line-Dropped Period	Input the time rule for the interruption of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be interrupted before the newly added connections should go through another WAN to connect with the Internet.
Shared- Circuit WAN environment	Choose whether this WAN share bandwidth with others from the same circuit or not
MTU	Input the packet maximum transmission unit of this WAN

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 (mostly for European countries).



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 interrupted. Users can set up the redialing time. The default is 30 seconds.
Enable Line-Dropped Scheduling	The WAN interruption 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 interrupted from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN interruption, all the external connections that go through this WAN will be interrupted too. Only after the interrupted lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of interruptions, 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 interruption can be minimized.
Line-Dropped Period	Input the time rule for the interruption of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be interrupted before the newly added connections should go through another WAN to connect with the Internet.

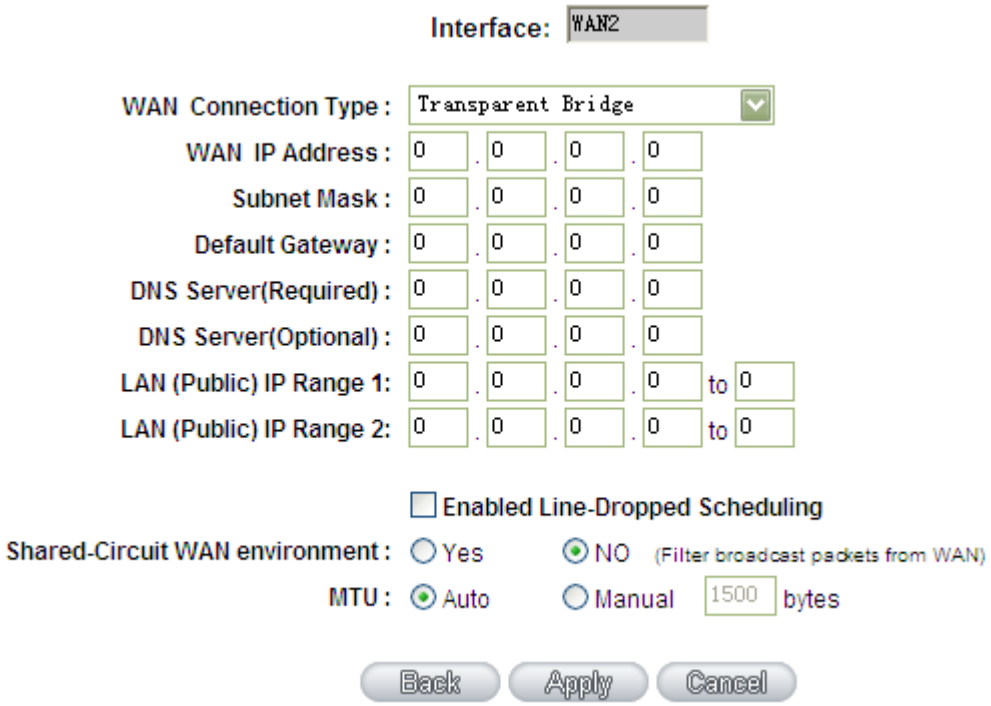
Shared- Circuit WAN environment	Choose whether this WAN share bandwidth with others from the same circuit or not
MTU	Input the packet maximum transmission unit of this WAN

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 IPs are applied as Internet IPs, and users don't want to substitute private network IPs for all Intranet IPs (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 IPs 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.



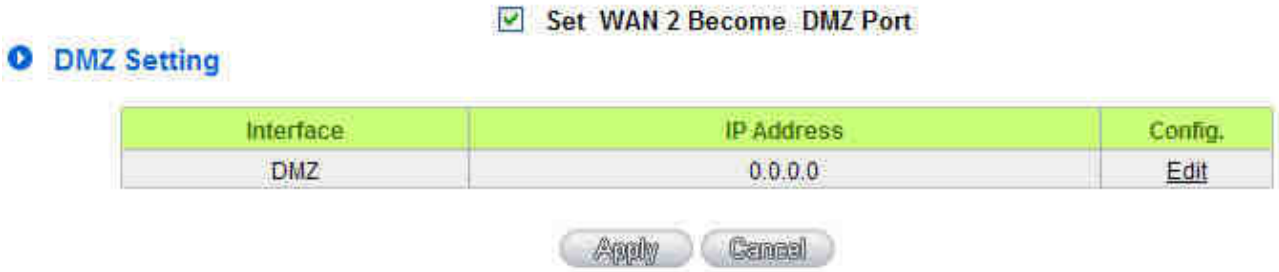
WAN IP Address:	Input one of the static IP addresses issued by ISP.

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 interruption 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 interrupted from 0:00 am to 6:00 am. Although there is a standby system in the device, at the moment of WAN interruption, all the external connections that go through this WAN will be interrupted too. Only after the interrupted lines are reconnected can they go through the standby system to connect with the Internet. Therefore, to avoid a huge number of interruptions, users can activate this function to arrange new connections through another WAN to the Internet. In this way, the effect of any interruption can be minimized.
Line-Dropped Period	Input the time rule for the interruption of this WAN service.
Line-Dropped Scheduling	Input how long the WAN service may be interrupted before the newly added connections should go through another WAN to connect with the Internet.
Shared-Circuit WAN environment	Choose whether this WAN share bandwidth with others from the same circuit or not
MTU	Input the packet maximum transmission unit of this WAN

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

DMZ Setting

For some network environments, an independent 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 DMZ ports for users to set up connections for servers with real IPs. The DMZ ports act as bridges between the Internet and LANs.

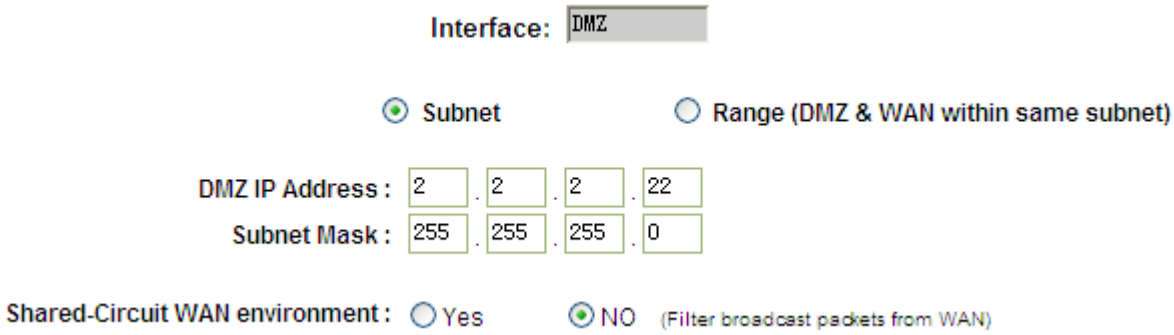


Set WAN 2 Become DMZ Port	To set WAN 2 as DMZ port.
Interface:	Indicated as a DMZ port.
IP address:	Indicates the current default static IP address.
Config.:	Indicates an advanced configuration modification: Click Edit to enter the advanced configuration page.

The DMZ configuration can be classified by Subnet and Range:

Subnet : The DMZ and WAN located in different Subnets

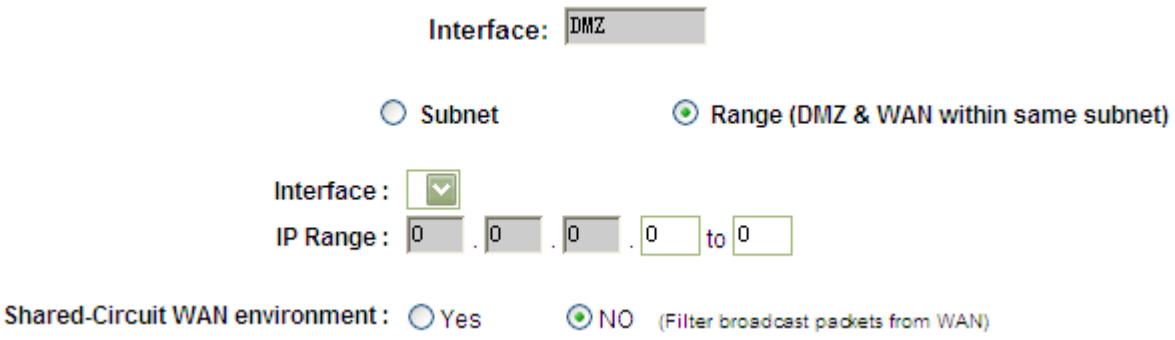
For example: If the ISP issued 16 real IPs: 220.243.230.1-16 with Mask 255.255.255.240, users have to separate the 16 IPs into two groups: 220.243.230.1-8 with Mask 255.255.255.248, and 220.243.230.9-16 with Mask 255.255.255.248 and then set the device and the gateway in the same group with the other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



DMZ IP Address:	Input the IP address located in the DMZ port.
Subnet Mask:	Input the subnet mask which maps to the IP address of DMZ port.
Shared-Circuit WAN environment:	Choose whether this WAN share bandwidth with others from the same circuit or not

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

Range: DMZ and WAN within same Subnet



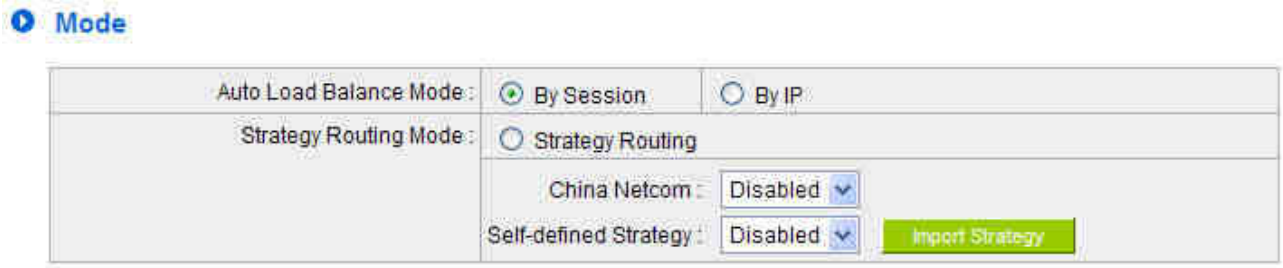
Interface:	To select a WAN port as a static IP.
IP Range:	Input the IP range located at the DMZ port.
Shared-Circuit WAN environment:	Choose whether this WAN share bandwidth with others from the same circuit or not

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

5.2 Traffic Management

5.2.1 Load Balance Mode

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. **(Please refer to 5.2.3 for an explanation of bandwidth configuration)**.

- **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 IPs 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 **5.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router modes with Protocol Binding.

Exclusive Mode (Remaining WAN Balance)

This mode enables users to assign specific intranet IPs, destination application service ports or destination IPs to go through an assigned WAN for external connection. After being assigned, the specific WAN will only support those assigned Intranet IPs, specific destination application service ports, or specific destination IPs. 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.

- **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 IP amount 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 IPs 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 **5.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding.

Strategy Routing Mode

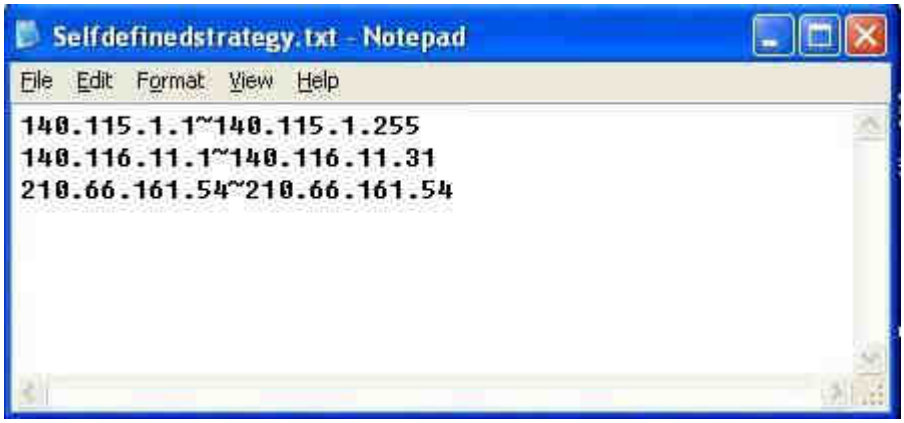
If strategy Routing is selected, the device will automatically allocate external connections based on routing policy (Shunting between Telecom and Netcom is to be used in China) embedded in the device. All you have to do is to select the WAN which is

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 shunted.

Import Strategy:

A shunting policy can be defined by users too. In the "Import Strategy" window, select the WAN or WAN group (ex. WAN 1) to be assigned and click the "Import IP Range" button; the dialogue box for document importation will be displayed accordingly. A policy document is an editable text document. It may contain a destination IP users designated. After the path for document importation has been selected, click "Import", and then at the bottom of the configuration window click "Apply". The device will then dispatch the traffic to the assigned destination IP through the WAN (ex. WAN 1) or WAN grouping users designated to the Internet.

To build a policy document users can use a text-based editor, such as Notepad, which is included with Windows system. Follow the text format in the figure below to key in the destination IPs users want to assign. For example, if the destination IP address range users want to designate is 140.115.1.1 ~ 140.115.1.255, key in 140.115.1.1 ~ 140.115.1.255 in Notepad. The next destination IP address range should be keyed in the next line. Attention! Even if only one destination IP address is to be assigned, it should follow the same format. For example, if the destination IP address is 210.66.161.54, it should be keyed in as 210.66.161.54~210.66.161.54. After the document has been saved (the extension file name is .txt), users can import the IP range of self-defined strategy.



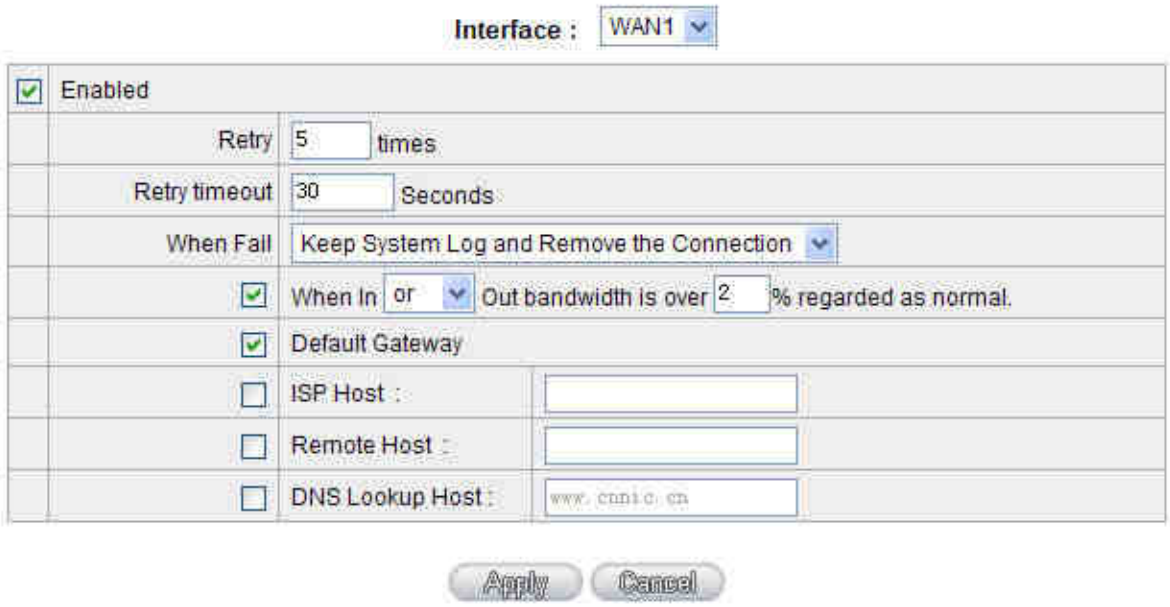
Note!

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

5.2.2 Network Service Detection

This is a detection system for network external services. If this option is selected, information such "**Retry Count**" 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:	To select a WAN port for the NSD system.
Retry Count:	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 Interrupted".
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 interrupted, 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 interrupted. (2) 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.
Detecting Feedback Servers:	
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 Server:	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 Server:	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).
Use DNS server for Domain Name Service:	This is the detect location for DNS. (Only a web address such as 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.

After the changes are completed, click "**Apply**" to save the network configuration

modification; or click "**Cancel**" to leave without making any change.

Note!
In the load balance mode for Assigned Routing, the first WAN port (WAN1) will be saved for the traffic of the IPs or the application service ports that are not assigned to the other WAN (WAN2). Therefore, in this mode, we recommend assigning one of the connections to the first WAN. When the other WAN (WAN2) is 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 the other WAN in turn. For example, the traffic will be shifted to WAN2.

5.2.3 Protocol Binding

Bandwidth Configuration

Automatic load balance ratio will be made according to the upstream bandwidth users input for the two WAN ports. For instance, if the upstream bandwidth for both WANs is 512Kbit/sec, the automatic balance ratio will be 1:1. If one WAN upstream bandwidth is 1024Kbit/sec while the other is 512Kbit/sec, the automatic balance ratio will be 2:1. Therefore, to ensure the load can be really balanced, please input the actual upstream and downstream bandwidth. In addition, the data users input will also affect the QoS configuration. Please refer to **7.1.2. QoS Configuration.**

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

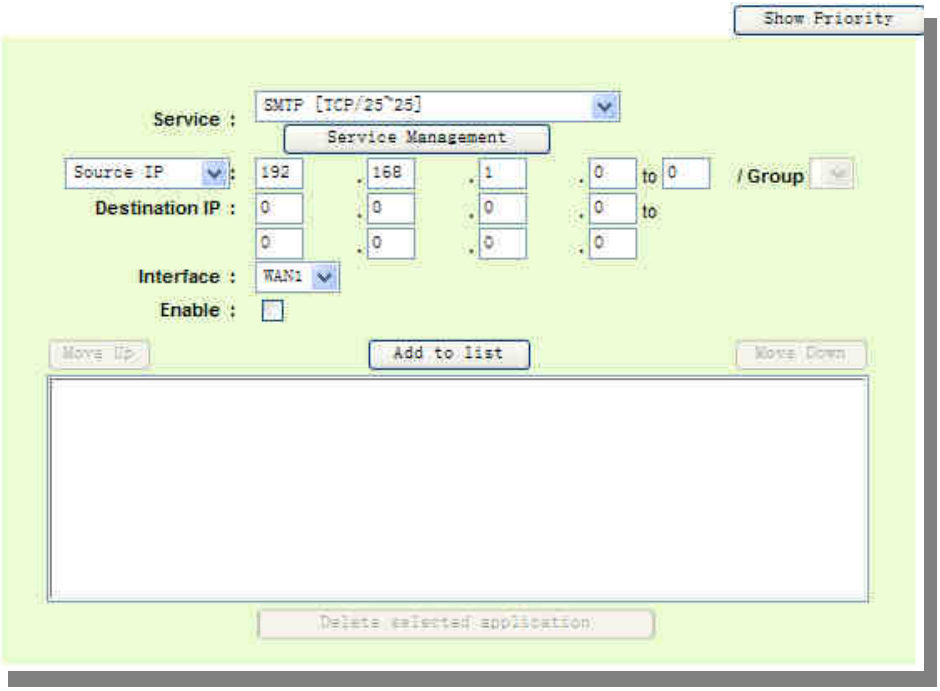
The Maximum Bandwidth provided by ISP

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

Auto Load Balance Mode

Users can define specific IPs or specific application service ports to go through a user-assigned WAN for external connections. For any other unassigned IPs and services,

WAN load balancing will still be carried out.



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.

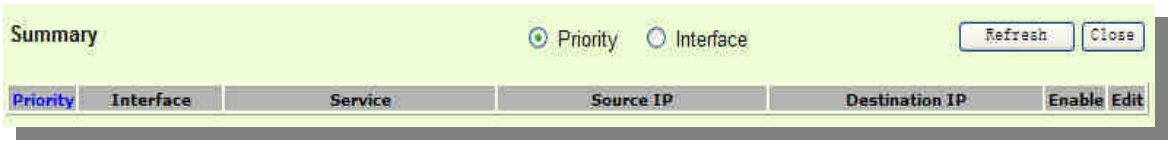
Interface:	Select the WAN for which users want to set up the binding rule.
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Delete selected application:	To remove the rules selected from the Service List.
Moving Up & Down:	The priority for rule execution depends on the rule order 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.

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

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

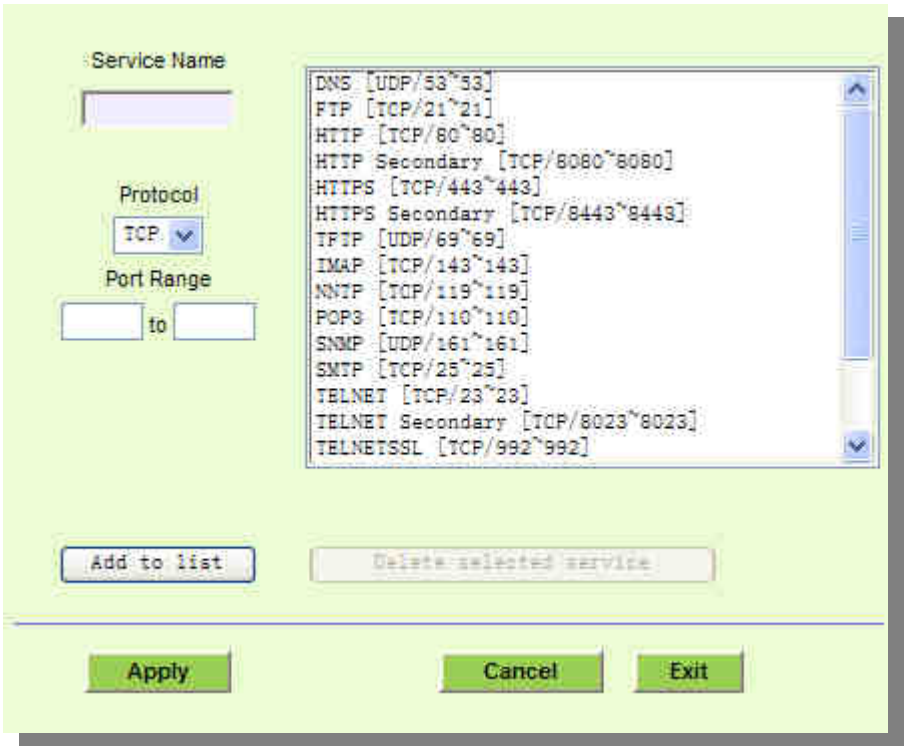
Priority

Click the "Priority" button at the right top. A dialogue box as shown in the following figure will be displayed. Users can choose to sort the list by priorities or by interface. Click "Refresh" and the page will be refreshed; click "Close" and the dialogue box will be closed.



Add Or Remove Service Ports

If the Service Port users want to activate is not in the list, users can click "Add or Remove Service Ports from "Service Management" to arrange the list, as described in the following:



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.
Exit:	To quit this configuration window.

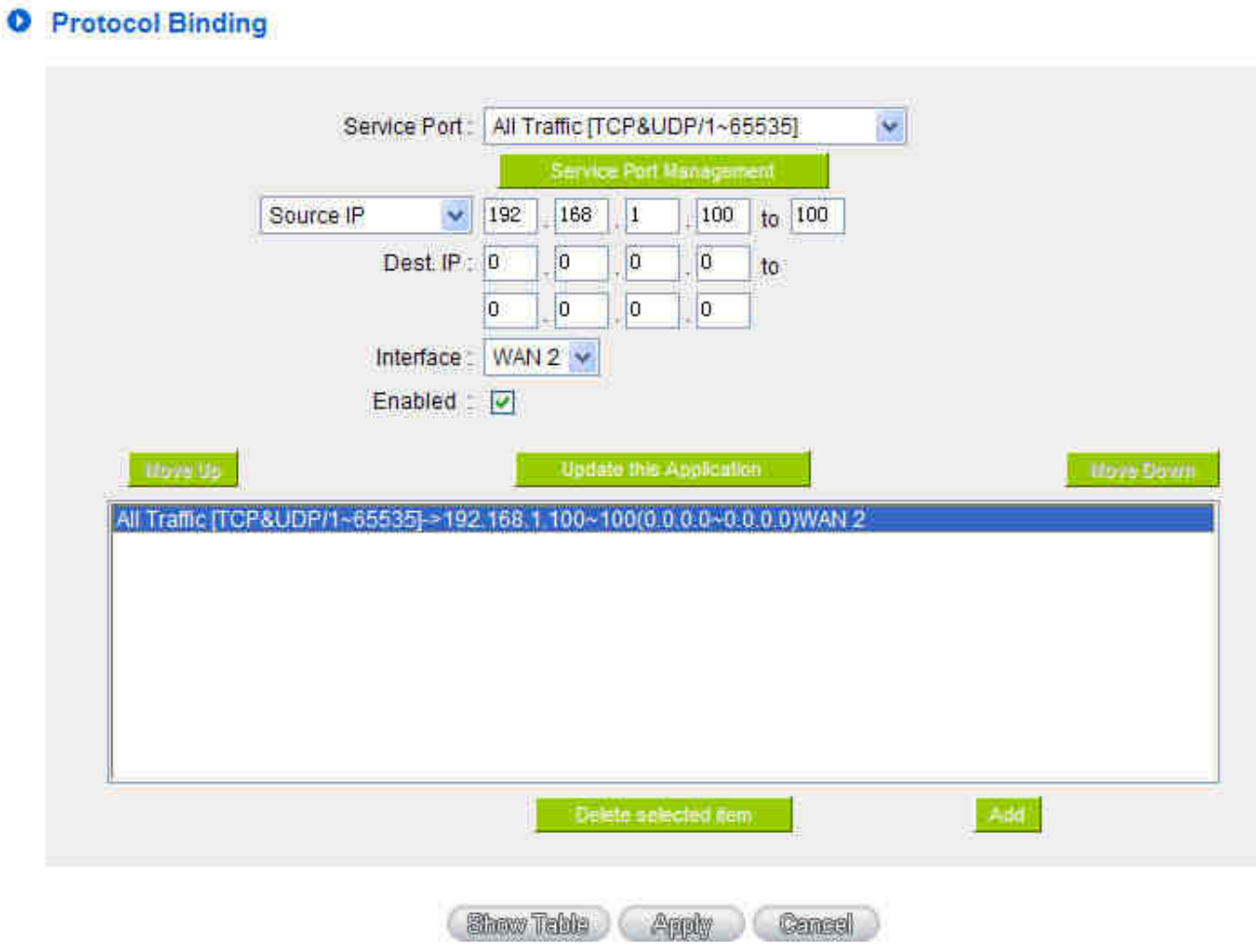
Auto load Balance Setting when enabled

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 IPs to specific destination

application service ports or assign specific destination IPs to a WAN users choose for external connections.

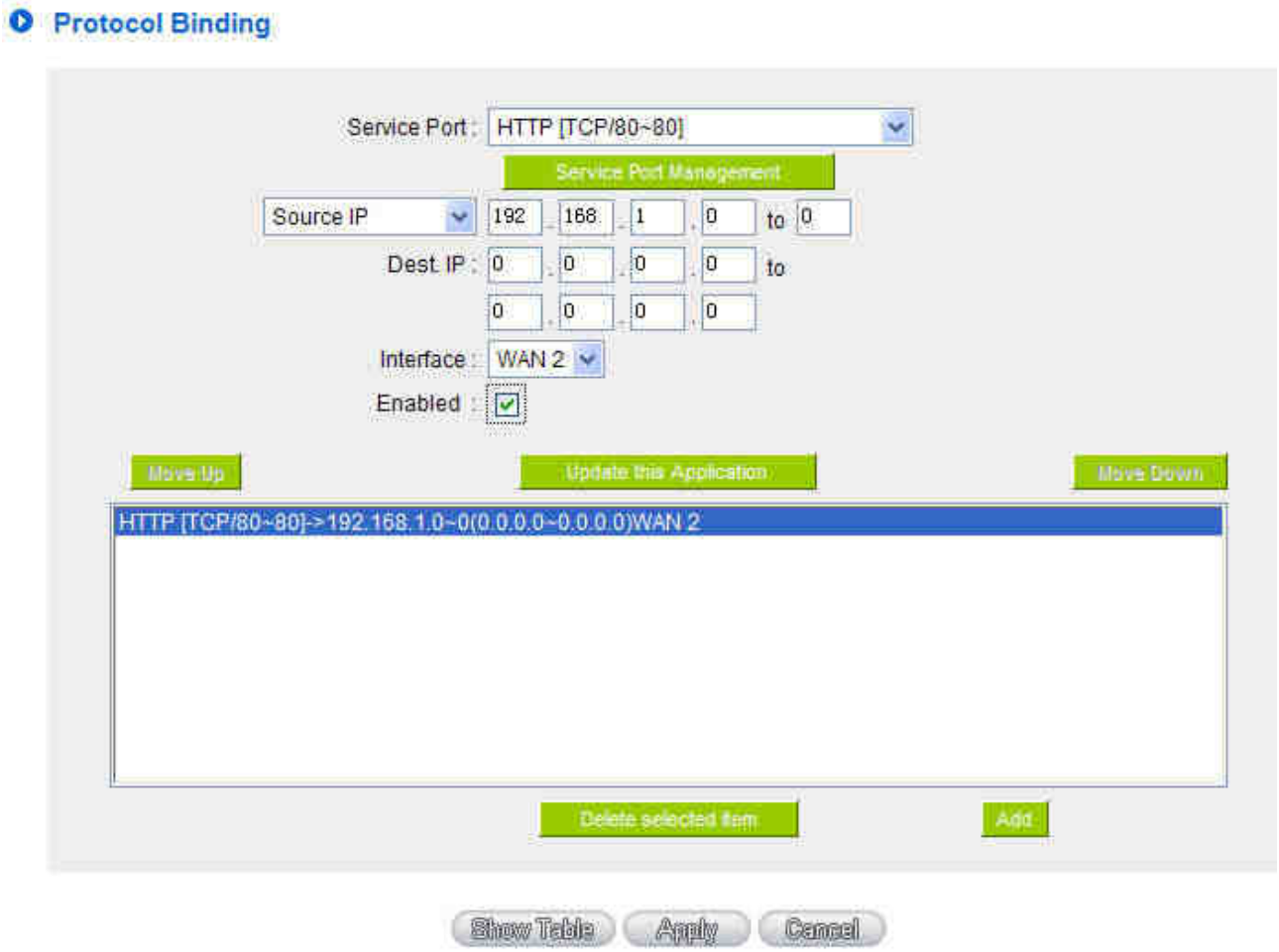
Example 1: How do I set up Auto Load Balance Mode to assign the Intranet IP 192.168.1.100 to WAN2 for the Internet?

As in the figure below, select "All Ports" 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.



Example 2: How do I set up Auto Load Balance Mode to keep Intranet IP 192.168.1.150 ~ 200 from going through WAN2 en route to 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 IPs 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.

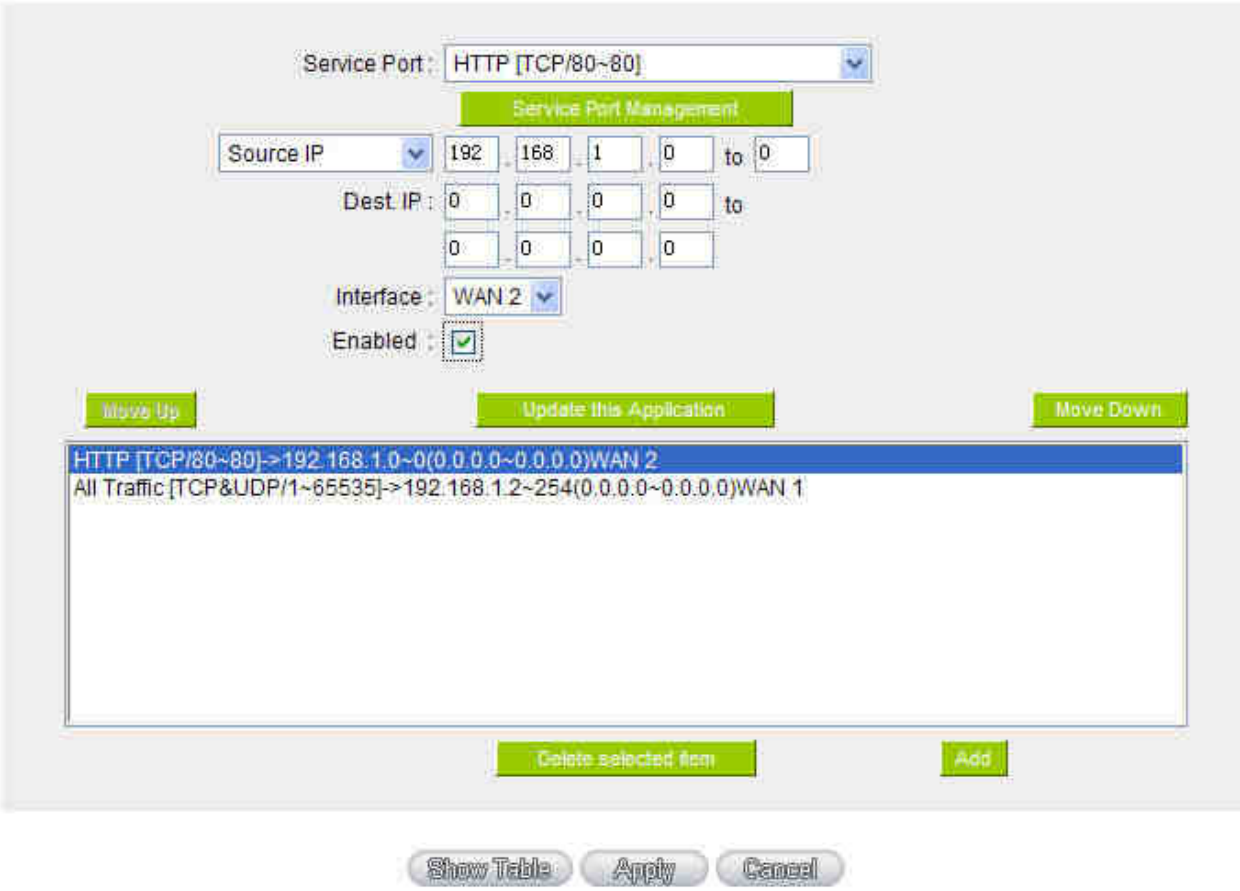


Example 3: How do I set up Auto Load Balance Mode to keep all Intranet IPs from going through WAN2 en route to Port 80 and keep all other services from going through WAN1?

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

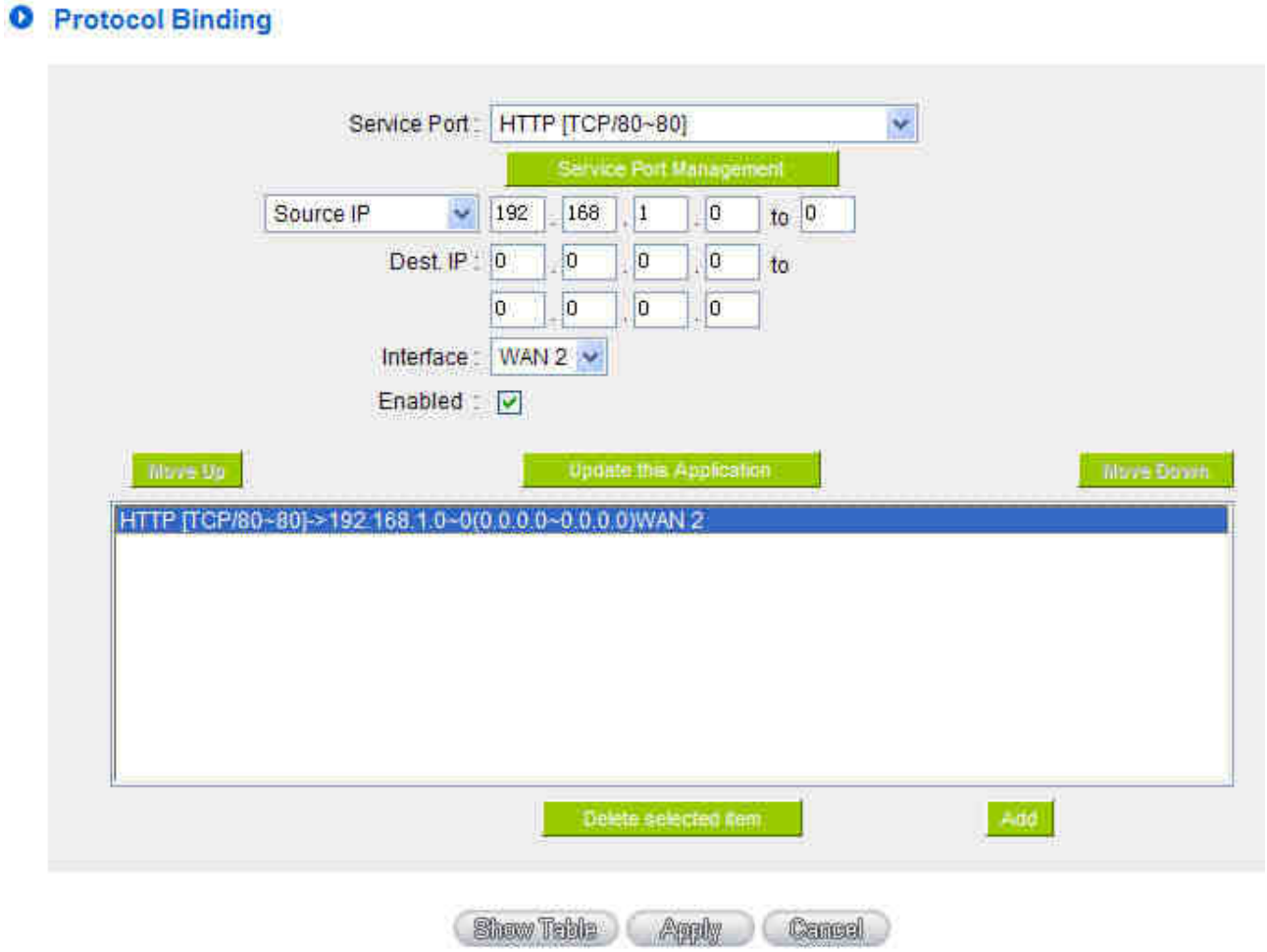


Configuring Assigned Routing Mode for Load Balance Mode

IP Group: This function allows users to assign packets from specific Intranet IPs or to specific destination Service Ports and to specific destination IPs through an assigned WAN to the Internet. After being assigned, the specific WAN will only support those assigned Intranet IPs, destination Service Ports, or destination IPs. 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 IPs from going through WAN2 when the destination is Port 80, and keep all other services from going through WAN1?

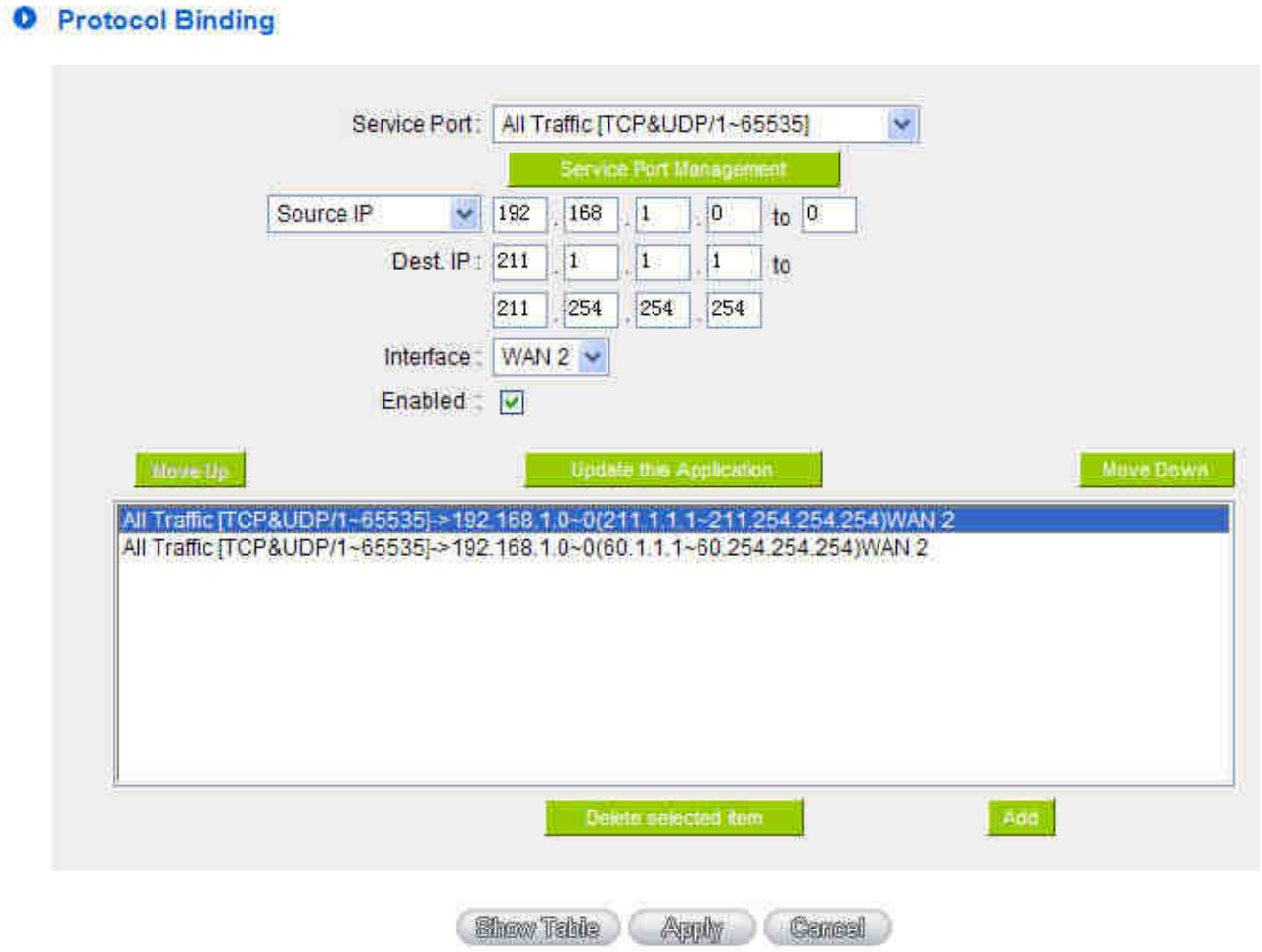
As in the figure below, select "HTTP[TCP/80~80]" from the pull-down option list "Service", and then in the boxes of "Source IP" input "192.168.1.0 ~ 0" (which means to include all Intranet IP addresses). Retain the original numbers "0.0.0.0" in the boxes of "Destination IP" (Which means to include all 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 traffic will be transmitted through WAN1.



Example 2: How do I configure Protocol Binding to keep traffic from all Intranet IPs 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 IPs). 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 IPs). 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.



6、Port Management

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.

6.1 Port Setup

Setup

Enable Port 1 as Mirror Port

Port ID	Interface	Disabled	Priority	Speed Status	Duplex Status	Auto Neg.	VLAN
1	LAN	☐	Normal	100M	Full	☑	VLAN1
2	LAN	☐	Normal	100M	Full	☑	VLAN1
3	LAN	☐	Normal	100M	Full	☑	VLAN1
4	LAN	☐	Normal	100M	Full	☑	VLAN1
DMZ/Internet	WAN2	☐	Normal	100M	Full	☑	
Internet	WAN1	☐	Normal	100M	Full	☑	

Apply Cancel

Mirror Port

Users can enable Port 1 as Mirror Port. All outbound traffic will be duplicated to the mirror port. So, users can monitor or filter the packets through the gateway. If you activate the function, you can see the physical port status in the homepage will be showed Port 1 as "Mirror Port."

Physical Port Status

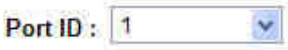
Port ID	1	2	3	4
Interface	Mirror Port	LAN		
Status	Connect	Enabled	Enabled	Enabled

Ethernet Port Settings

Port ID:	Display the order of each port.
Interface:	The type of each port, including LAN1~LAN 4, WAN1~WAN2 and DMZ. According to the current network configuration settings, the setup of these ports will be adjusted automatically.
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 Status:	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. In each LAN port, users may define up to 5 VLAN local network groups.
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.

6.2 Port Status

Through this option, users may select the Ethernet port to view the real-time parameters as illustrated below:



Summary

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

Statistics

Receive Packets Count	7560822
Receive Packets Byte Count	7560822
Transmit Packets Count	31637452
Transmit Packets Byte Count	31637452
Error Packets Count	0

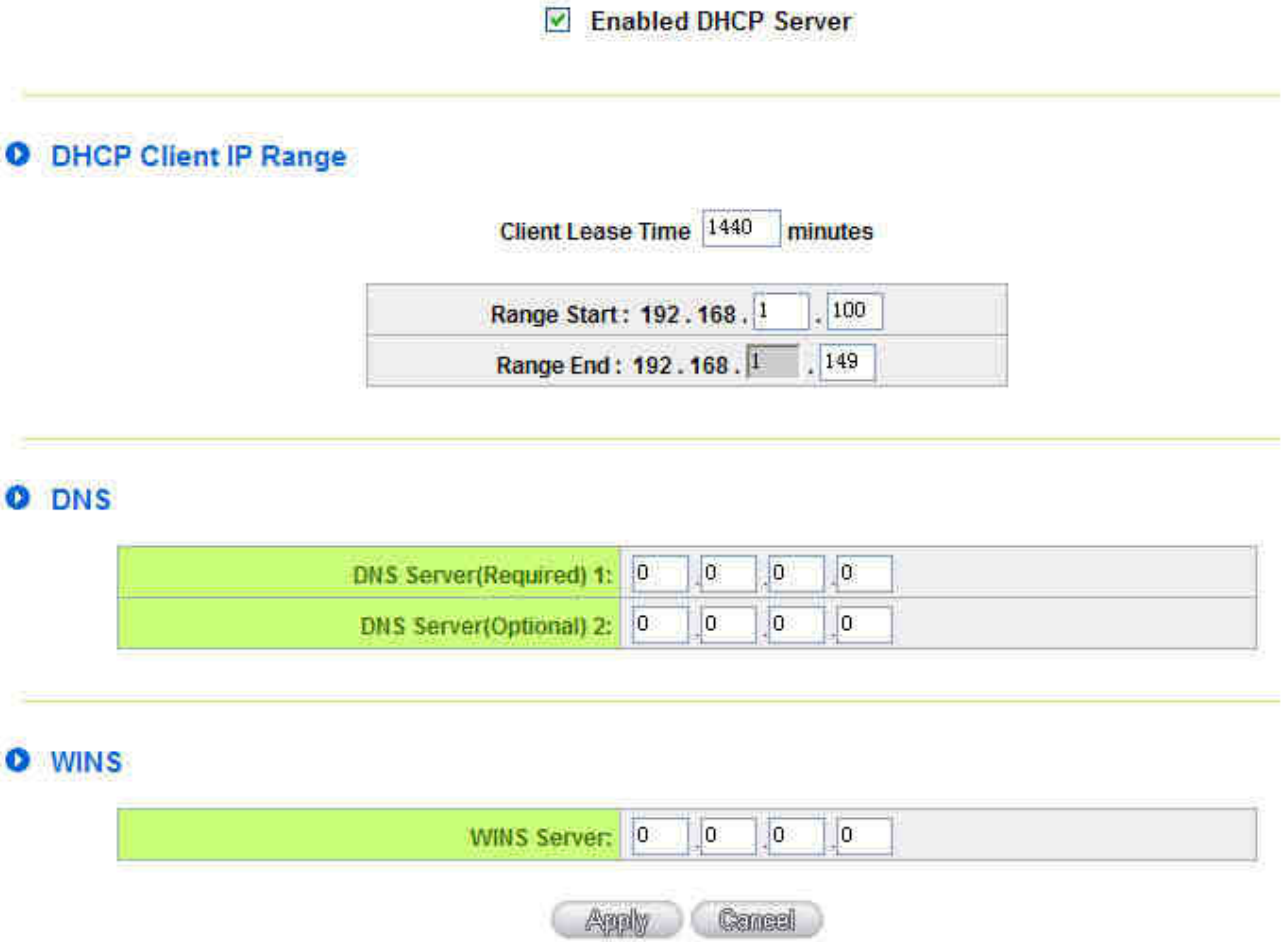
Through the general message list of the Port Status, the current port hardware setting items will be displayed. For example, there are Network Connection Type（10Base-T / 100Base-TX / 1000Base-T）, Interface, Link Status (Up/Down), Port Activity (Port Enabled), Priority Setting (High or Normal), Speed Status (10Mbps or 100Mbps), Duplex Status (half

duplex or full duplex), Auto Neg. (Enabled/Disabled), VLAN and so forth.

Through the message list displaying the real-time traffic of the network port, the packet data of this 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.

6.3 DHCP IP Issuing Server

With an embedded DHCP server, it supports automatic IP acquisition 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.)



Dynamic IP

Enabled 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 means DHCP will terminate the lease at this IP address. The default terminal IP address is 149. Though the default supports automatic IP acquisition for 50 computers, users can increase or reduce the number according to their needs.

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

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.

DNS Server (Required) 1:	Input the IP address of the DNS server. The default is "0".
DNS Server (Optional) 2:	Input the IP address of the DNS server. The default is "0".

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

WINS Server

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

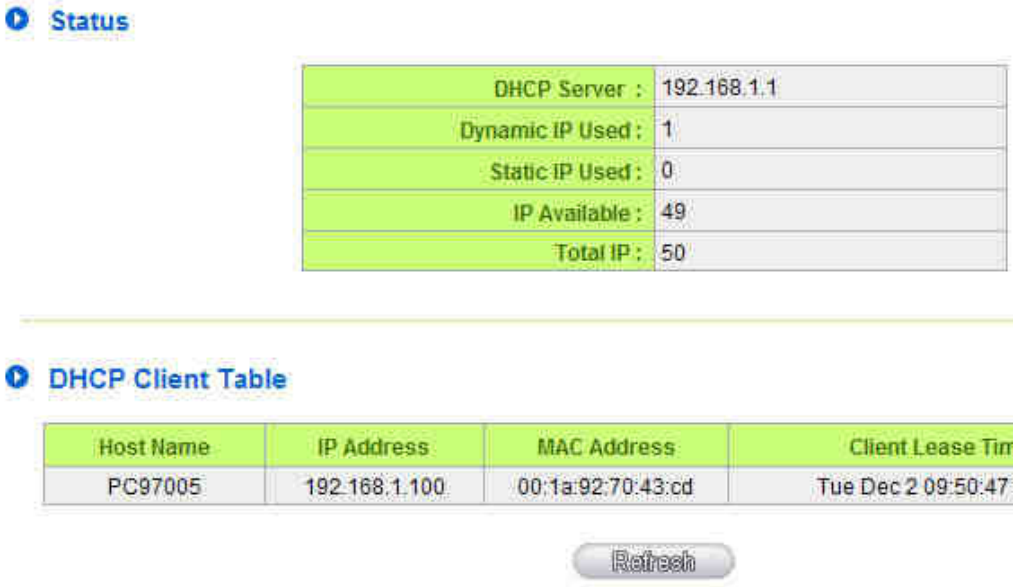
WINS:	Input the IP address of WINS. The default is "0".

After the changes are completed, click **"Apply"** to save the network configuration

modification, or click **"Cancel"** to leave without making any changes.

6.4 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. The content of the Introduction list is as follows:



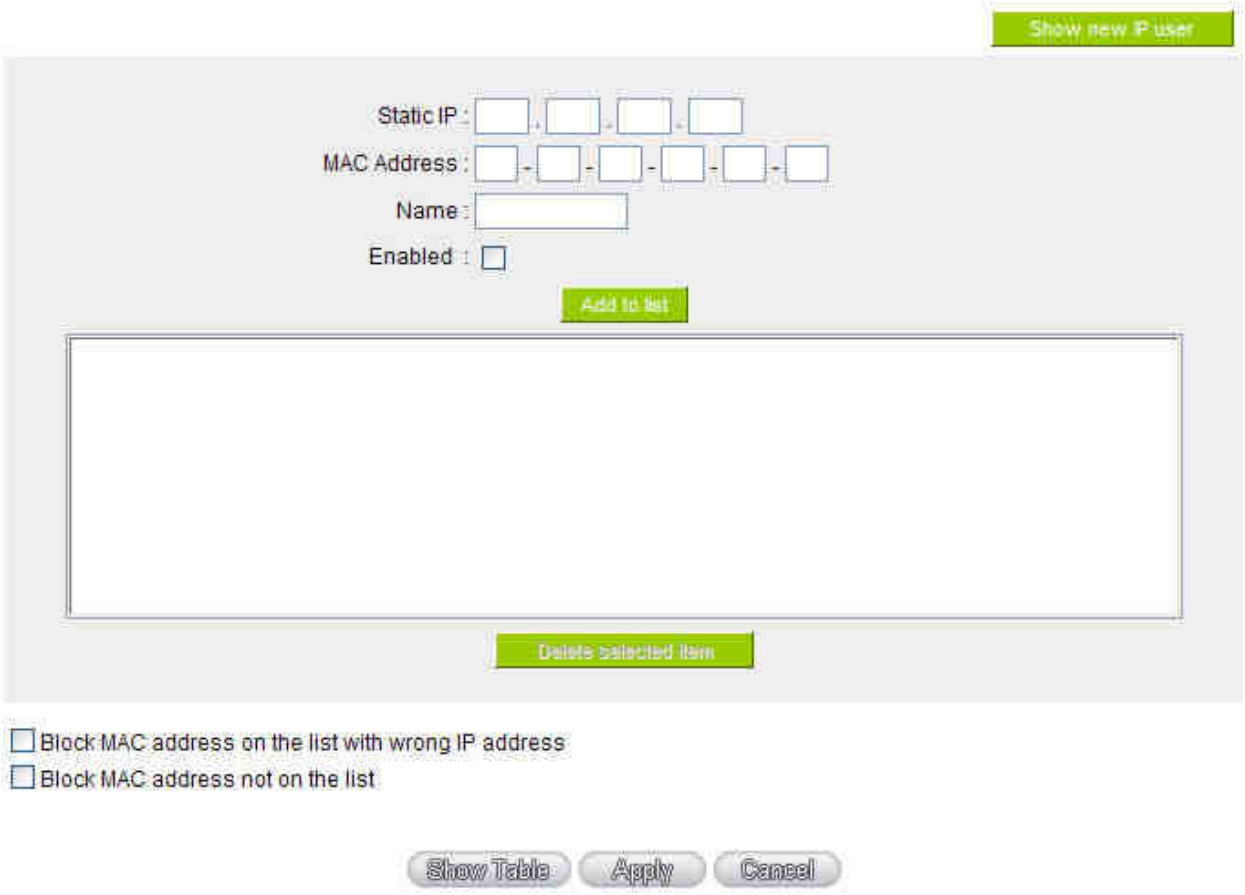
DHCP Server:	DHCP IP address
Dynamic IP Used:	The amount of dynamic IP leased by DHCP.
Static IP Used:	The amount of static IP assigned by DHCP.
DHCP Available:	The amount of IP still available in the DHCP server.
Total:	The total IP which the DHCP server is configured to lease.
Host Name:	The name of 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:	To remove a record of an IP lease.

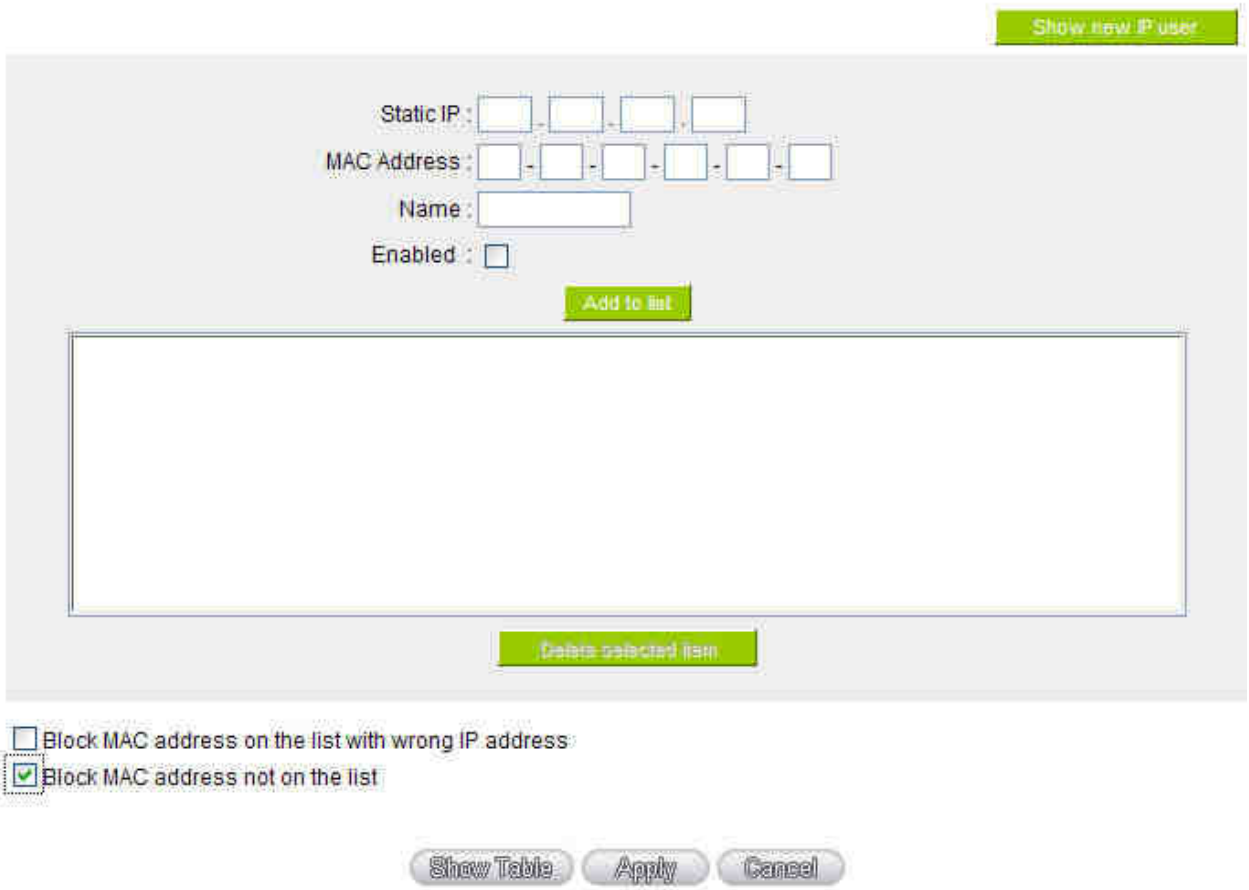
After the changes are completed, click "**Apply**" to save the network configuration modification, or click "**Cancel**" to leave without making any change.

6.5 IP & MAC Binding

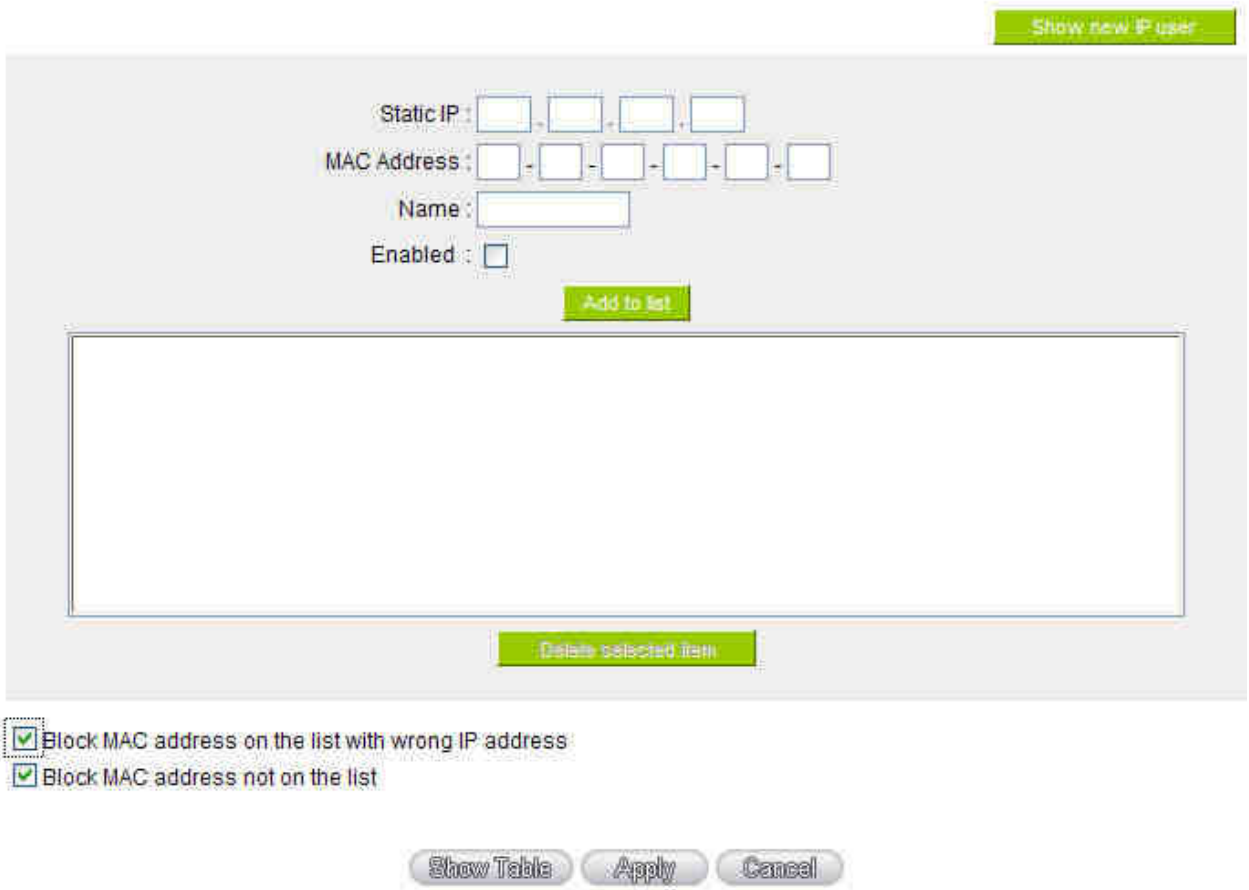
IP & MAC Binding



IP & MAC Binding



IP & MAC Binding

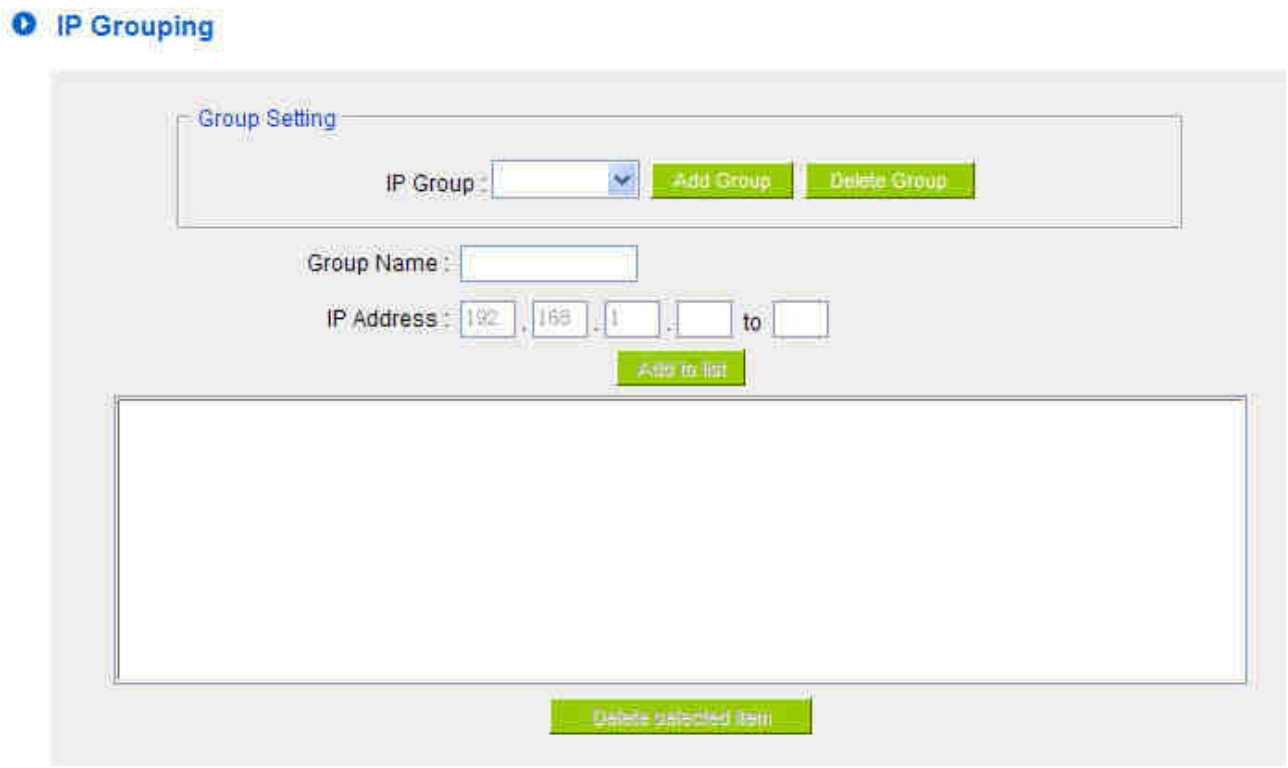


Static IP:	There are two ways to input static IP: 1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a static IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty. 2. If users want DHCP to assign a static IP for a PC every single time, users should input 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. Either Chinese or English can be accepted.
Enabled:	To activate this configuration.
Add To List:	To add the configuration or modification to the list.
Delete Selected Items:	To remove the selected binding from the list.
Add:	To 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.
Block MAC address not on the list:	When this option is checked, user-modified IP or IP which is not configured in the list will not be able to connect with the Internet.
Show New IP User:	Select the IP/MAC which is to be bound and define a client name for it, and then activate it.

6.6 IP Group

The function enables users to make the same configuration for a range of continuous IP addresses in the network. For example, if a IP range (192.168.1.100~192.168.1.110) has been assigned to a department of a company, we can bind all the IPs together and make an accessing rule configuration for them all at the same time, instead of configuring each IP respectively, which takes more time and is more prone to error.

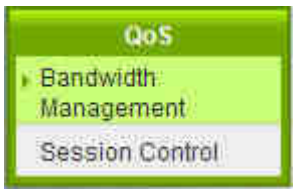


Group:	Select a group to which the modification is to be made.
Group Name:	Input a name for the group such as "Marketing Department", "Sales Department", etc.
IP address:	Input the assigned IP range.
Add:	Add a new IP.

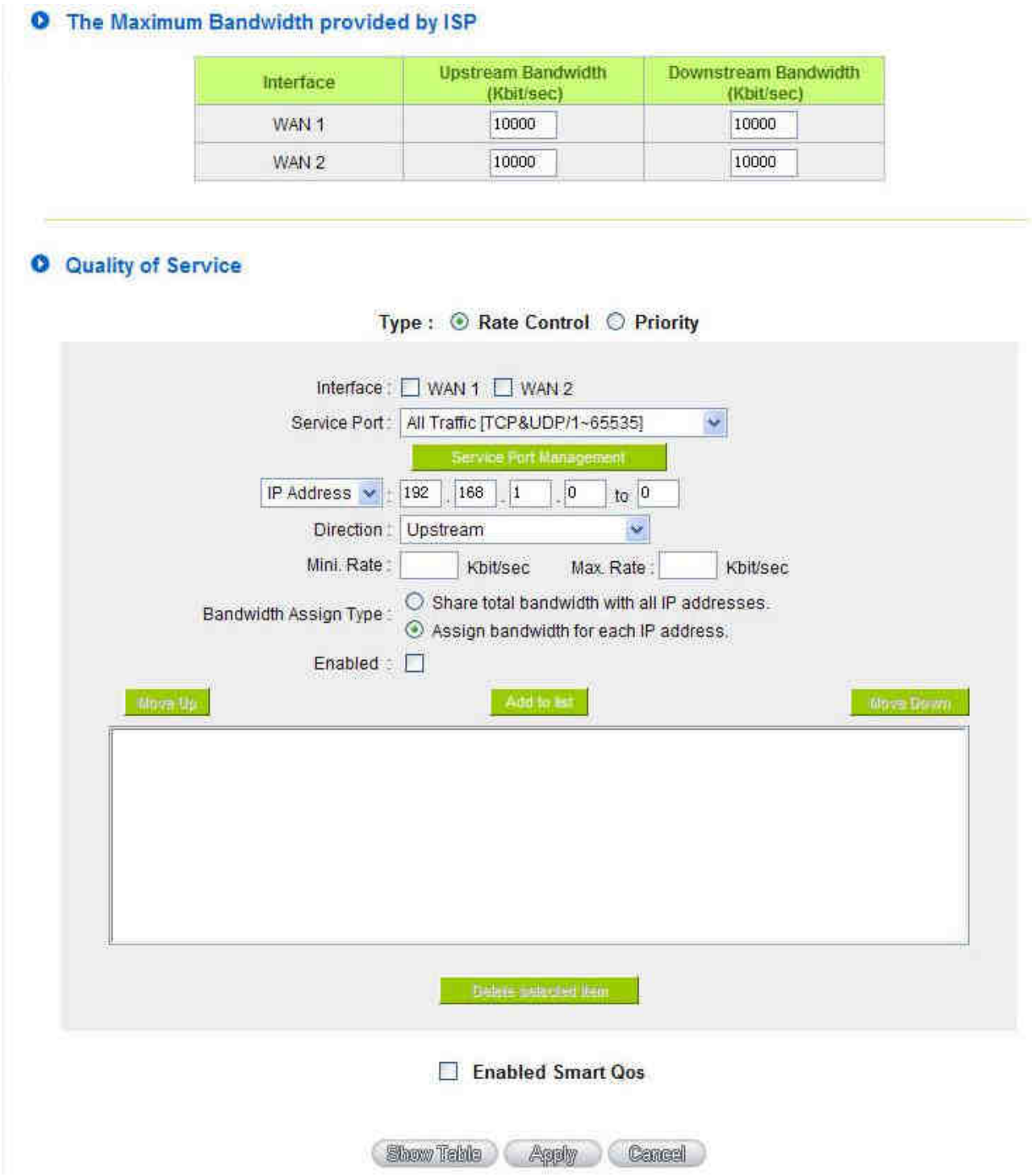
After the changes are completed, click **"Apply"** to save the network configuration modification, or click **"Cancel"** to leave without making any changes.

7、QoS (Quality of Service)

QoS is an abbreviation for Quality of Service. The main function is to restrict bandwidth usage for some services and IPs 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.



7.1 Bandwidth Management (QoS)



7.1.1 The Maximum Bandwidth provided by ISP

The Maximum Bandwidth provided by ISP

Interface	Upstream Bandwidth (Kbit/sec)	Downstream Bandwidth (Kbit/sec)
WAN 1	10000	10000
WAN 2	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 IPs 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.

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

Attention!
The unit of calculation in this example is Kbit. Some software indicates the downstream/upstream speed with the unit KB. 1KB = 8Kbit.

7.1.2 QoS Configuration

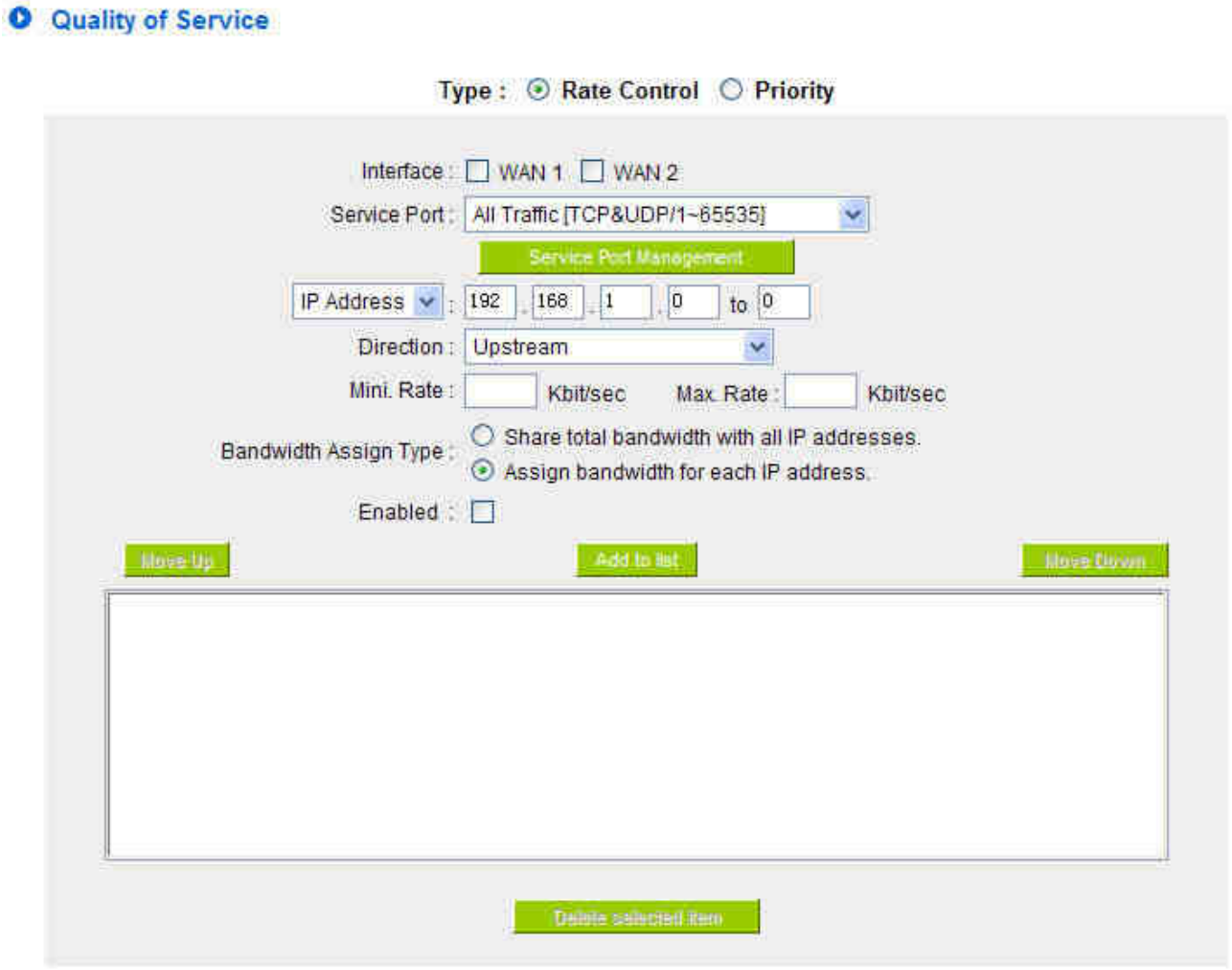
To satisfy the bandwidth requirements of certain users, the device enables users to set up QoS: Rate Control and Priority Control for certain WANs. Users can select only one of the above QoS choices.

There are two options for bandwidth management: one is Rate Control, the other is Priority Control. The two kinds of management cannot be used at the same time. Network administrators must choose one or the other based on the Intranet needs.

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.

Rate Controlo



Interface:	To select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service:	To 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:	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 IPs from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input "0" in the

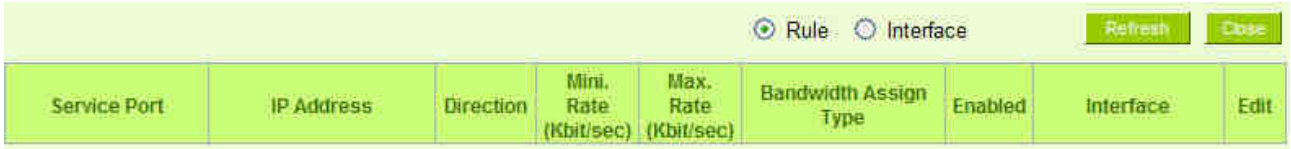
	boxes of IP address. This means all Intranet IPs will be restricted. QoS can also control the range of Class B.
Direction:	● **Upstream:** Means the upload bandwidth for Intranet IP. ● **Downstream:** Means the download bandwidth for Intranet IP. ● **Server in LAN, Upstream:** If a Server for external 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 Sharing:	● **Sharing total bandwidth with all IP addresses:** If this option is selected, all IPs 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:	To activate the rule.
Add To List:	To add this rule to the list.
Move up & Move Down:	The 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 IPs would then be moved upward.
Delete selected application:	To remove the rules selected from the Service List.

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

Show Table

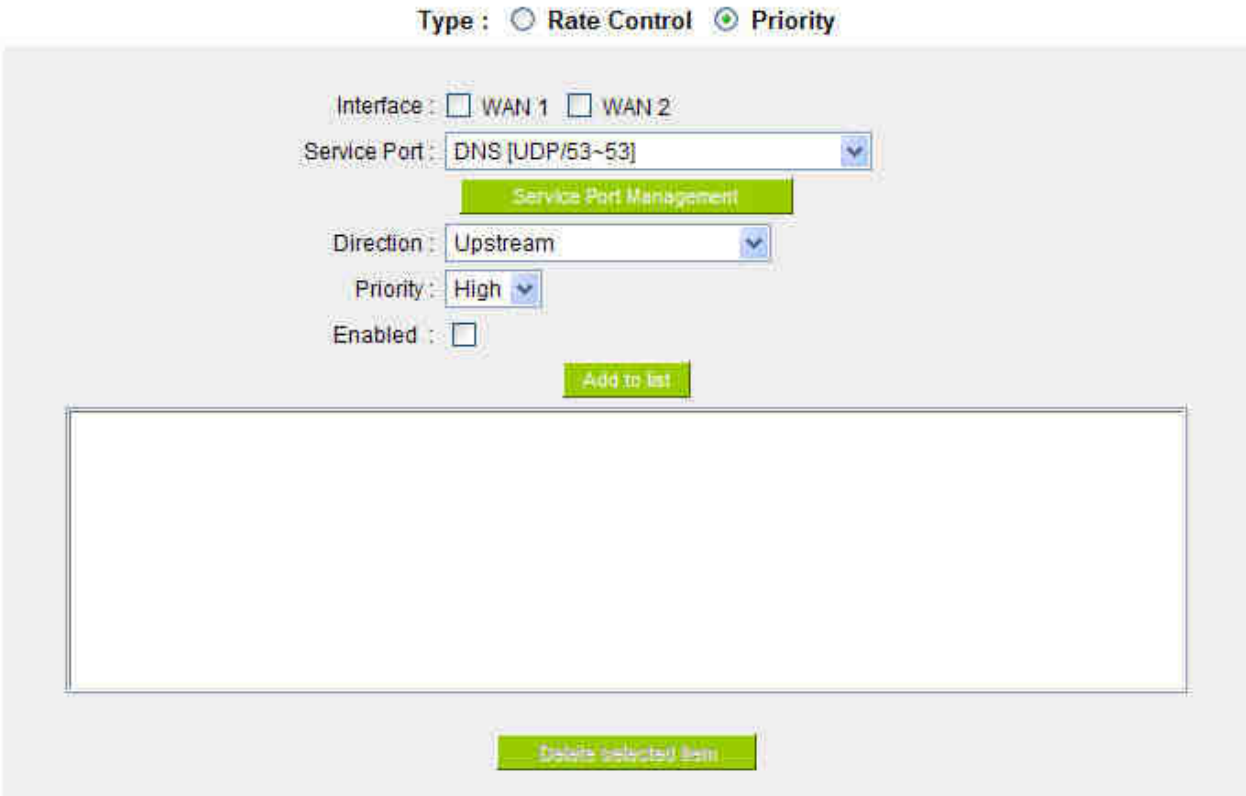
This will display all the Rate Control Rules users made for the bandwidth. Click "Edit" to modify.



Priority

The Router will distribute the bandwidth as 60% (the highest) and 10% (the lowest). If you set the service port 80 as "High" priority, the router will give 60% bandwidth to the port 80. In the other hand, if you give the port 21 as "Low" priority, the device will only give it 10% bandwidth. The remained 30% bandwidth will be shared by other service.

Quality of Service



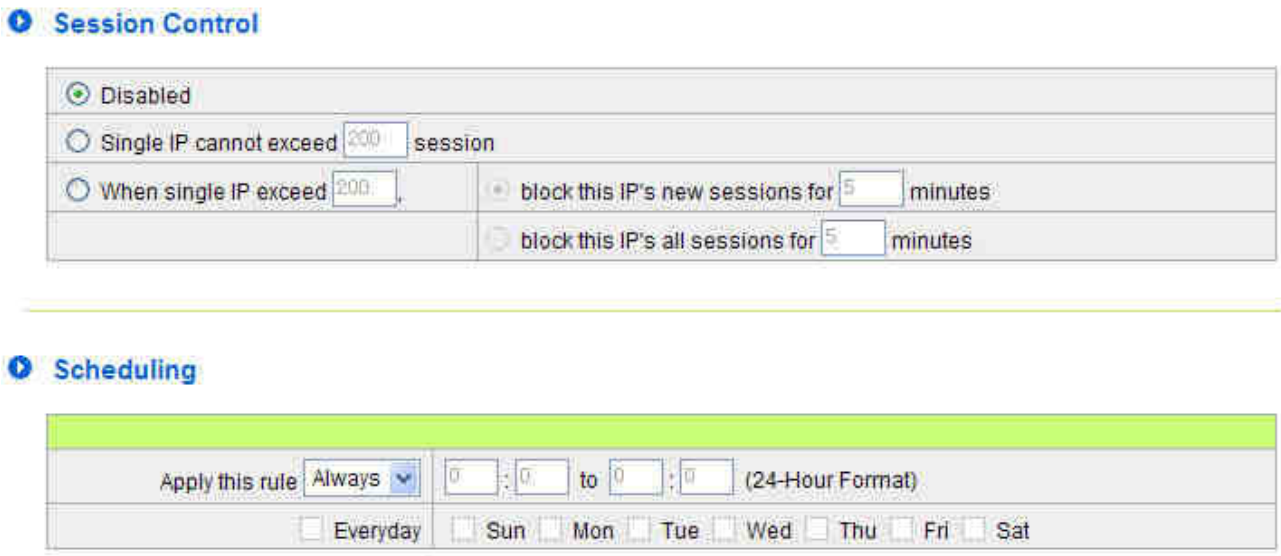
Interface	To select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service	To select what bandwidth control is to be configured in the QoS rule. If FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
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.

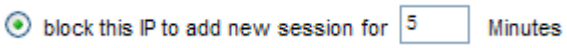
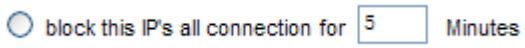
Priority	High: 60% guaranteed bandwidth to the service Low: Only 10% bandwidth offerd to the service
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Delete selected application:	To remove the rules selected from the Service List.
Show Table:	This will display all the Priority Rules users made for the bandwidth. Click "**Edit**" to modify.
Apply	Save the configuration
Cancel	Leave without making any change

7.2 Session Control

Session management controls the acceptable maximum simultaneous connections 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 connections. Setting up proper limitations on connections can effectively control the connections created by P2P software. It will also have a limiting effect on bandwidth usage.

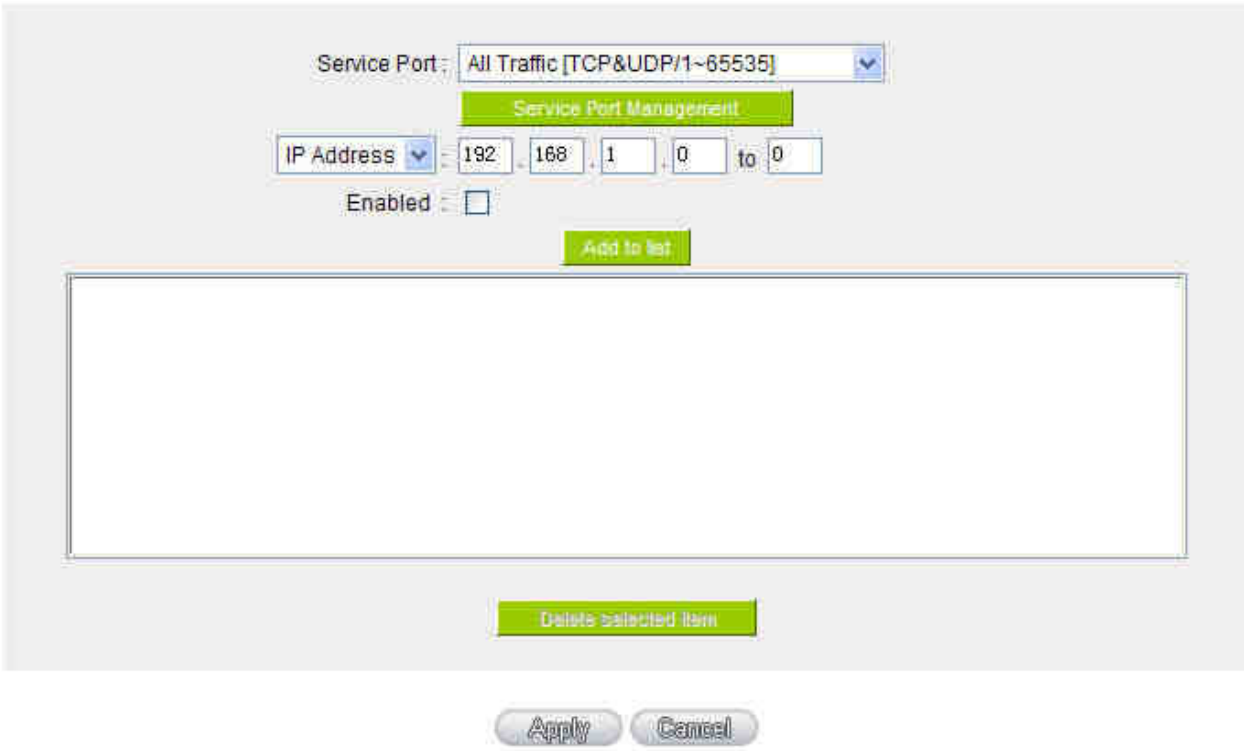
In addition, if any Intranet PC is attacked by a virus like Worm.Blaster and sends a huge number of connection requests, session control will restrict that as well.



Disable:	To disable Session Control function.
Single IP cannot exceed ____ Session	This option enables the restriction of maximum external connections to each Intranet PC. When the number of external connections reaches the limit, to allow new connections to be built, some of the existing connections must be closed. For example, when BT or P2P is being used to download information and the connections exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.
Network Service Detection: **(When single IP exceed limit)**	 If this function is selected, when the user's port connection reach the limit, this user will not be able to make a new connection for five minutes. Even if the previous connection has been closed, new connections cannot be made until the setting time ends.  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.
Days Management:	If "**Everyday**" is selected, the rule will be activated for the control time range every day. Users can choose to activate the rule during certain days of the week.

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

Exempted Port or IP Service



Exempted Port or IP Service:	The important services or IPs in a company or business can be configured to be free of the Connection Restriction Rule.
Service:	To select a Service Port to be free of the connection rule.
Service Management:	To add or remove a Service Port.
Source IP/Group:	To add IP addresses/Groups that are free from restriction.
Enable:	To activate the added rule.
Add To List:	To add the rule into the list.

7.3 Smart QoS

The smart QoS function enables the administrators to constrain the bandwidth occupied automatically without any configuring.

Enabled Smart Qos	To activate the Smart QoS function.
When the usage of any WAN's bandwith is over than __ %, Enable Smart Qos(0: Always Enabled)	When the usage of any WAN's bandwith is over than __ %, Smart QoS will be enabled. You can enter the needed value, the default is 60%.
Each IP's upstream bandwidth threshold(for all WAN)	Input the allowed maximum threshold.
Each IP's downstream bandwidth threshold(for all WAN)	Input the allowed maximum threshold.
If any IP's bandwith is over maximum threshold, its maximum bandwidth will remain **WAN1:__kbit/sec** **WAN2:__kbit/sec**	If any IP's bandwith is over maximum threshold, the penalty mechanism will be activated. After being punished, its maximum upstream/downstream bandwidth will remain as a determined value.
Enabled Penalty Mechanism	To activate the penalty mechanism.

Show Penalty List	To show the IPs with upstream constraint、downstream constraint and in the penalty mechanism.
Applied Time	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.

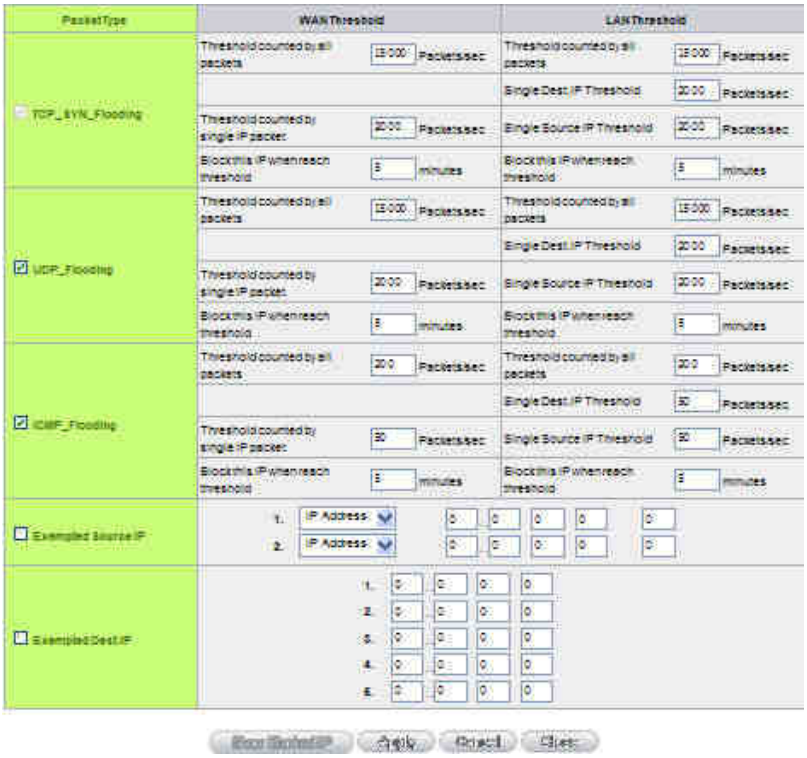
8、Firewall Configuration

8.1 General Setting

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.

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 Through:	There are many audio and visual streaming media on the network. Broadcasting 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:	 **Packet Type:** This device provide 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 minutesOBJ 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 minutesOBJ 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.
Exempted Source IP	Input the exempted source IP.
Exempted Dest. IP	Input the exempted Destination IPs.

Show Blocked IPs	 To show the blocked IP list and the remained blocked time.

Restrict WEB Features:

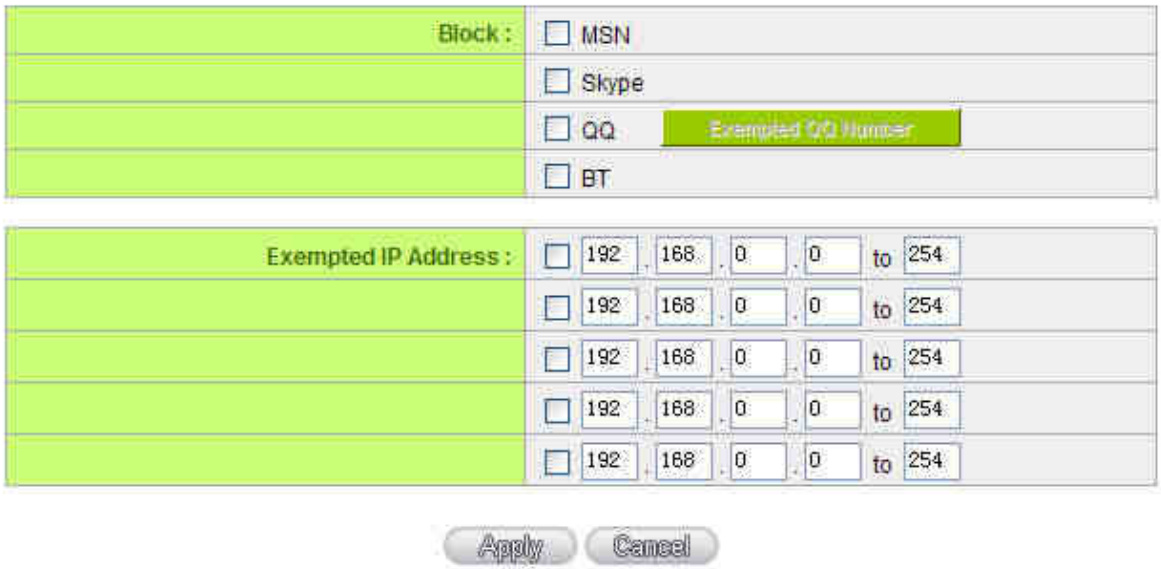
Restrict WEB Features:	It supports the block that is connected through: Java, Cookies, Active X, and HTTP Proxy access.
Don't Block Java / ActiveX / Cookies Proxy to Trusted Domain:	If this option is activated, users can add trusted network or IP address into the trust domain, and it will not block items such as Java/ActiveX/Cookies contained in the web pages from the trust domains.
Apply	Save the configuration
Cancel	Leave without making any change

Restrict Application

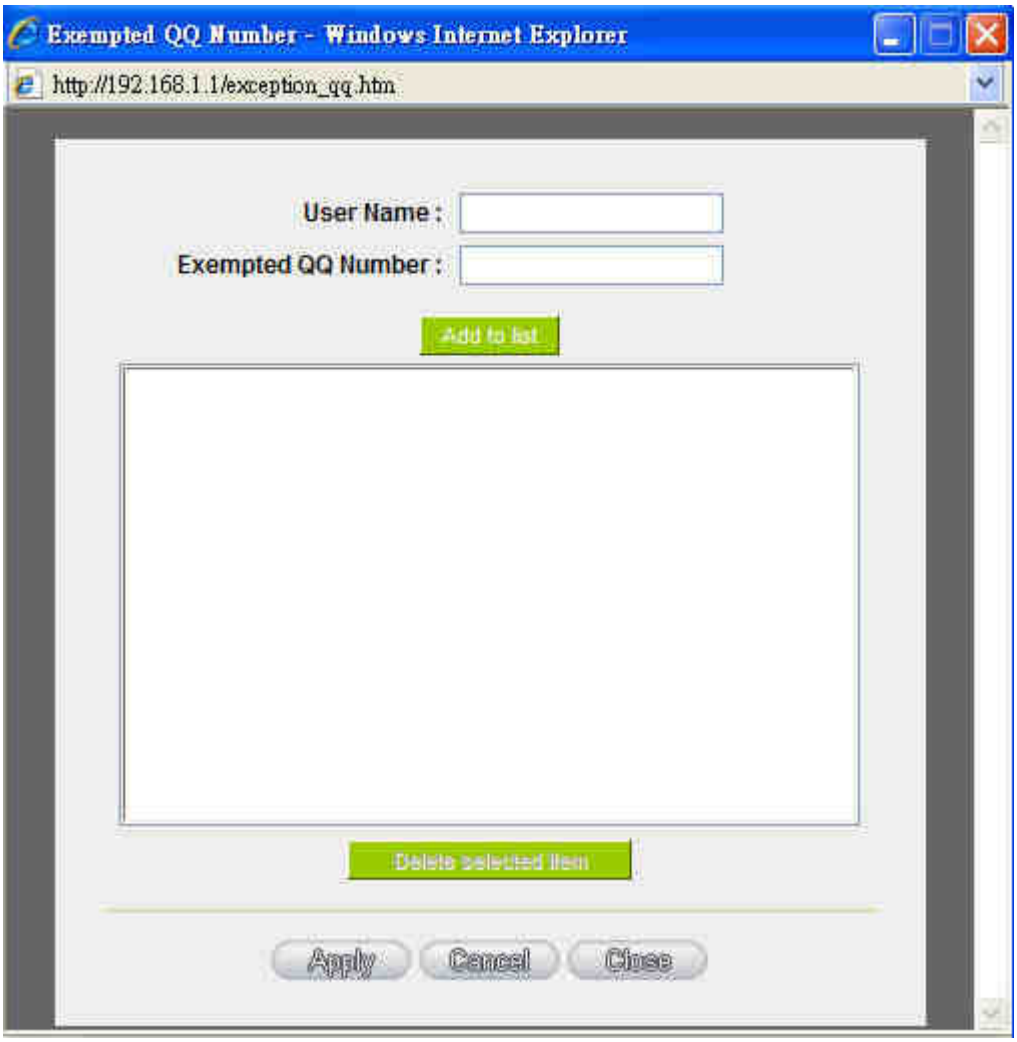
Users can tick **MSN/ Skype/ QQ/ BT** and the device will block the service users ticked. However, to provide this service for certain IP address in the intranet, users may tick the following item and then enter the specific IP address or IP address session to use the services which are ticked above.

After modification, press "**Apply**" to save the network settings or press "**Cancel**" to keep the settings unchanged.

Restrict Application



In the other hand, if Blocked QQ is activated, users can set the exempted QQ number list.



User Name :	Input the information of the QQ number, etc. Qno Sales。
Exempted QQ number	Input the number.
Add to list	To add the number to the list.
Delete selected item	Delete the selected rule in the list.

8.2 Network 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.

8.2.1 Default Access 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)

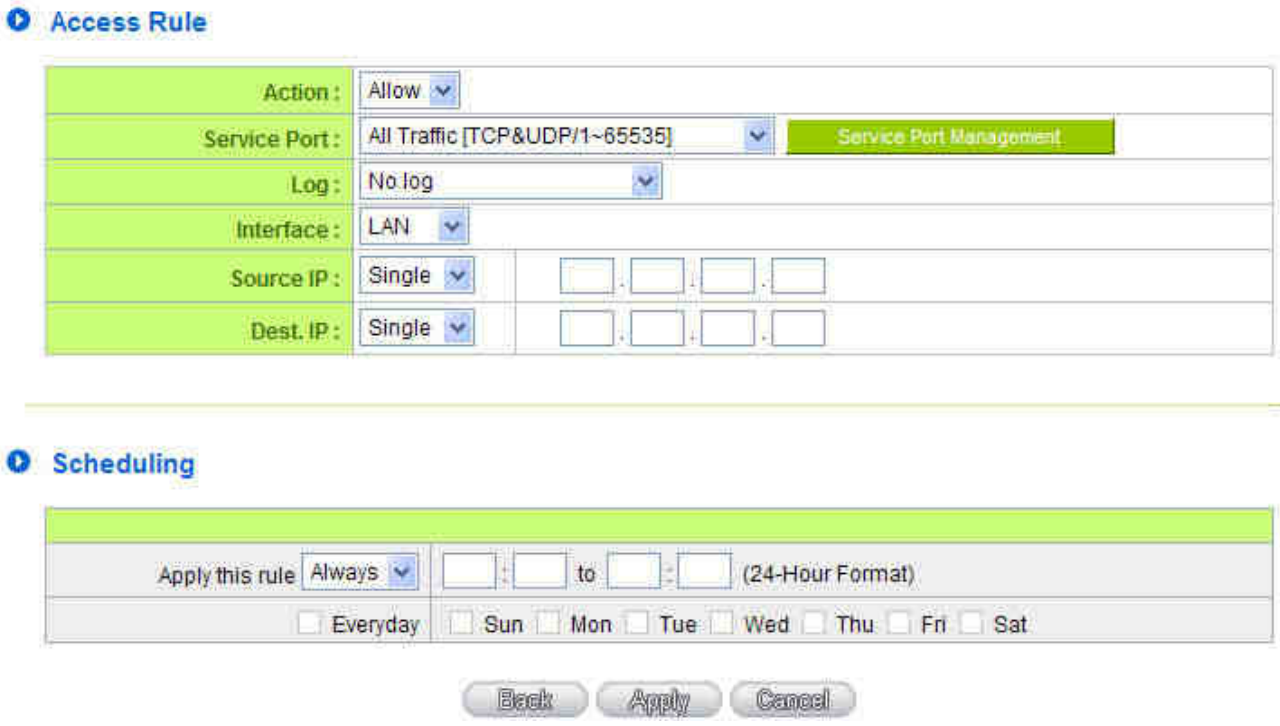
* Ping Service (from LAN to Device) is on by default (for connection and test)

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. Click on **Edit** to define the network access rule item and press **Delete** to remove the item.

Press **Add New Rule** to create a new network access rule. Or press **Return to Default Rules** to restore all settings to the default values and delete all the self-defined settings.

After modification, press "**Apply**" button to save the network settings or press "**Cancel**" to keep the settings unchanged.

8.2.2 Add New Access Rules



Service

Action:	This allows setting the rule under control. ● Allow: Permits the pass of packets compliant with this control rule ● Deny: Prevents the pass of packets not compliant with this control rule
Service:	From the drop-down menu, select the service that users grant or do not give permission.
Service 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.
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. 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.

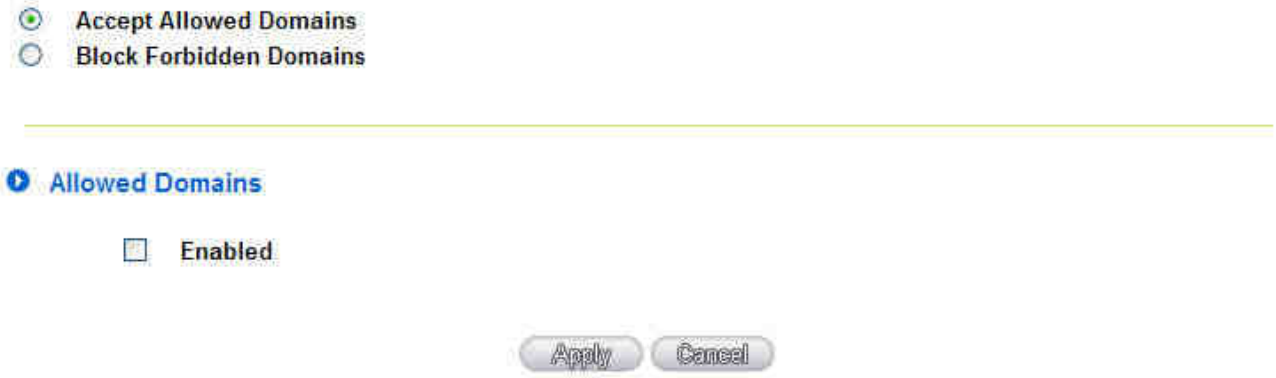
Apply this rule:	Select "**Always**" to apply the rule on a round-the-clock basis .If "**From**" is selected, the activation time is introduced as below
… to …:	This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)
Day Control:	"**Everyday**" 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.

After modification, press "**Apply**" to save the network settings or press "**Cancel**" to

keep the settings unchanged.

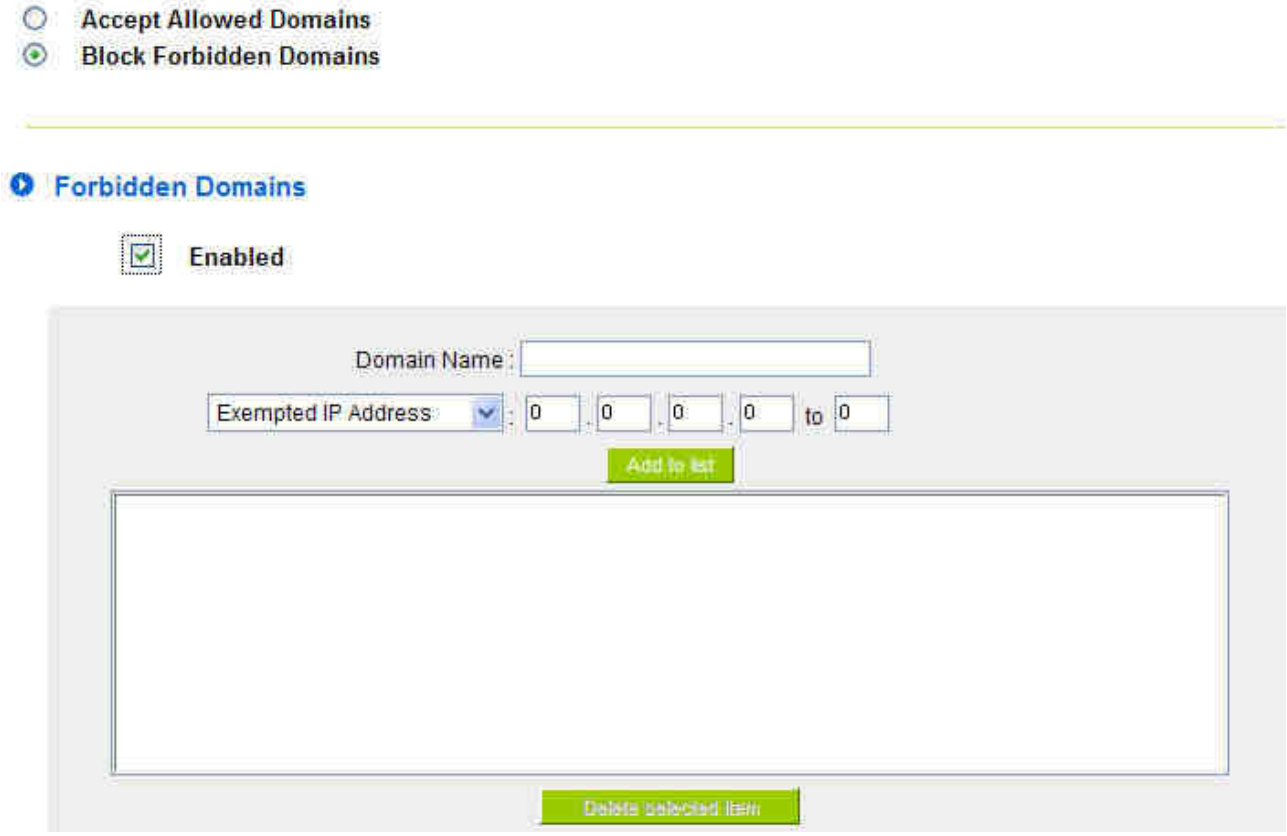
8.3 Content Filter

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

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

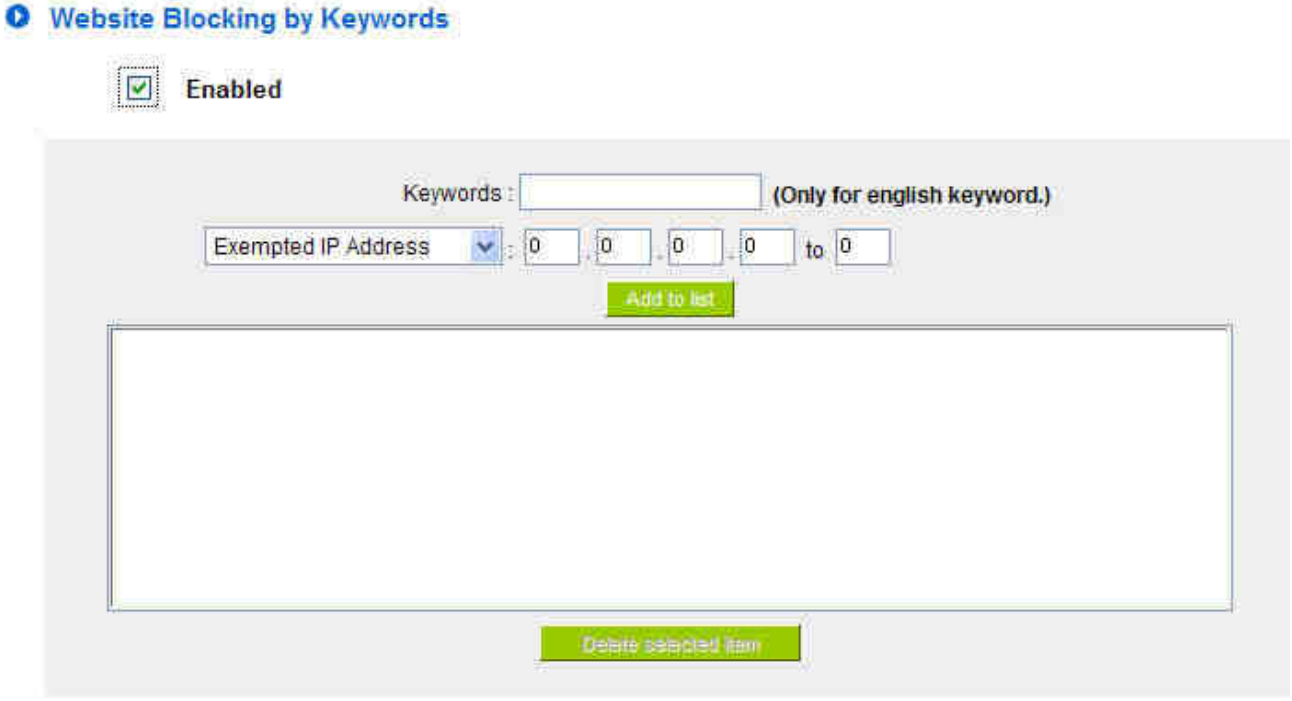


Block Forbidden Domains

Click to enable this feature. The default setting is Disabled.

Domain name:	Enter the websites to be controlled such as www.playboy.com
Add to list:	Click ”Add to list” to create a new website to be controlled.
Delete selected item:	Click to select one or more controlled websites and click this option to delete.

Website Blocking by Keywords

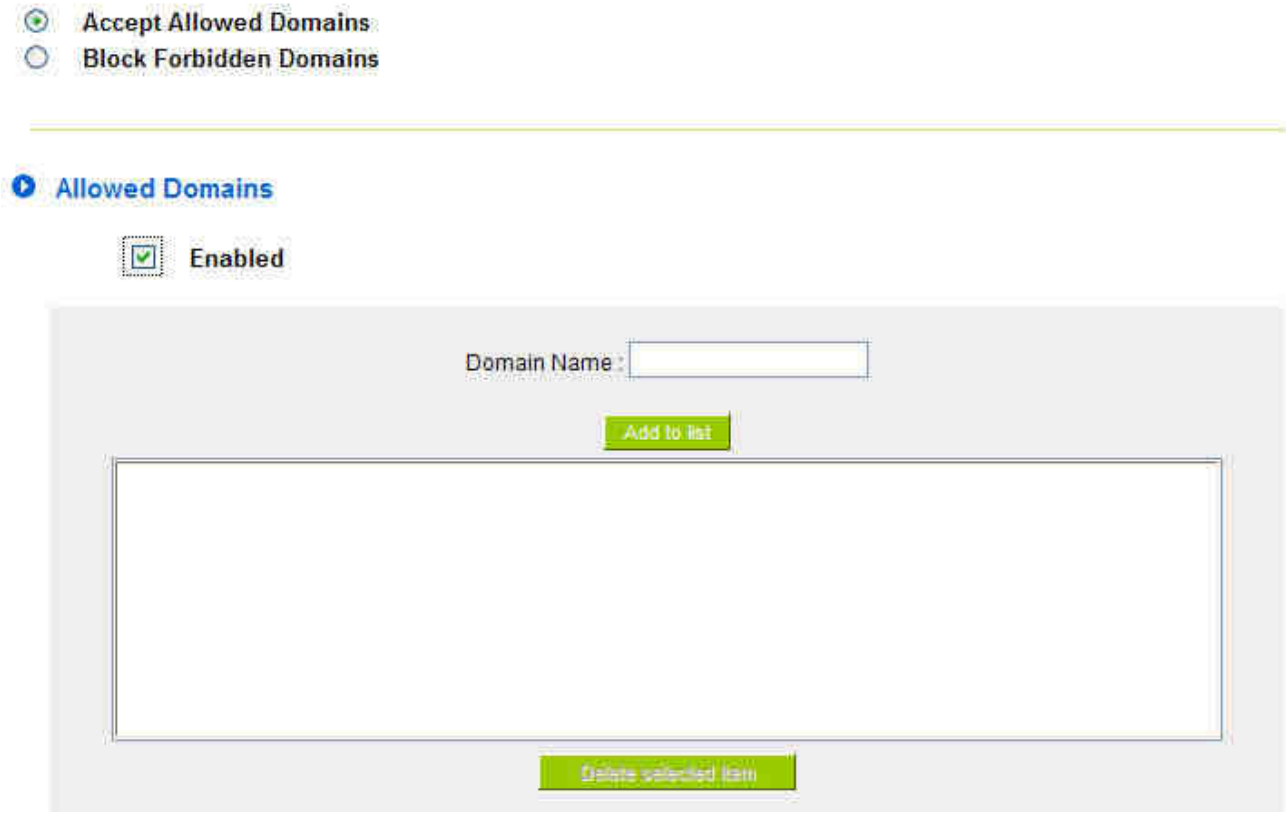


Click to activate this feature. The default setting is disabled. For example: If users enter the string ”sex”, any websites containing ”sex” will be blocked.

Keywords:	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. This act is only valid before "Apply" is used.

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 fuction.



Enabled:	To activate the fuction. 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.

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.

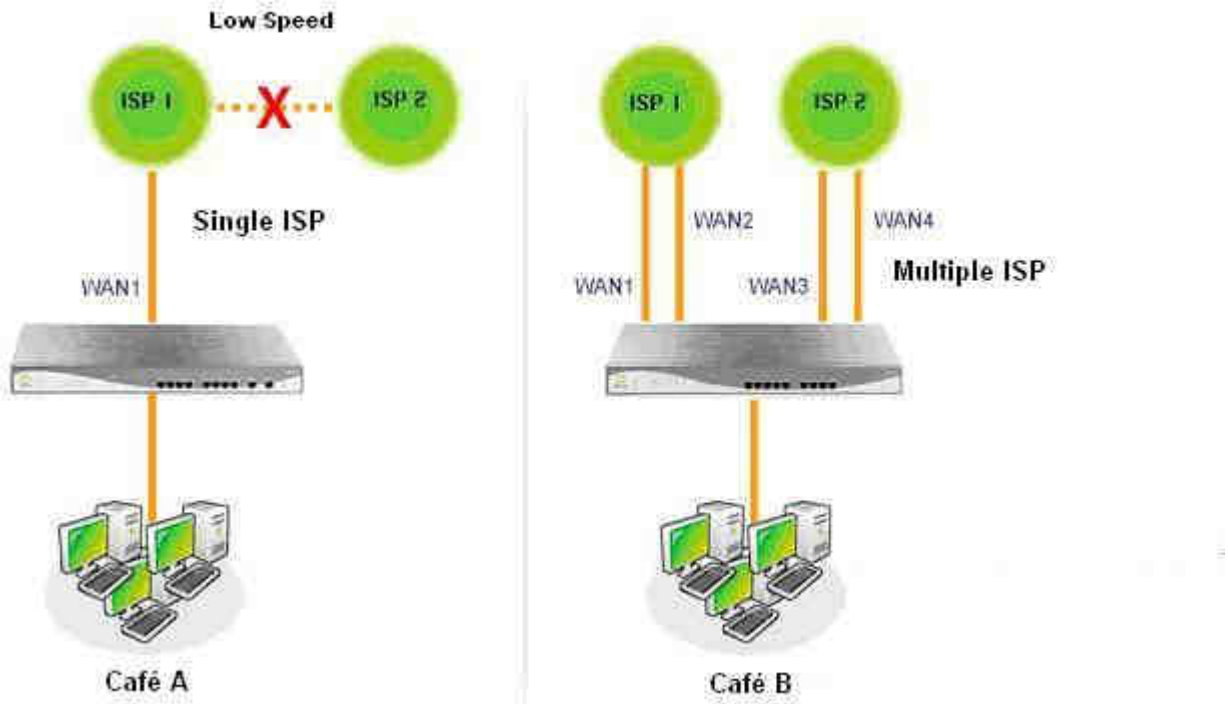
Scheduling

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

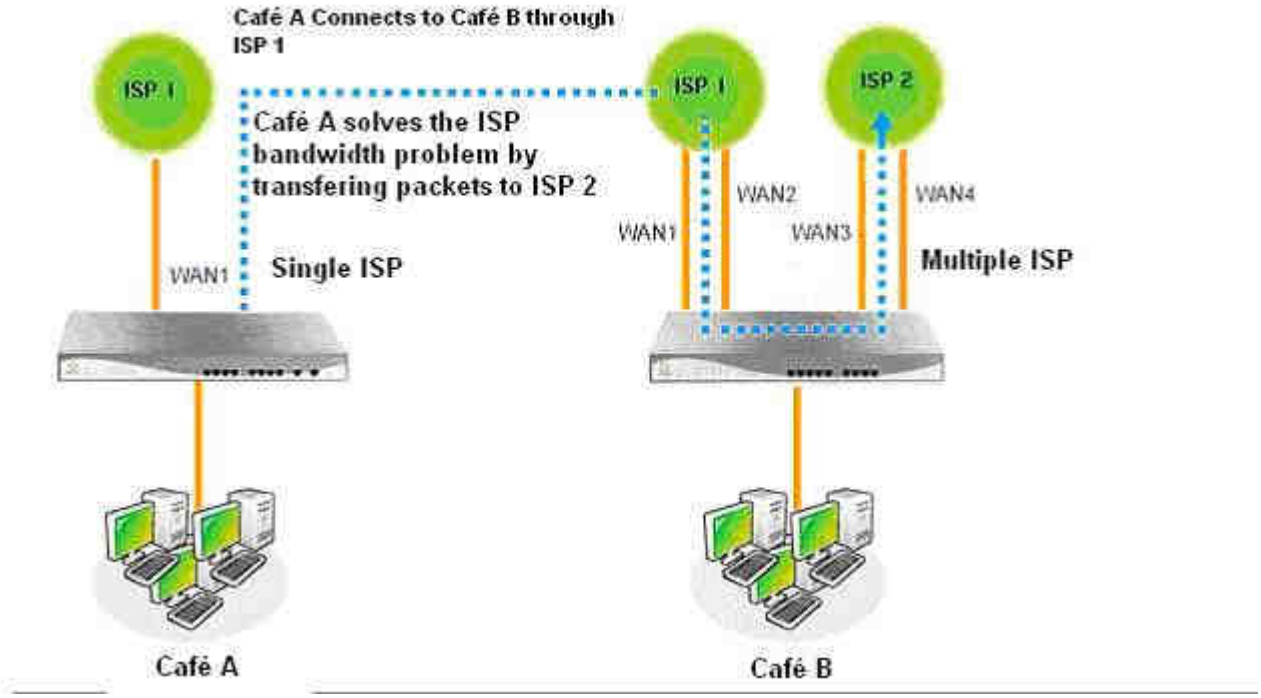
Apply Cancel

9、Virtual Route

Virtual Router enable the branch only has single ISP service can enjoy two different broadband network. The branch can access another ISP network with connecting to headquarter server with dual-bradband connection. As the result, the linking problem between different ISP network will be sloved.

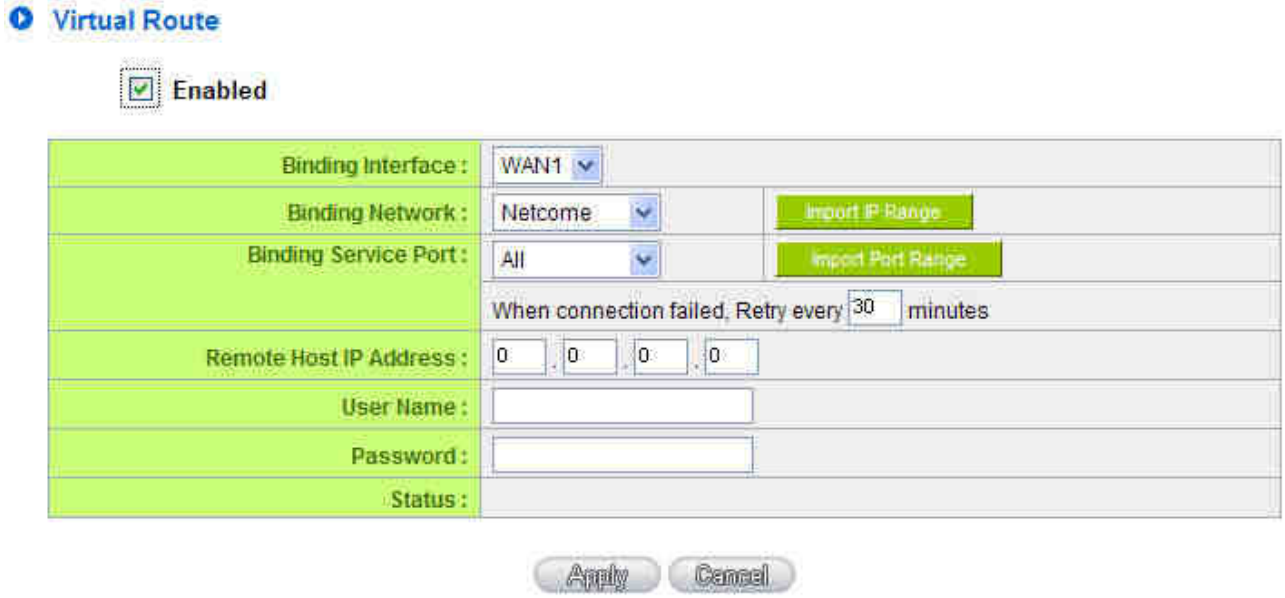


As the figure showed above, Café A has only one ISP service. Because of narrow bandwidth between two different ISP, the connection speed that users access to the web or on-line game on another network will be very slow. On the other hands, Café B owns two different ISP service. No matter what network users access to, the connection speed will be fast.



Café A can enable virtual route function and link to Café B's device. They can access another ISP service through Café B's network. It seems that Café A employ dual ISP service, too. If users in Café A want to access to another ISP network, the link speed won't be restricted.

9.1 Virtual Route (Client)

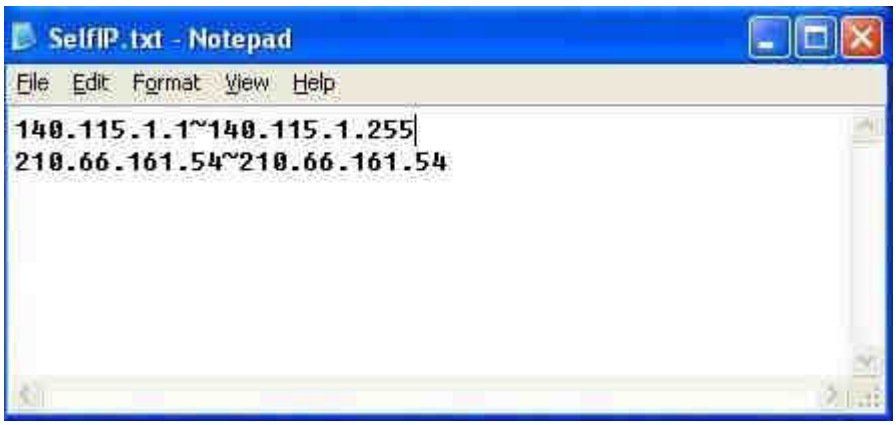


Enabled	To activate the function.
Binding Interface	To select which WAN port is binded: WAN1~WAN2
Binding Network	To select the binding network: Netcome or Self-Defined.
Import IP Range	Click "Browse" to import binding IP range.
Binding Service Port	To select the port that will execute virtual route: All port, Game, or Self-defined.
Import Port Range	Click "Browse" to import binding port range.
When connection failed, Retry every 30 **minutes**	Input the retry period when connection failed. The default value is 30 minutes.
Remote Host IP	Input the IP of virtual route server.

Address	
User Name	Input the user name.
Password	Input the password.
Status	Show the link status: Connect or Disconnect.

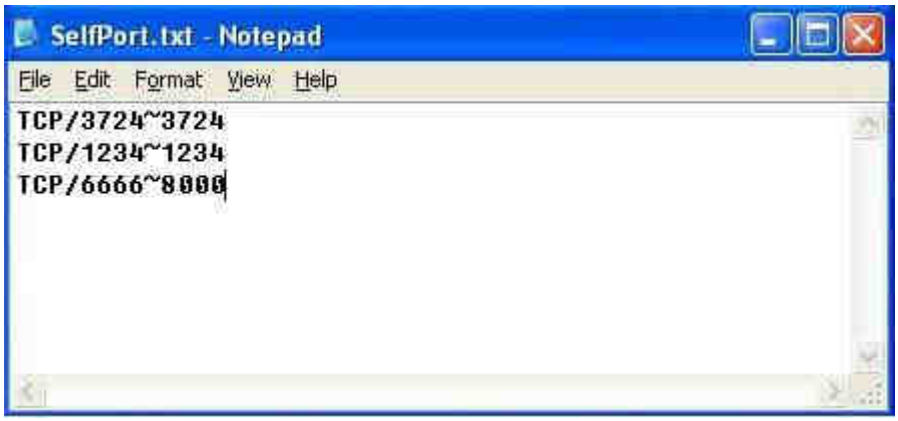
Self-Defined IP

To build a self-defined IP 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 IPs 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.



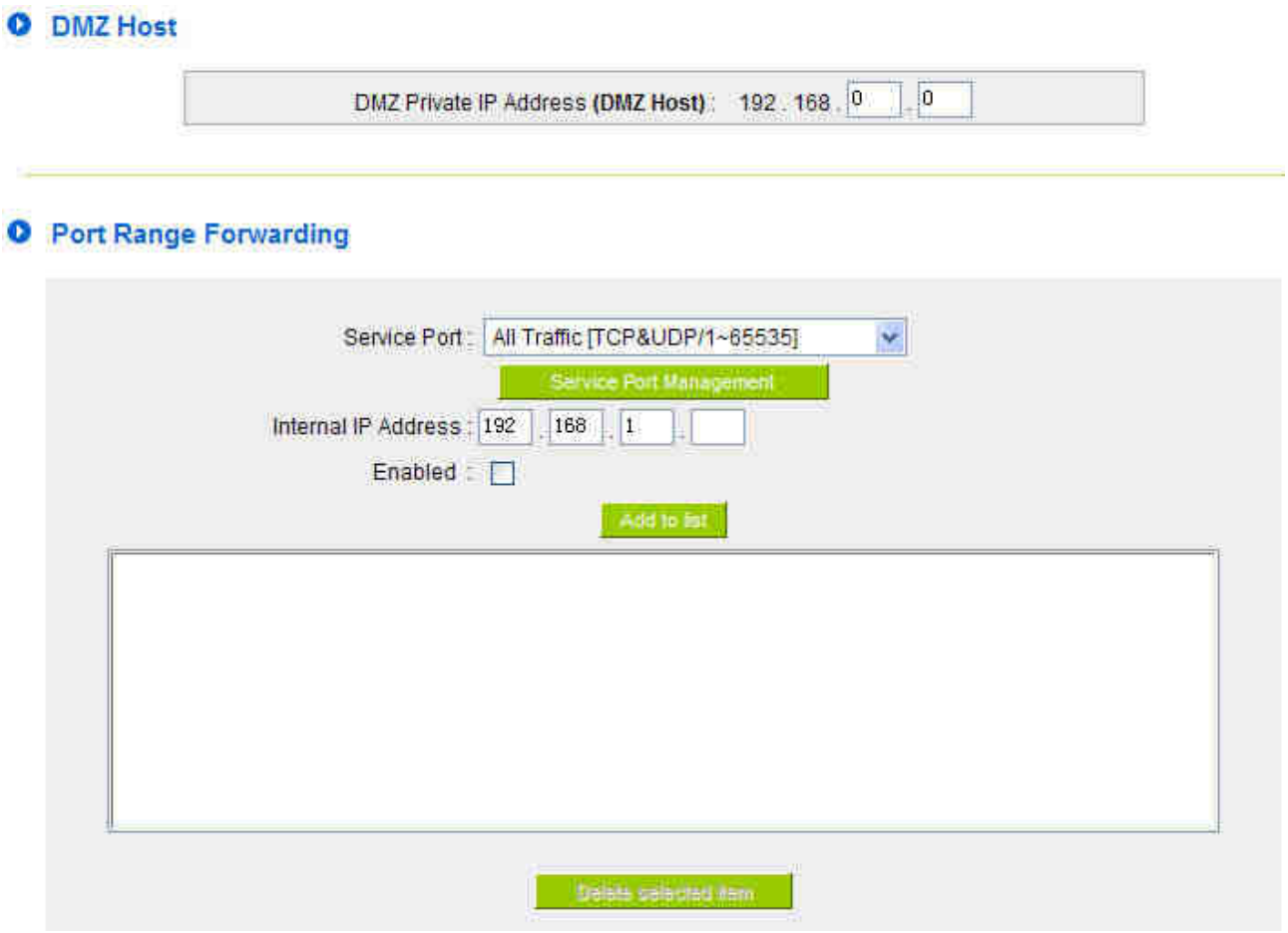
Self-Defined Port

To build a self-defined Port users can use a text-based editor, such as Notepad, which is included with Windows system. For example, if the destination port users want to designate is TCP/3724~3724, key in TCP/3724~3724 in Notepad. The next destination port should be keyed in the next line. After the document has been saved (the extension file name is .txt), users can import the port of self-defined strategy.


SelfPort.txt - Notepad
File Edit Format View Help
TCP/3724~3724
TCP/1234~1234
TCP/6666~8000

10、Advanced Setting

10.1 DMZ Host / Forwarding



10.1.1 DMZ Host

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

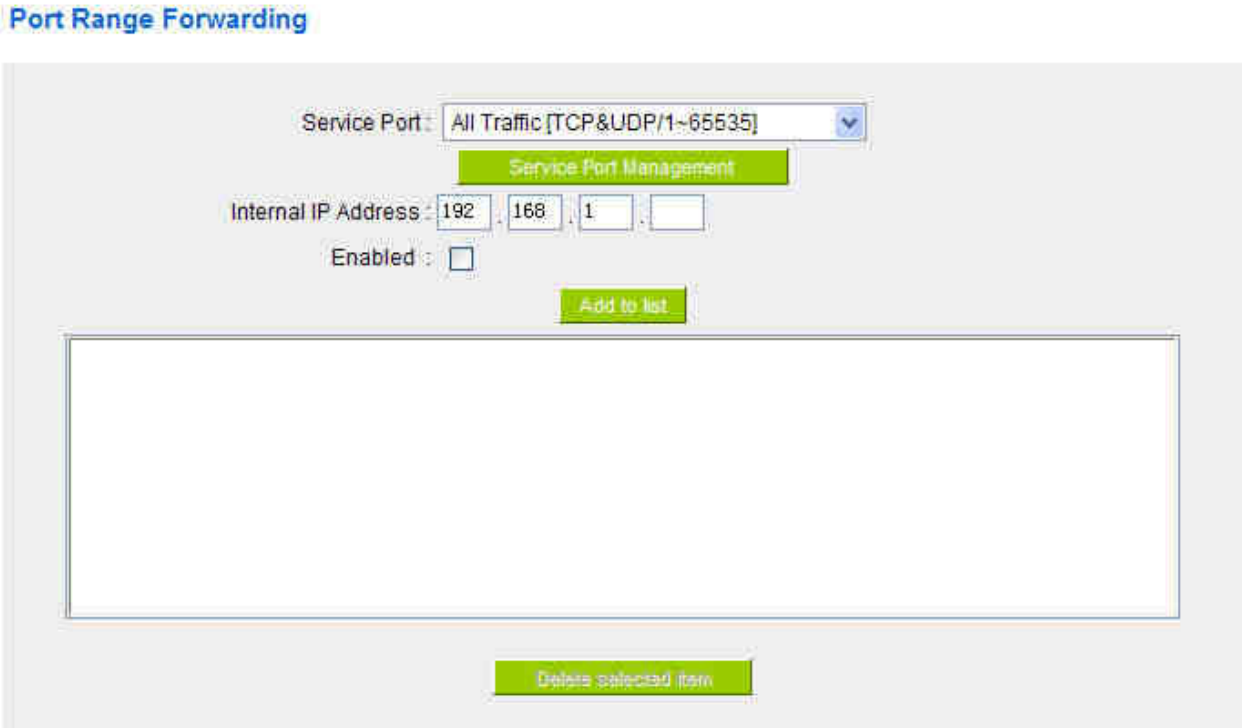
After the changes are completed, click "**Apply**" to save the network configuration modification, or click "**Cancel**" to leave without making any changes.

10.1.2 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 IPs (the Internet IPs) 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 have 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.

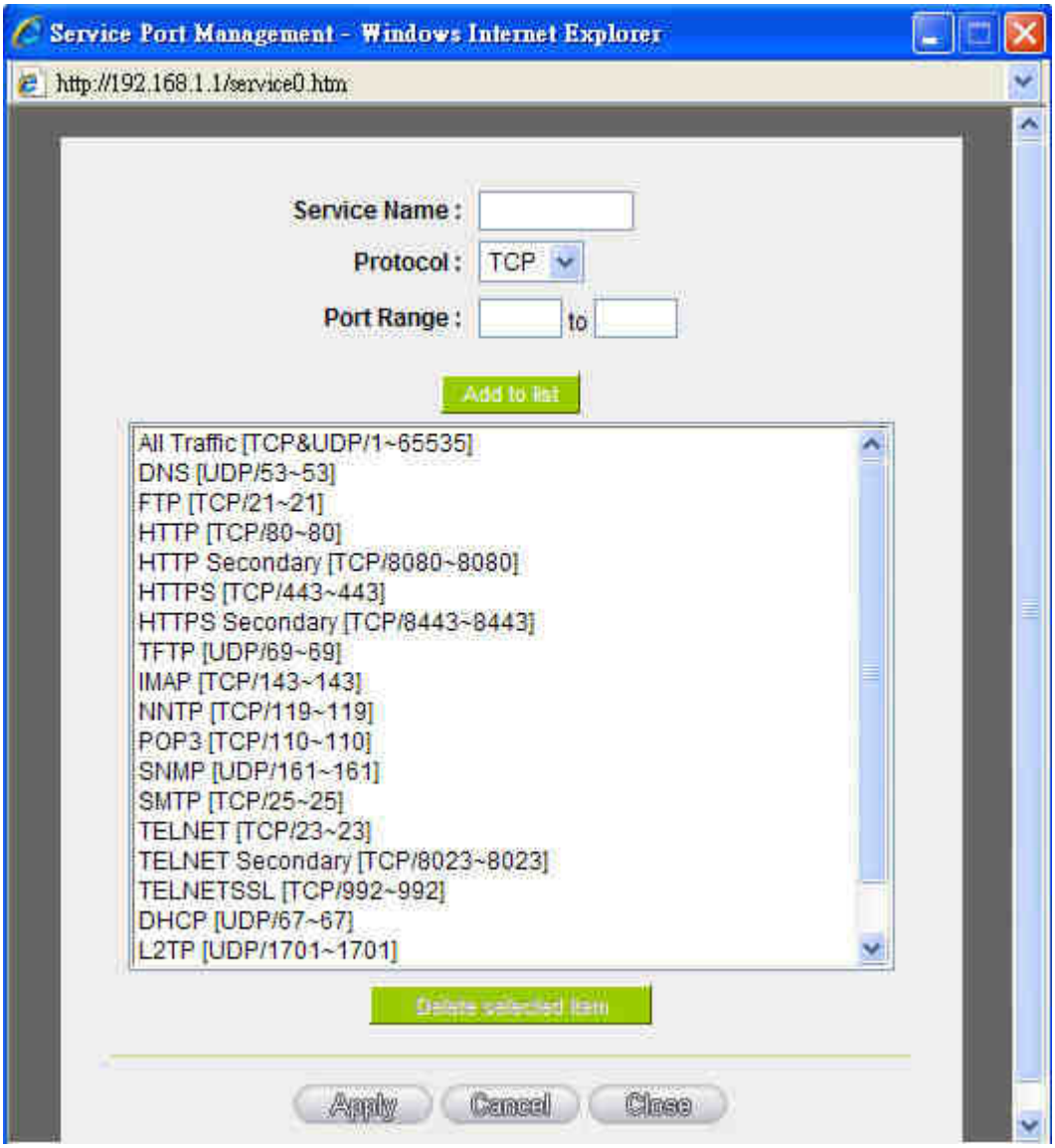


Service:	To select from this option the default list of service ports of the virtual host that users want to activate. Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and 21~21 for FTP. Please refer to the list of default service ports.

Internal IP Address:	Input the virtual host IP addresses.
Enable:	To 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 Management" to add or remove ports, as follows:

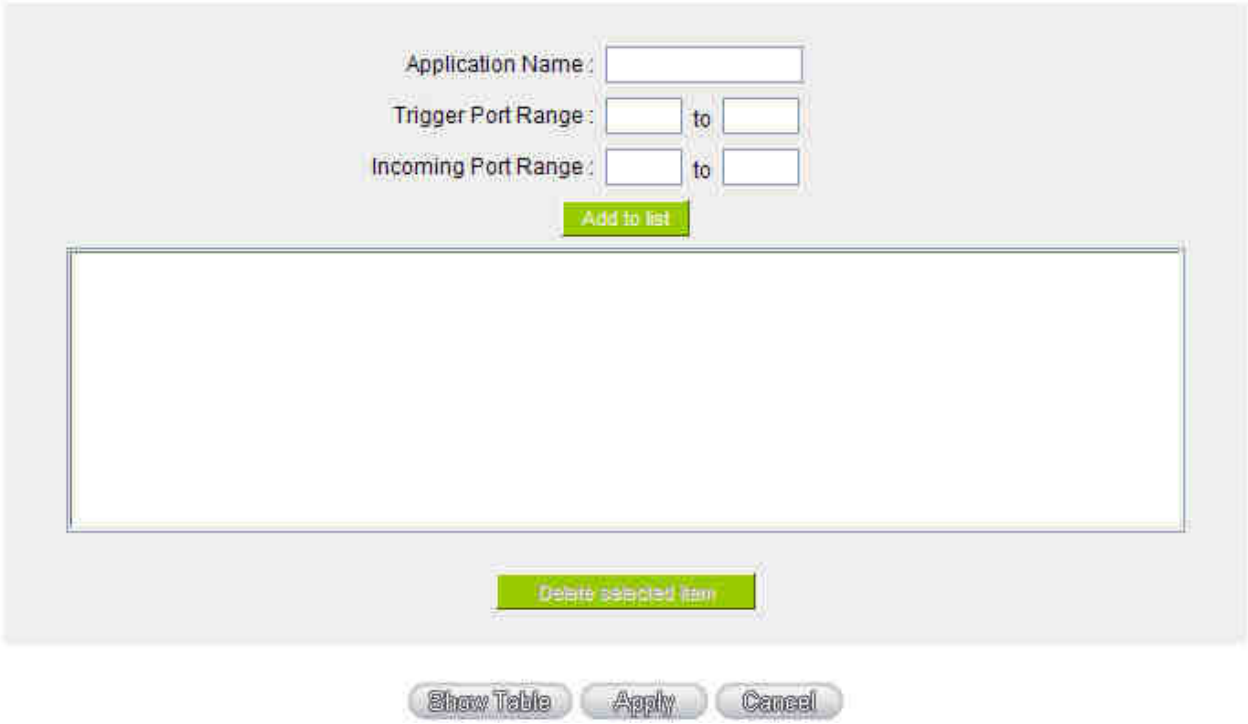


Service Name:	Input the name of the service port users want to activate on the list, such as Edonkey, etc.
Protocol:	To select whether a service port is TCP or UDP.
Port Range:	To activate this function, input the range of the service port locations users want to activate such as 500~500 or 2300~2310, etc.
Add To List:	Add the service to the service list.
Delete Selected Services:	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.
Exit:	To quit this configuration window.

10.1.3 Port Triggering

For some special application software, the Internet accessing port numbers are unsymmetrical. Therefore, the port numbers for this special software must be input in the "Port Triggering", as in the above fig.

Port Triggering



Application Name	Users can define names for special application software. This is to make management simple.
Trigger Port Range	Input the port numbers for data going from the device to the Internet. (Such as 9000~6600).
Incoming Port Range	Input the port numbers for data coming in from the Internet to the device. (Such as 2004~2005).
Add to list	Add the service to the active service list.
Delete selected application	To remove selected services.

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

The following are frequently used ports that have to be configured with the functions introduced above.

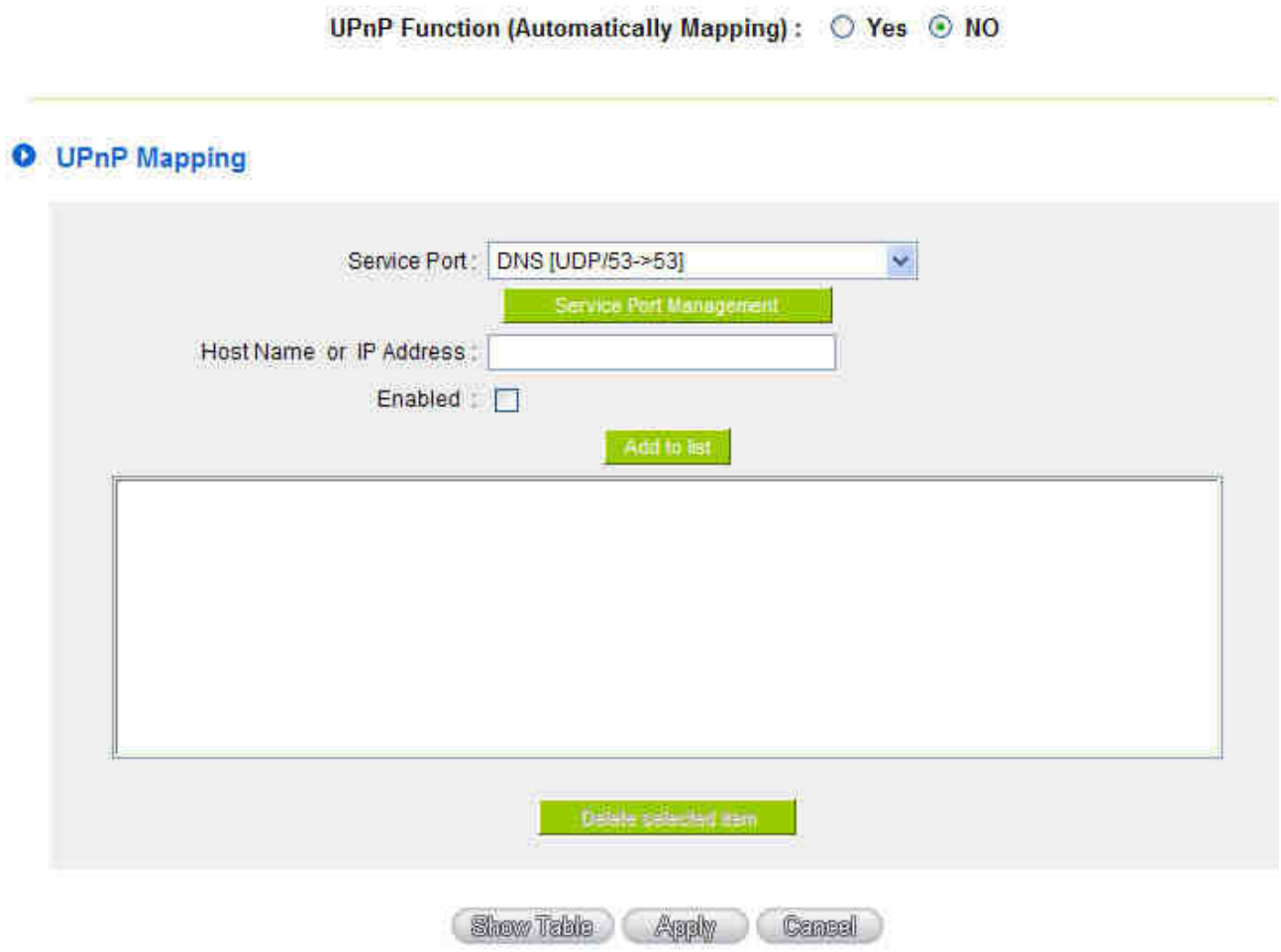
Application	**Outgoing Control**	**Incoming Data**
Battle.net	6112	6112
DialPad	7175	51200，51201，51210

ICU II	2019	2000-2038，2050-2051 2069，2085，3010-3030
MSN Gaming Zone	47624	2300-2400，28800-29000

10.2 UPnP

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

The function supports UPnP Forwarding. If you want to set a virtual gateway, you can use this fuction or set "**Forwarding**" introduced before. Do not duplicate to configure to prevent interfering.



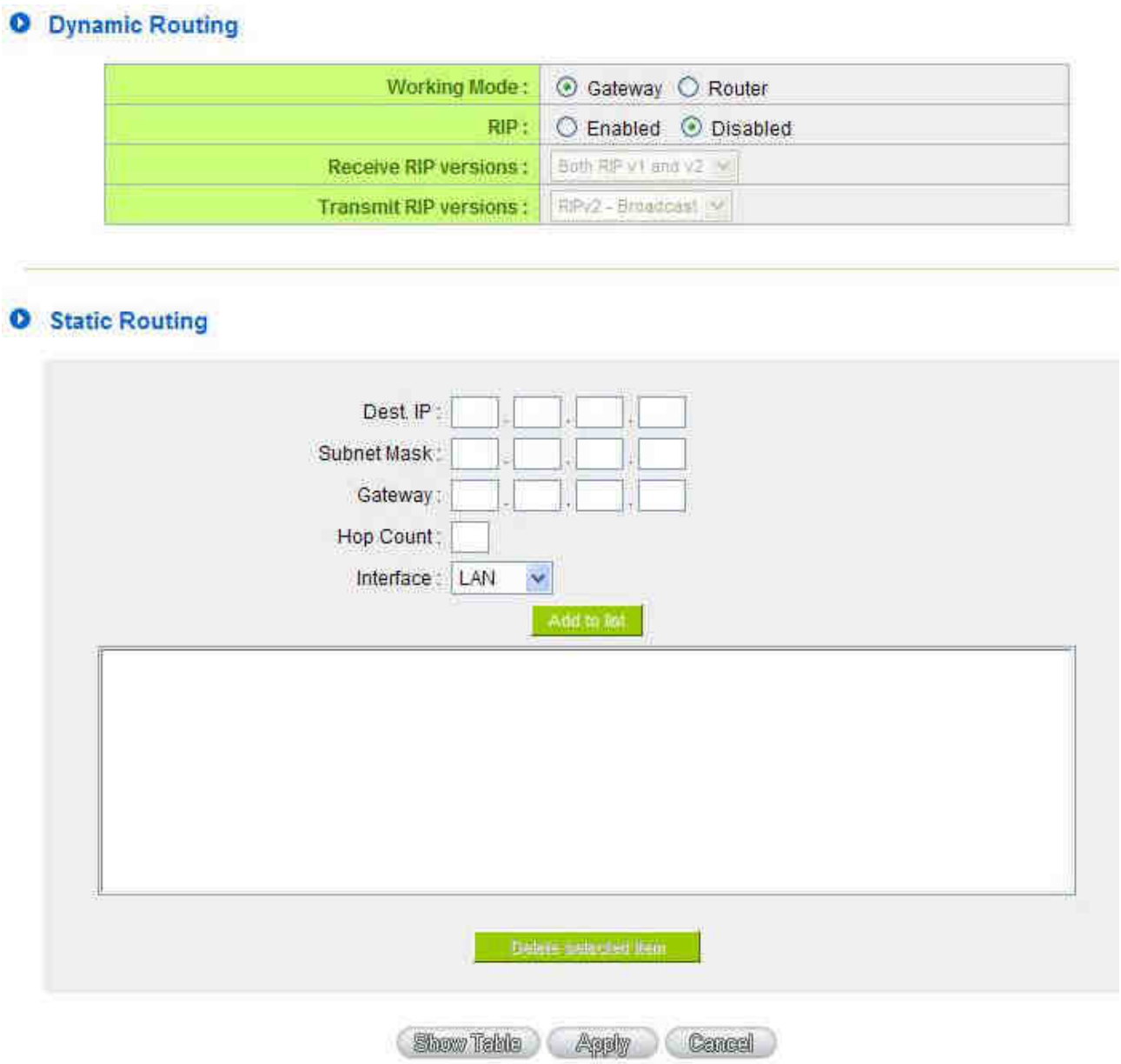
Service:	To select the UPnP service number default list here; for example, WWW is 80(80~80), FTP is 21~21. Please refer to the default service number list.
Host Name or IP Address:	Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.

Enabled:	To activate this function.
Service Management:	Add or remove service ports from the management list.
Add To List:	Add to active service content.
Delete selected item:	To remove selected services.
Show Tables:	This is a list which displays the current active UPnP functions.

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

10.3 Routing

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



10.3.1 Dynamic Routing Information Protocol

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 to 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

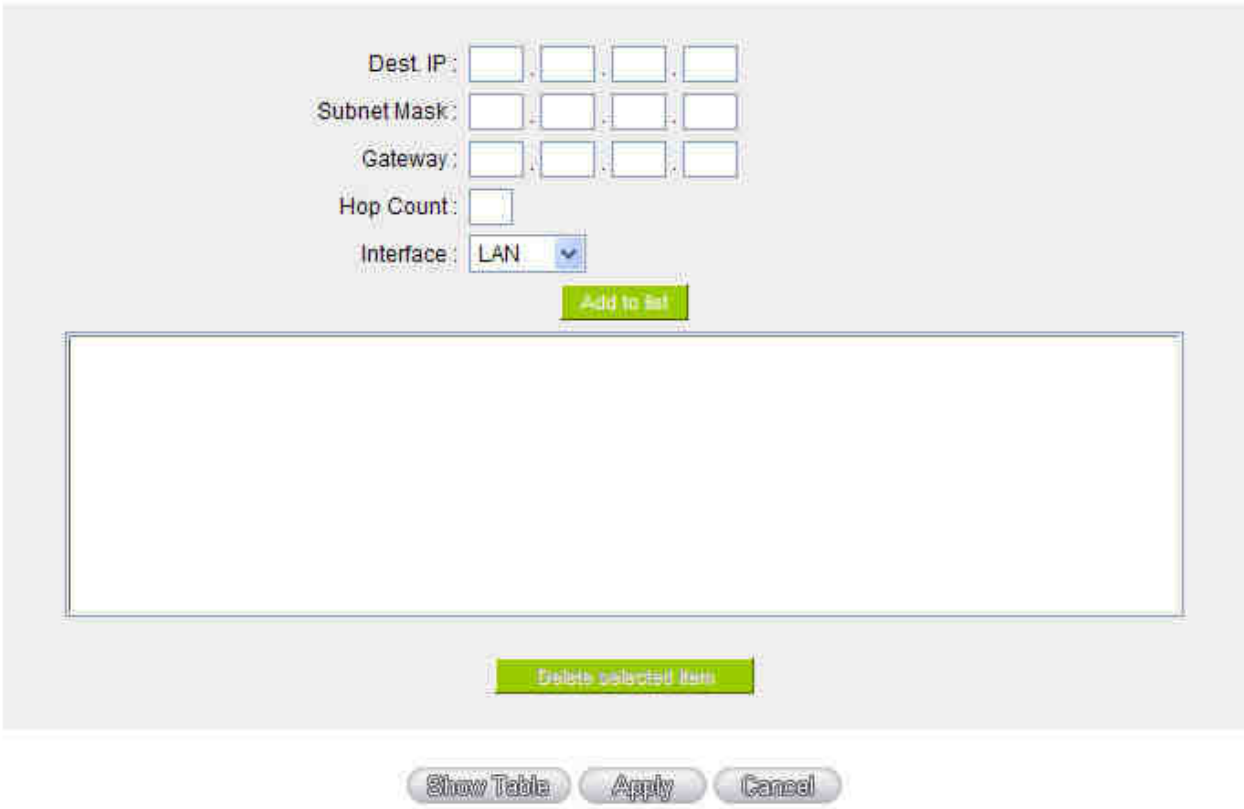
Working Mode:	To select the working mode of the device: NAT mode or router mode.
RIP:	Click "Enabled" to open the RIP function.
Receive RIP versions:	Use Up/Down button to select one of "**None**， **RIPv1**， **RIPv2**， **Both RIPv1 and v2**" as the "**TX**" function for transmitting dynamic RIP.
Transmit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

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

10.3.2 Static Routing Information Protocol

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



Destination IP and 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.
Default Gateway:	The default gateway location of the network node which is to be routed. Such as 192.168.2.1
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:	To add or remove a device.
Display selected IP:	To display the current routing list.

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

10.4 One-to-One NAT Mapping

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 IPs or more), users can map the remaining real IPs to the intranet PC virtual IPs.

Application

If any application such as Network Game, which does not support virtual IP addresses, is used, we recommend that users map the actual Internet IP directly to the virtual Intranet IP. Follow the next example to input IP addresses:

Example

Users have five available IPs - 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 IPs 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.

One-to-One NAT:	To activate or close the One-to-One NAT function. (Check to activate the function).
Private IP Range Begin:	To input the Private IP address for the Intranet One-to-One NAT function.
Public IP Range Begin:	To input the Public IP address for the Internet One-to-One NAT function.
Range Length:	The numbers of final IPs of actual Internet IPs. (Please do not include IPs in use by WANs.)
Add To List:	Add this configuration to the One-to-One NAT list.
Delete selected Item:	To remove a selected One-to-One NAT list.

Attention!

The 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 in Chapter 8 Firewall.

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

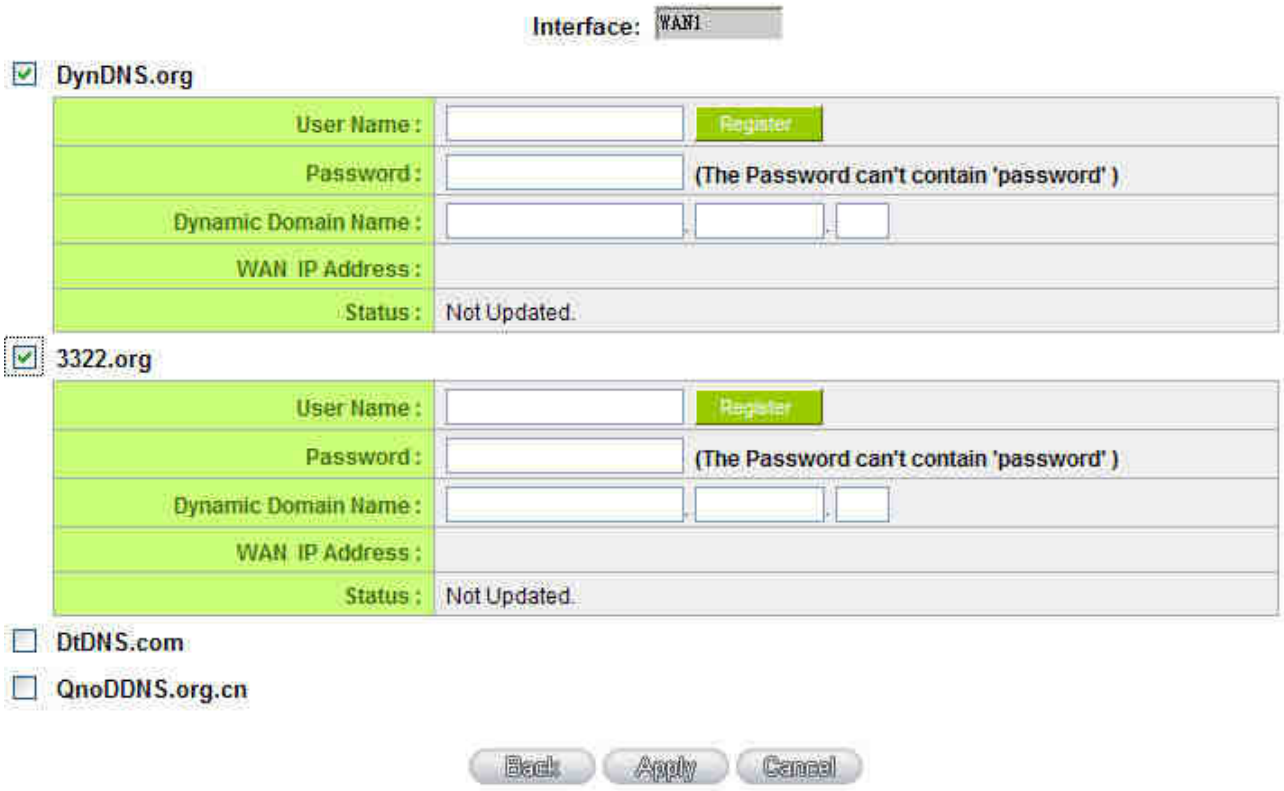
10.5 DDNS (Dynamic Domain Name Service)

DDNS supports the dynamic web address transfer for QnoDDNS.org.cn、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.qno.com.tw, www.3322.org, www.dyndns.org, or www.dtdns.com, and these are free.

DDNS

Interface	Dynamic Domain Name	Status	Config.
WAN 1	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Edit
WAN 2	Dyndns:--- 3322:--- Dtdns:--- Qnoddns:---	Dyndns Disabled 3322 Disabled Dtdns Disabled Qnoddns Disabled	Edit

Click the hyperlink "**Edit**" of the respective configuration to enter it.



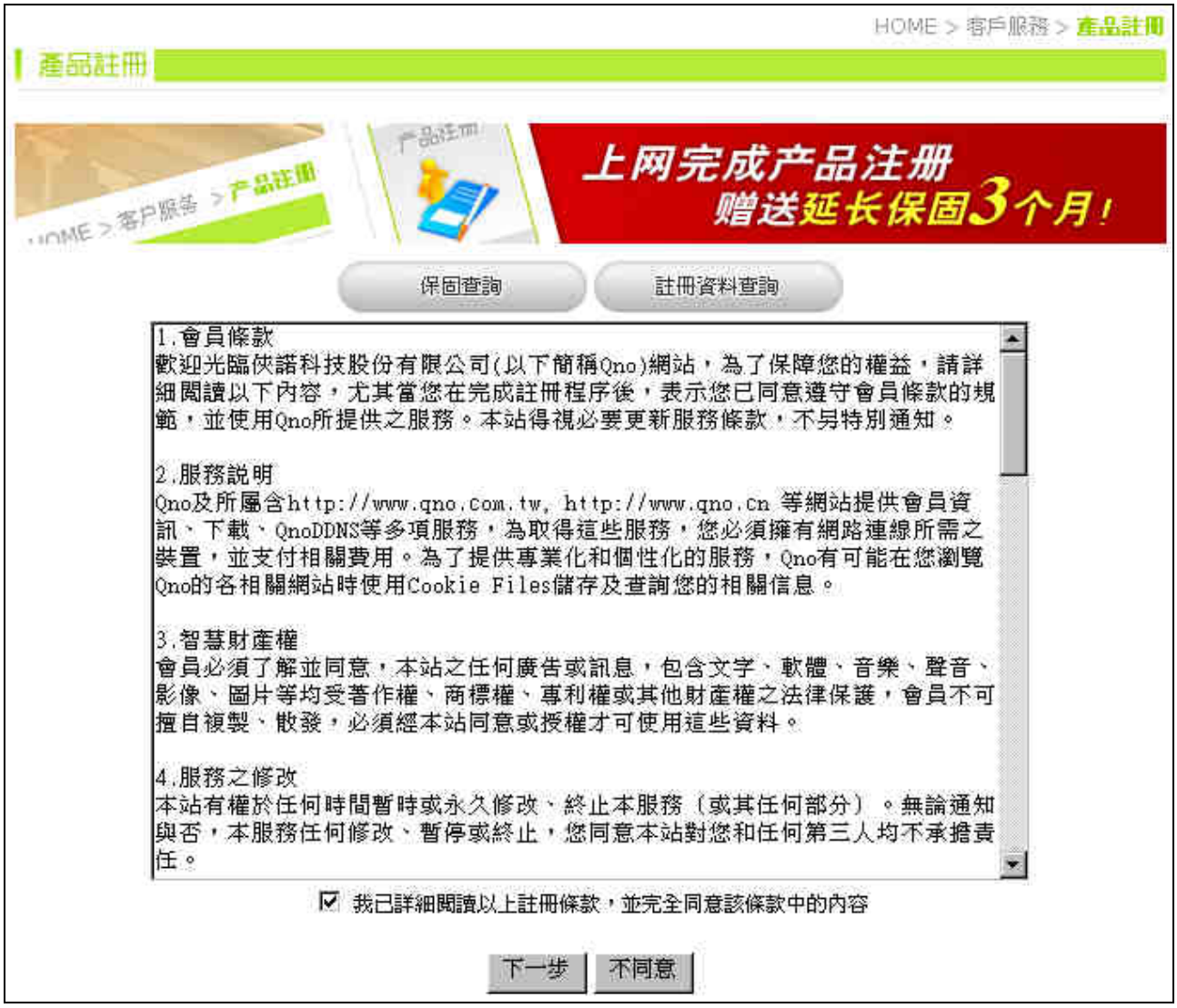
Interface:	This is an indication of the WAN port the user has selected
DynDNS.org 3322.org DtDNS.com QnoDDNS.org.cn	Check either of the boxes before DynDNS.org, 3322.org, DtDNS.com and QnoDDNS.org.cn to select one of the four DDNS website address transfer functions.
User Name:	The name which is set up for DDNS. **Input a complete website address such as abc.qnoddns.org.cn as a user name for QnoDDNS.**
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.
Internal 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.

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

Registering Qno DDNS

1 · First, go to Qno's web site http : //www.qno.com.tw to register the product.



2 · Input the e-mail address which users used to register this product and the product's serial number to log in to the QnoDDNS Service System.

Be sure to input an available e-mail address so that the password sent from the system to activate QnoDDNS service can be received after the domain name registration.

3. The Rule for Applying a Domain Name:

- The Domain should have at least four letters and no more than 63 letters.
- The Domain name should only consist of a-z (lowercase letter) and 0-9 (numerals) and the first character should be an English letter.
- The Domain name should not contain special symbols such as **"."**, **"-"**, **"_"**, etc.
- For products with two WANs, users can apply no more than two DDNS configurations.
- For products with four WANs, users can apply no more than four DDNS configurations.
- For products with eight WANs (or over), users can apply no more than four DDNS configurations.

:: 使用者資料 ::

姓名	
Email	
序號	
型號	
Wan數量	
目前登入IP	
伺服器時間	

:: 申請規則 ::

1. 如果您申請QnoDDNS服務，代表"您無條件同意" Qno倪諾科技動態網域名稱服務條款。
2. "使用者名稱" 最少需要4個字，最多63個字(4-63個字)。
3. "使用者名稱" 只能由a-z(英文小寫)、0-9(數字)所組成，且第一個字需爲英文字母。
4. "使用者名稱" 內不允許含有 'qno'、'dns'的英文字母在內！
5. "使用者名稱" 不得有特殊符號(例如："."；"-"；"_"…等等)。(範例)
6. 2 Wan 系列產品最多申請 2 組DDNS設定。
7. 4 Wan 系列產品最多申請 4 組DDNS設定。
8. 8 Wan 系列產品最多申請 4 組DDNS設定。
9. 設定 QnoDDNS 之前，請先確認產品之 "系統時間" 正確，請參考系統時間、時間設置。
10. 如果您無法透過網路使用NTP服務來更新路由器時間，請參考伺服器時間來手動更新。
11. Qno NTP Server：1. ntp.qnoddns.org.cn 2. ntp.ddns.org.cn
12. 其他NTP Server：1. 香港天文台 2. 台灣中華電信研究所 3. 國際亞洲NTP Server。
13. 其他注意事項請參考 QnoDDNS服務使用教學。

:: 使用者名稱測試 ::

已輸入0個字

測試 使用者名稱： 網域名稱： qnoddns.org.cn 送出 重設

尚可申請 4 組DDNS

已輸入0個字

第1組 使用者名稱： 網域名稱： qnoddns.org.cn 申請

已輸入0個字

第2組 使用者名稱： 網域名稱： qnoddns.org.cn

已輸入0個字

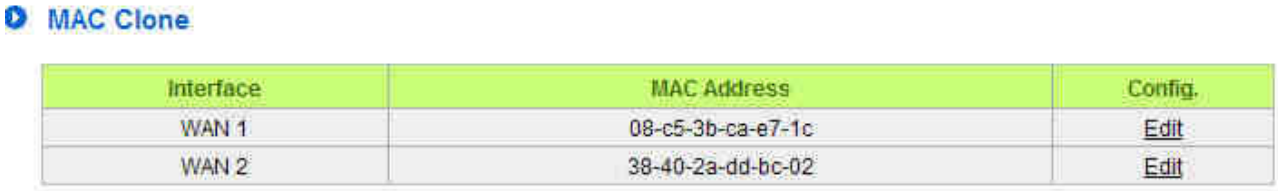
第3組 使用者名稱： 網域名稱： qnoddns.org.cn

已輸入0個字

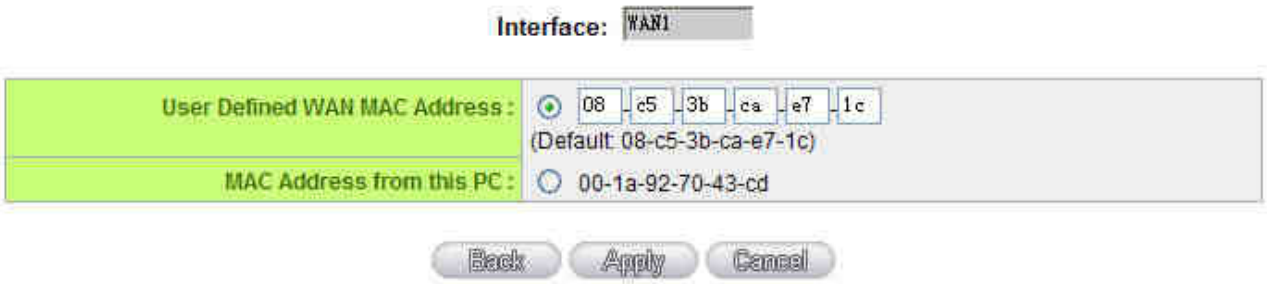
第4組 使用者名稱： 網域名稱： qnoddns.org.cn

10.6 MAC Clone

This function is mainly for two-way cable modem users so that if the network card is locked, users can input the original network hardware address (MAC Address:00-xx-xx-xx-xx-xx) to unlock the card.



Select the WAN port to which the configuration is to be edited; click the hyperlink to enter and edit its configuration.



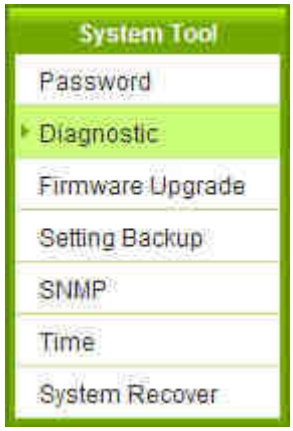
Interface:	This is an indication of the WAN port the user selects
Enabled Disabled	Check the option to activate or disable this function.
User Defined WAN MAC Address:	The default MAC location of the current equipment.
MAC Address from connected device:	Current address of MAC that is connected with this PC.

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

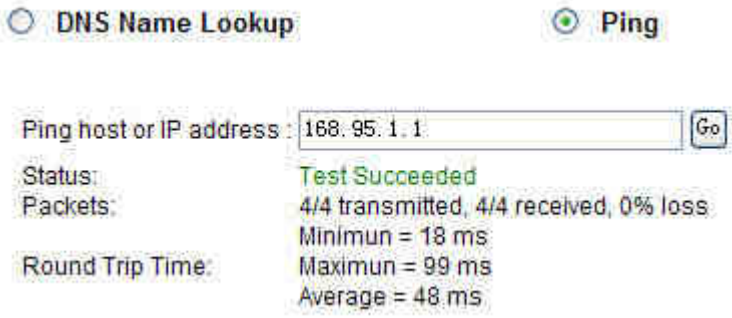
11、System tools, ports and security settings

This chapter introduces operation methods of some tools, port management and network security settings. These settings facilitate user management of the device and device ports so as to enhance the device security.

11.1 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).



Domain Name Inquiry Test (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.abc.com and press "Go" to start the test. The result will be displayed on this page.

Ping - Packet Delivery/Reception Test

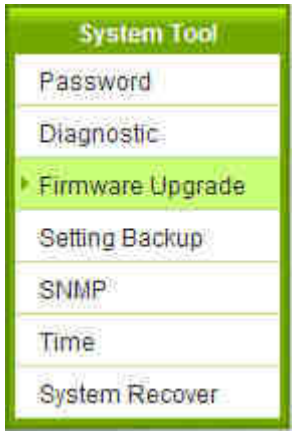
This item informs users of the status quo of the outbound session and allows the user

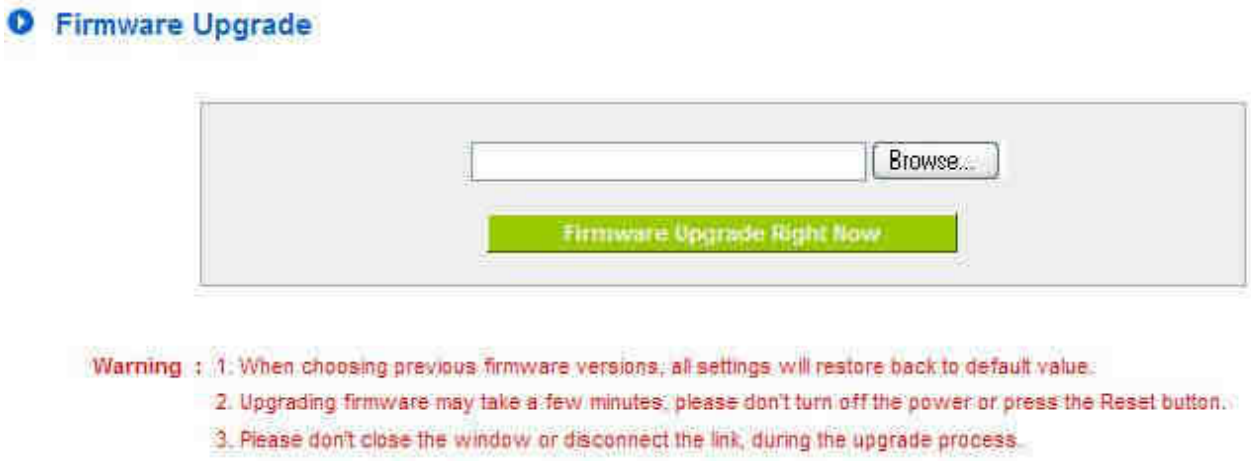
to know the existence of computers online. On this test screen, please enter the host IP that users want to test such as 192.168.5.20. Press "Go" to start the test. The result will be displayed on this screen.

11.2 Firmware Upgrade

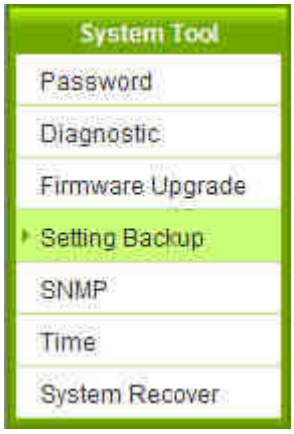
Users may directly upgrade the device firmware on the Firmware Upgrade page. Please confirm all information about the software version in advance. Select and browse the software file, click **"Firmware Upgrade Right Now"** to complete the upgrade of the designated file.

Note: Users must not exit this screen during upgrade. Otherwise, the upgrade may fail.





11.3 Setting 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.

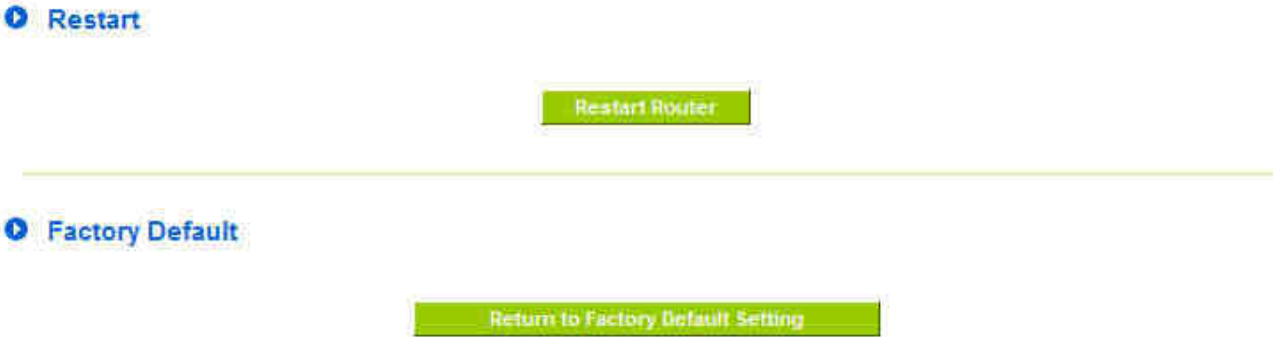
11.4 SNMP

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.

Enabled SNMP:	Activate SNMP feature. The default is activated.
System Name:	Set the name of the device such as QoS Router.
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.

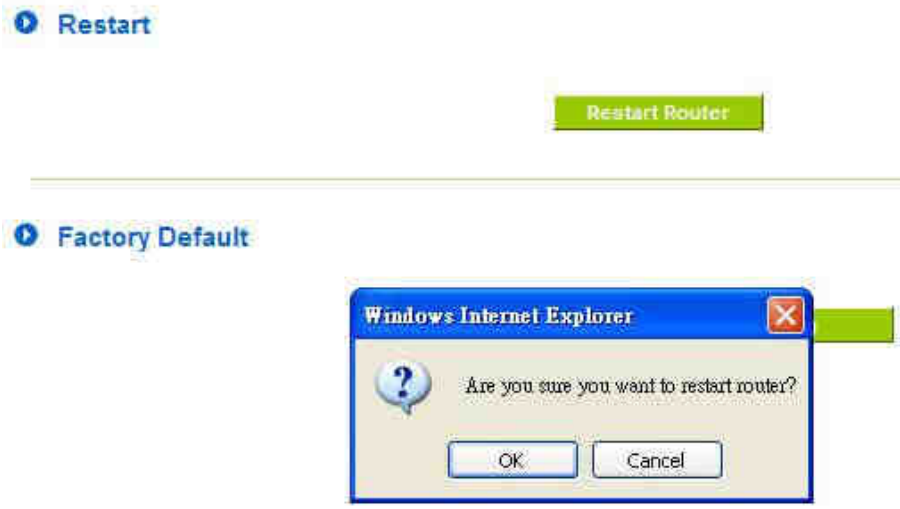
After modification, press "**Apply**" to save the network settings or press "**Cancel**" to keep the settings unchanged.

11.5 System Recovery



Restart

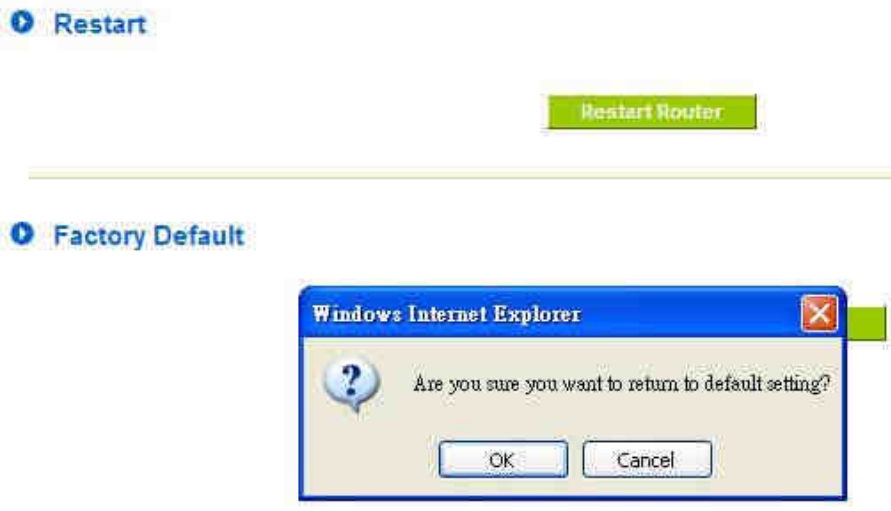
Click "**Restart Router**" to start it again. This operation message will then be recorded in system log. Press "**Reset**" on the device panel to reset manually. **Press Reset and hold for 5 seconds** and the device will restart after the yellow light flickers 5 times.



Factory Default

Select "**Return to Factory Default Setting**" to reset all the settings and restart the device. Alternatively, users may press "**Reset**" button on the device to manually restore the default value and clear all settings including port configures, password setting and etc. **Press "Reset" and hold for more than 10 seconds**. The flicker of the yellow light indicates the default value is being restored.

Please note that this feature resets all the data on the device!

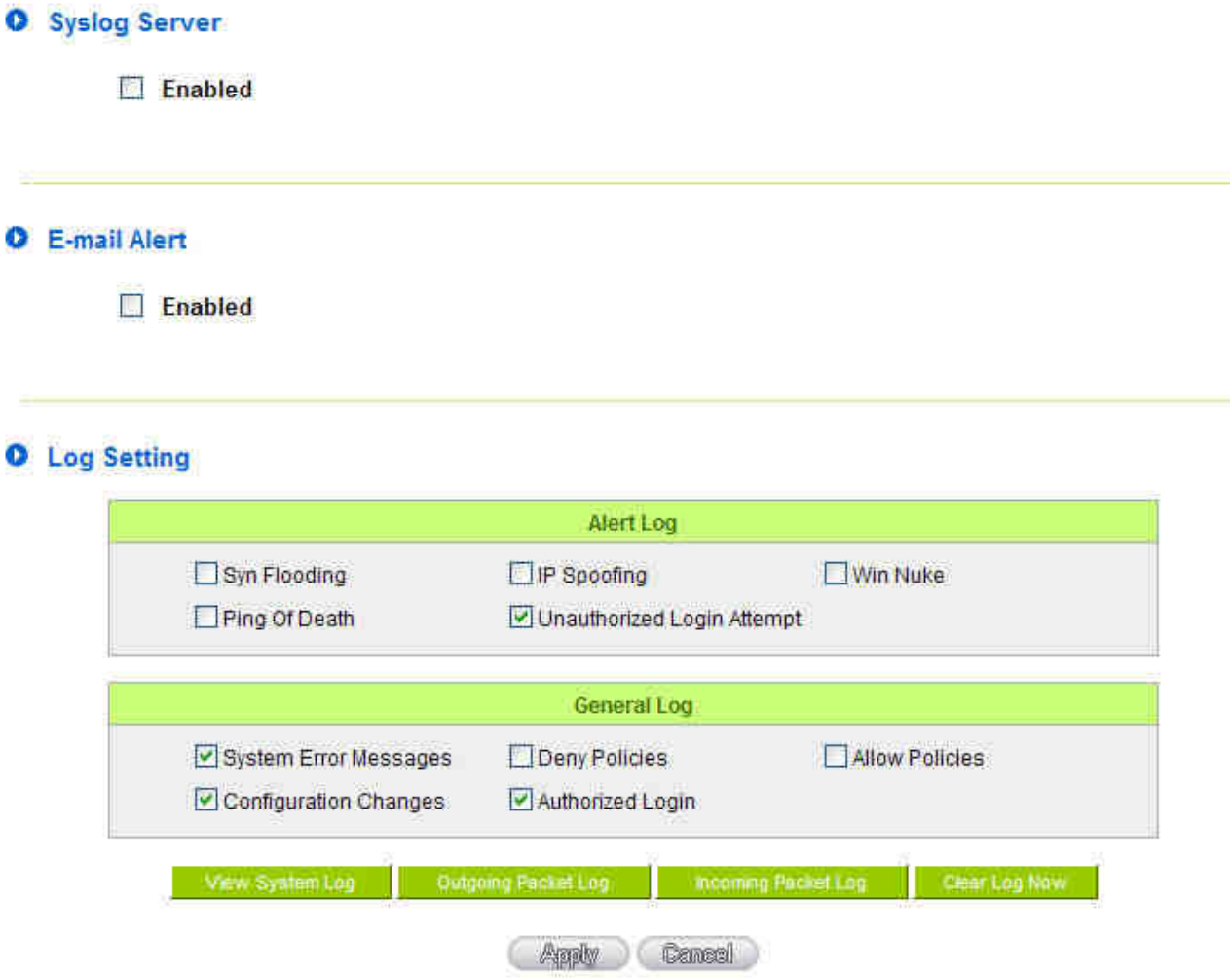


12、Log

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.

12.1 System Log

Its system log offers three options: Syslog Server, E-mail Alert and Log Setting.



Syslog Server

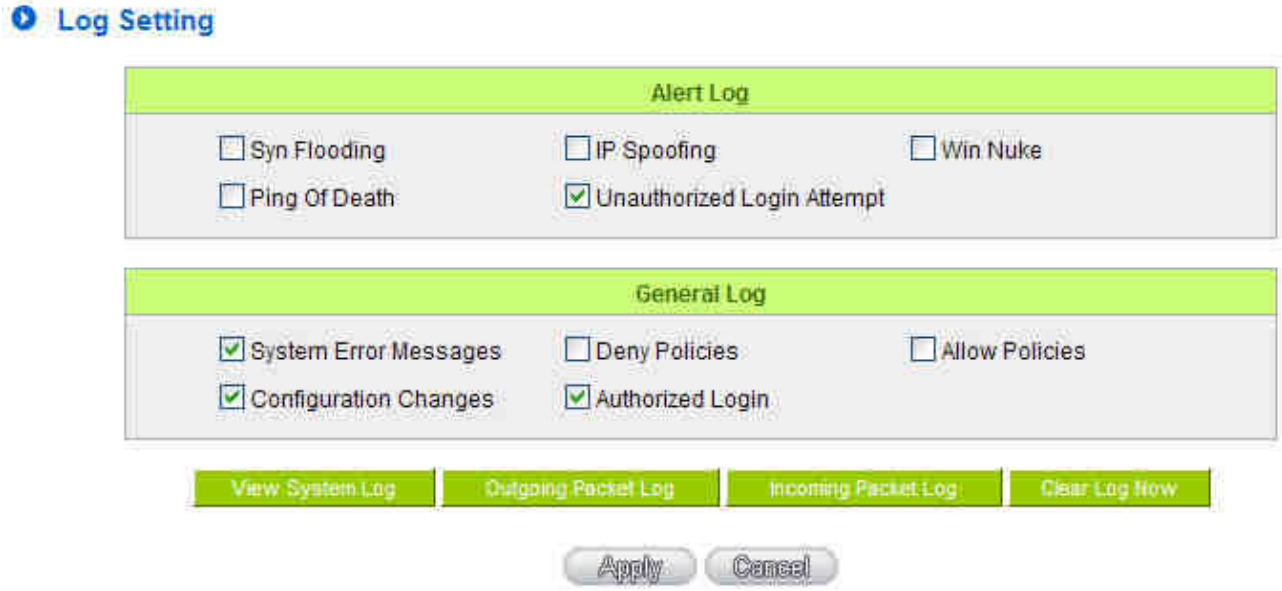
Enabled:	If this option is selected, the SysLog feature will be enabled.
Host Name:	The device provides external system log servers with log collection feature. System log is an industrial standard communications protocol. It is designed to dynamically capture related system message from the network. 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 "Host Name" field.

After modification, press "**Apply**" to save the network setting or press "**Cancel**" to keep the settings unchanged.

E-mail Alert

Enabled:	If this option is selected, E-mail Alert will be enabled.
Mail Server:	If users wish to send out all the logs, please enter the E-mail server name or the IP address, for instance:mail.abc.com
E-mail:	This is set as system log recipient email address such asabc@mail.abc.com
Log Queue Length:	Set the number of Log entries, and the default entry number is 50. When this defined number is reached, it will automatically send out the log mail.
Log Time Threshold:	Set the interval of sending the log, and the default is set to 10 minutes. Reaching this defined number, it will automatically send out the Mail log. The device will detect which parameter (either entries or intervals) reaches the threshold first and send the log message of that parameter to the user.
Send Log to Email:	Users may send out the log right away by pressing this button.

Log Setting



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.

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 Attempt:	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.

System Error Messages:	Provides the system log with all kinds of error messages. For example: wrong settings, occurrence of abnormal functions, system reactivation, disconnection of PPPoE and so on.
Deny Policies:	If remote users fail to enter the system because of the access rules, such message will be recorded in the system log.
Allow policies:	If remote users enter the system because of compliance with access rules, such message will be recorded in the system log.
Configuration Changes:	When the system settings are changed, this message will be sent back to 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.

After modification, press **"Apply"** to save the network setting or press **"Cancel"** to keep the settings unchanged.

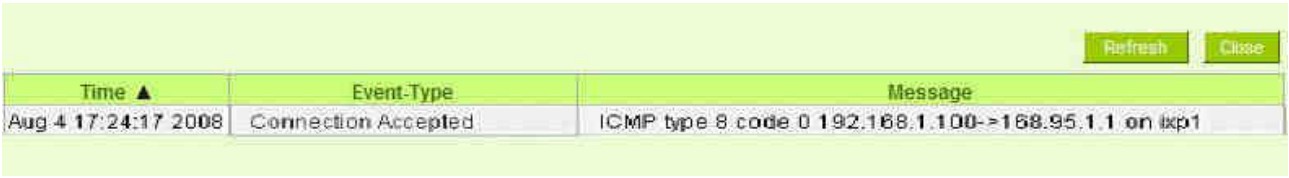
The following is the description of the four buttons allowing online inquiry into the log:

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.

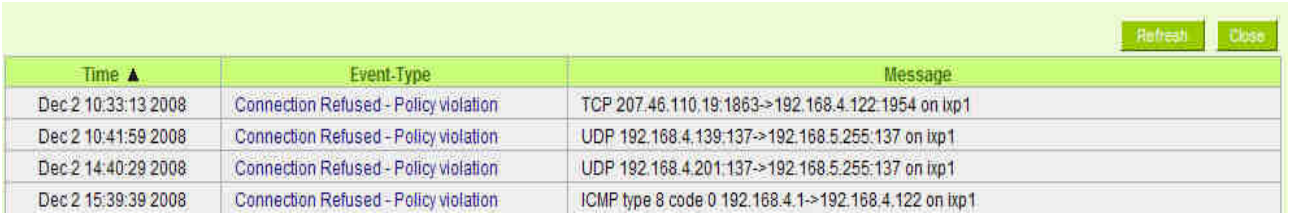
Outgoing Packet Log

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.



Incoming Packet Log

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



Clear Log Now

This feature clears all the current information on the log.

12.2 System Status

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 (%).

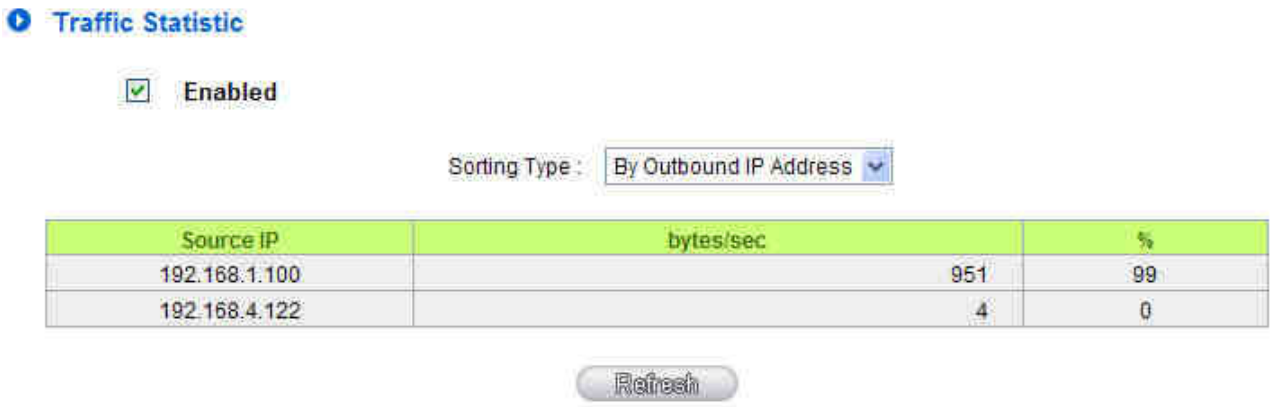
System Status

Interface	WAN 1	WAN 2	LAN
Device Name	ixp1	ixp2	ixp0
Link Status	Connected	Down	Connected
IP Address	192.168.4.122	0.0.0.0	192.168.1.1
MAC Address	08-c5-3b-ca-e7-1c	38-40-2a-dd-bc-02	30-7e-95-99-94-be
Subnet Mask	255.255.254.0	0.0.0.0	255.255.255.0
Default Gateway	192.168.4.1	0.0.0.0	---
DNS Server	192.168.5.21	0.0.0.0	192.168.1.1
Network Service Detection	Test Succeeded	Test Failed	---
Receive Packets Count	71789223	0	72794
Transmit Packets Count	12398611	0	76681
Total Packets Count	84187834	0	149475
Receive Packets Byte Count	71789223	0	13370174
Transmit Packets Byte Count	12398611	0	51769364
Total Packets Byte Count	84187898	0	65139538
Receive Byte/Sec	787	0	64
Transmit Byte/Sec	64	0	126
Error Packets Count	0	0	0
Dropped Packets Count	34384	0	0
Session	7	0	---
New Session/Sec	0	0	---
Upstream Bandwidth Usage(%)	0	0	---
Downstream Bandwidth Usage(%)	0	0	---

Refresh

12.3 Traffic Statistic

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

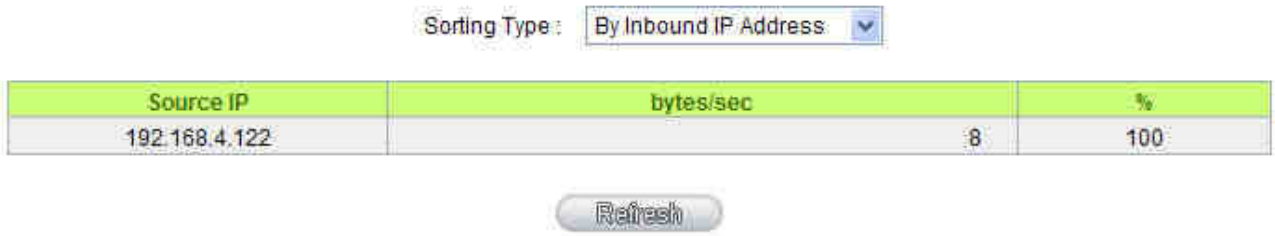


By Onbound IP Address

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

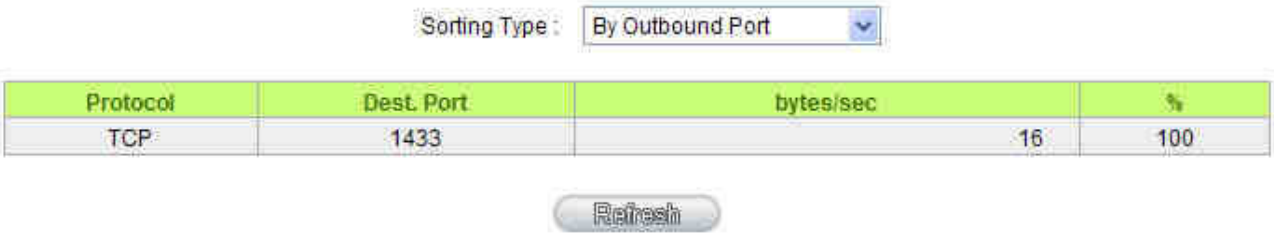
By Iutbound IP Address

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



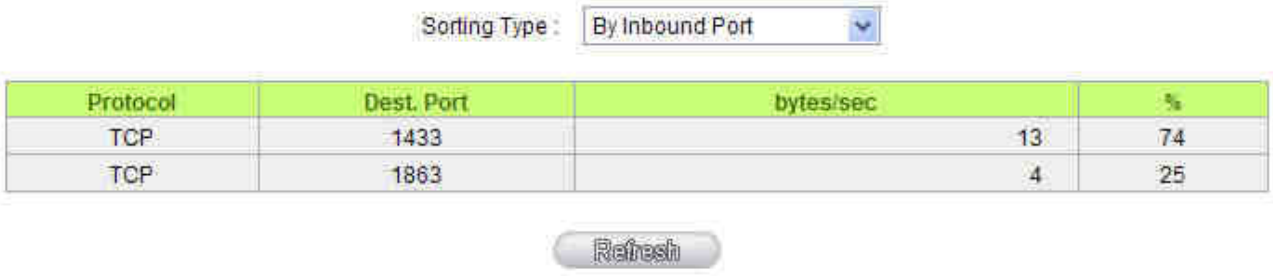
By Outbound Ports

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



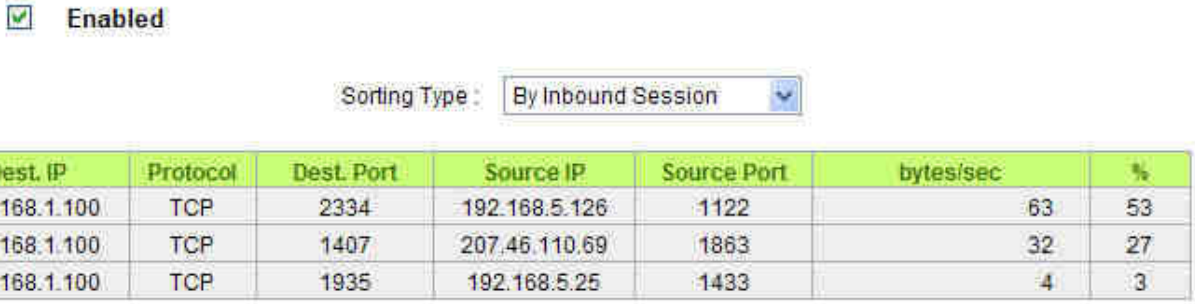
By Inbound Port

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



By Inbound Session

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



By Outbound Session

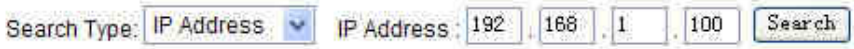
The figure displays the source IP address, network protocol type, source port, destination IP address, destination port, bytes per second and percentage.

12.4 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 single WAN port rather than Multi-WAN. 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 Status

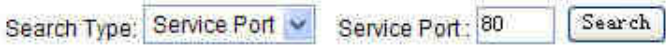
Enter the IP address that users want to inquire, and then the entire destination IP connected to remote devices as well as the number of ports will be displayed.



Source IP	Protocol	Source Port	Interface	Dest. IP	Dest. Port	Downstream Bandwidth Bytes/Sec	Upstream Bandwidth Bytes/Sec
192.168.1.100	TCP	1934	WAN1	192.168.5.25	1433	0	0
192.168.1.100	TCP	1933	WAN1	192.168.5.25	1433	0	0
192.168.1.100	TCP	2334	WAN1	192.168.5.126	1122	0	0
192.168.1.100	TCP	1935	WAN1	192.168.5.25	1433	0	0
192.168.1.100	TCP	2467	WAN1	207.46.108.20	1863	67	9
192.168.1.100	TCP	2495	WAN1	207.46.112.37	443	0	0
192.168.1.100	TCP	2498	WAN1	67.167.203.188	1742	0	0

Service Port

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



Source IP	Protocol	Source Port	Interface	Dest. IP	Dest. Port	Downstream Bandwidth Bytes/Sec	Upstream Bandwidth Bytes/Sec
192.168.1.100	TCP	2469	WAN1	65.55.239.188	80	0	0
192.168.1.100	TCP	2471	WAN1	211.20.179.44	80	0	0
192.168.1.100	TCP	2473	WAN1	124.219.16.136	80	0	0
192.168.1.100	TCP	2475	WAN1	65.55.15.123	80	0	0
192.168.1.100	TCP	2478	WAN1	192.221.68.126	80	0	0

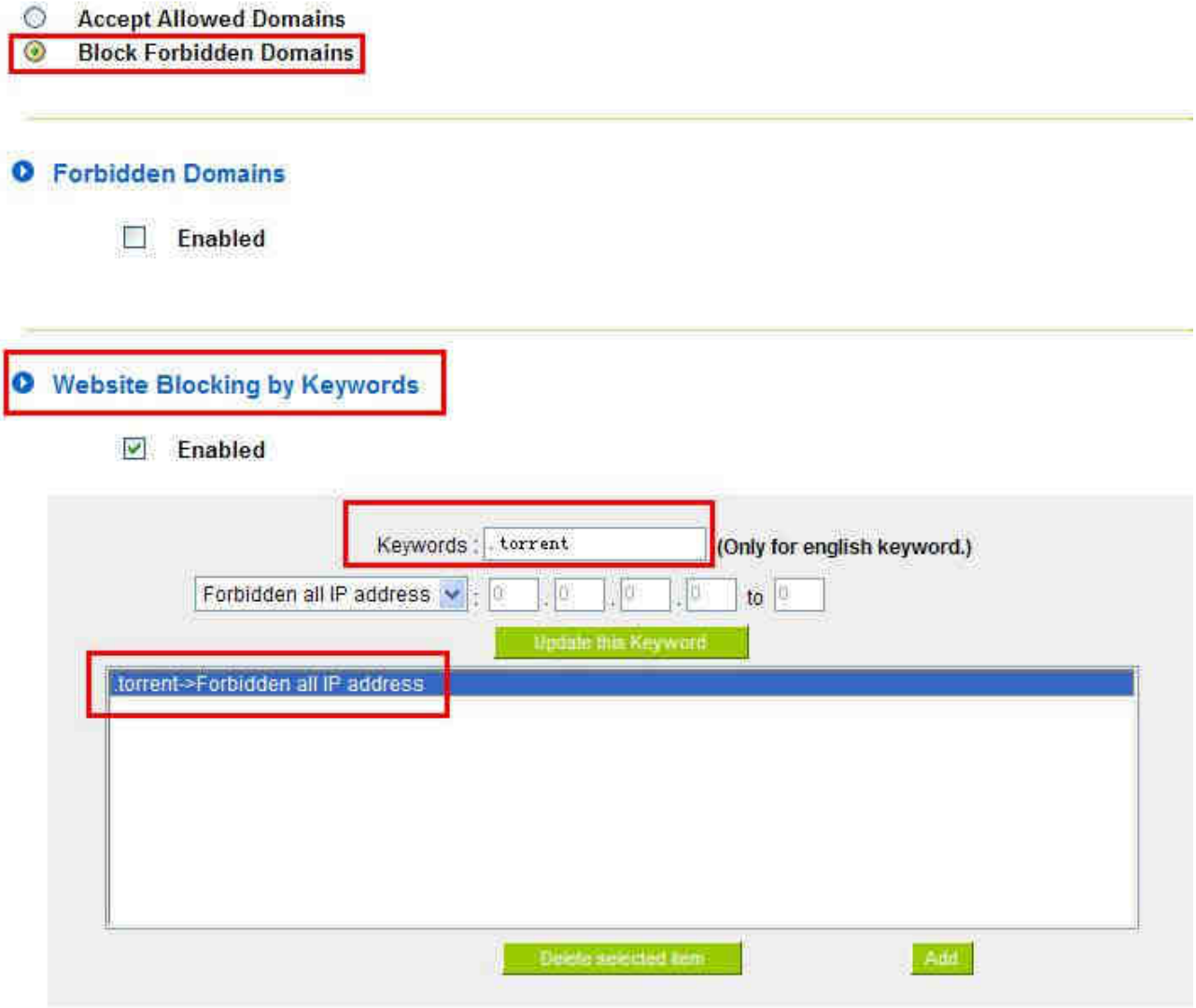
13、Log Out

On the top right corner of the web- based UI, there is a Logout button. Click on it to log out of the web- based UI. To enter next time, open the Web browser and enter the IP address, user name and password to log in.

Appendix 1：TroubleShooting

（1）Block Basic BT Download Method

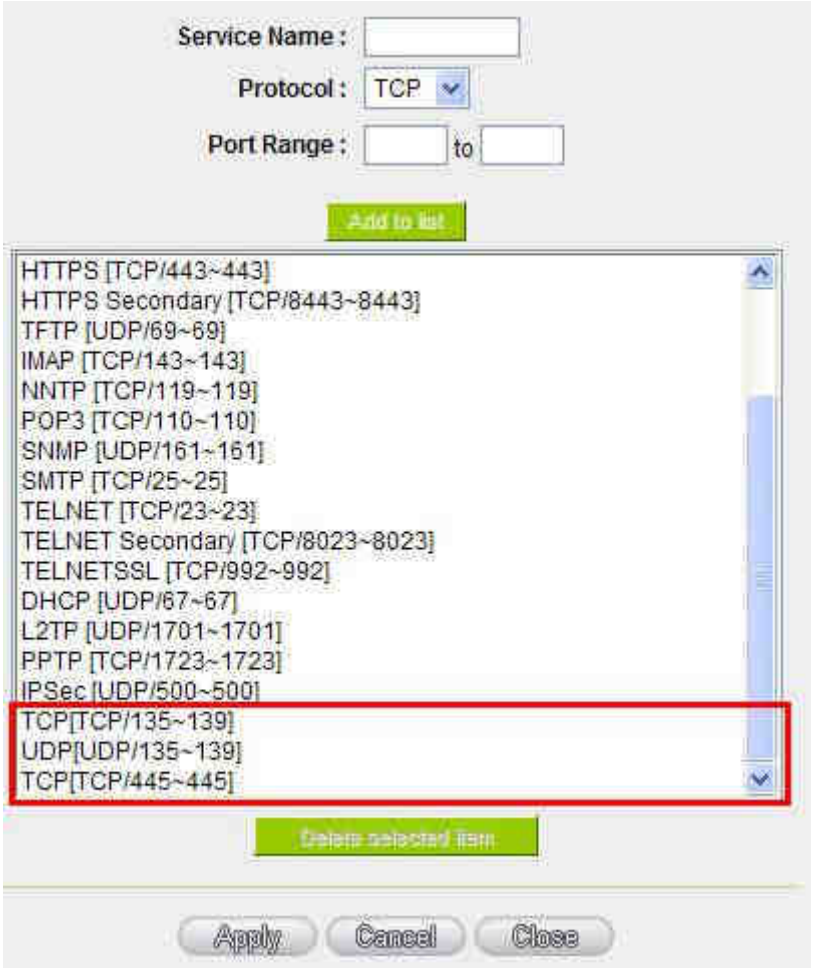
To block BT and prevent downloading by users, go to the "Firewall -> Content Filter" and select "Enable Website Block by Keywords, " followed by the input of ".torrent" This will prevent the users from downloading.



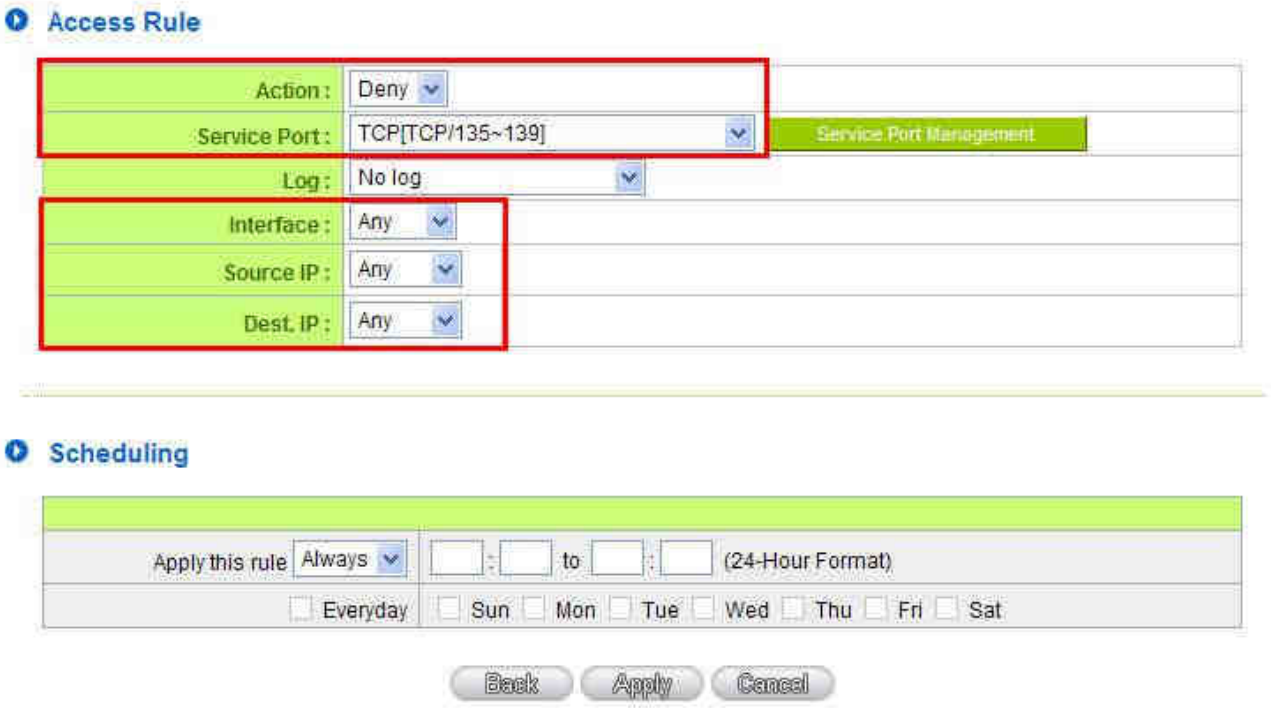
（2） Prevention of Shock Wave and Worm Virus

Since many users have been attacked by Shock Wave and Worm viruses recently, the internet transmission speed was brought down and the Session bulky increase result in the massive processing load of the device. The following guides users to block this virus' corresponding port for prevention.

a. Add this TCP135-139, UDP135-139 and TCP445 Port:



b. Use the "Access Rule" in the firewall and set to block these three ports:



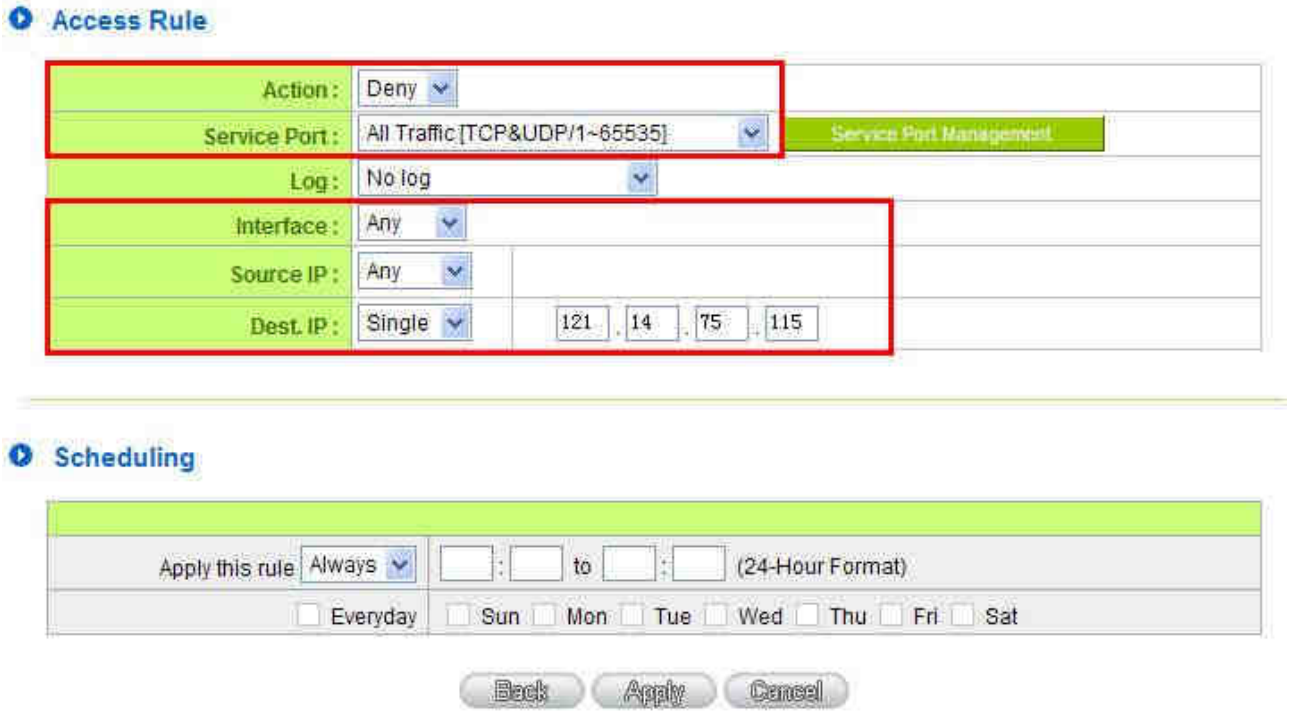
Use the same method to add UDP [UDP135~139] and TCP [445~445] Ports.

c. Enhance the priority level of these three to the highest:

（3） Block QQLive Video Broadcast Setting

QQLive Video broadcast software is a stream media broadcast software. Many clients are bothered by the same problem: When several users apply QQLive Video broadcast software, a greater share of the bandwidth is occupied, thus overloading the device. The device thus responds more slowly or is paralyzed. If the login onto the QQLive Server is blocked, the issue can be resolved. The following relates to Qno products and provides users with solutions by introducing users how to set up the device.

a). Log into the device web- based UI, and enter "Firewall -> Access Rule'.



b). Click "Add New Rule" under "Access Rule" page. Select "Deny" in "Action" under the "Service" rule setting, followed by the selection of "All Traffic [TCP&UDP/1~65535]" from "the service" and select "Any" for Interface, "Any" for source IP address (users with relevant needs may select either "Single" or "Range" to block any QQLive login by using one single IP or IP range), followed by the selection of "Single" of the "Dest. IP and enter the IP address as "121.14.75.115" for the QQLive Server (note that there are more than one IP address for QQLive server. Repeated addition may be needed). Lastly, select "Always" under the Scheduling setting so that the QQLive Login Time can be set. (If necessary, specific time

setting may be undertaken). Click "Apply" to move to the next step.

c). Repeatedly add the "Dest. IP" and enter the IP address as following:

121.14.75.115

60.28.234.117

60.28.235.119

222.28.155.17

This solution is certified to be successful with the version of QQ Live 2008 (7.0.4017.0)

Test Date:2008-07-29

After repeated addition, users may see the links to the QQLive Server are blocked. Click "Apply" to block QQLive video broadcast.

（4） ARP virus attack prevention

1). ARP Issue and Information

Recently, many cyber cafes in China experienced disconnection (partially or totally) for a short period of time, but connection is resumed quickly. This is caused by the clash with MAC address. When virus-contained MAC mirrors to such NAT equipments as host devices, there is complete disconnection within the network. If it mirrors to other devices of the network, only devices of this affected network have problems. This happens mostly to legendary games especially those with private servers. Evidently, the network is attacked by ARP, which aims to crack the encryption method. By doing so, they hackers may intercept the packet data and user information through the analysis of the game's communication protocol. Through the spread of this virus, the detailed information of the game players within the local network can be obtained. Their account and information are stolen. The following describes how to prevent such virus attack.

First, let us get down to the definition of **ARP** (Address Resolution Protocol). In LAN, what is actually transmitted is "frame", in which there is MAC address of the destination host device. So-called "Address Analysis" refers to the transferring process of the target IP address into the target MAC address before the host sends out the frame. The basic function of ARP protocol aims to inquire the MAC address of the target equipment via the IP

address of the target equipment so as to facilitate the communications.

The Working Principle of ARP Protocol: Computers with TCP/IP protocol have an ARP cache, in which the IP address corresponds to the MAC address (as illustrated).

IP Address	MAC Address
192.168.1.1	00-0f-3d-83-74-28
192.168.1.2	00-aa-00-62-c5-03
192.168.1.3	03-aa-01-75-c3-06
……	……

For example, host A (192.168.1.5) transmits data to Host B (192.168.1.1) .Transmitting data, Host A searches for the destination IP address from the ARP Cache. If it is located, MAC address is known. Simply fill in the MAC address for transmission. If no corresponding IP address is found in ARP cache, Host A will send a broadcast. The MAC address is "FF.FF.FF.FF.FF.FF," which is to inquire all the host devices in the same network session about "What is the MAC address of "192.168.1.1"? Other host devices do not respond to the ARP inquiry except host device B, which responds to host device A when receiving this frame: "The MAC address of 192.168.1.1 is 00-aa-00-62-c6-09". So Host A knows the MAC address of Host B, and it can send data to Host B. Meanwhile, it will update its ARP cache.

Moreover, ARP virus attack can be briefly described as an internal attack to the PC, which causes trouble to the ARP table of the PC. In LAN, IP address was transferred into the second physical address (MAC address) through ARP protocol. ARP protocol is critical to network security. ARP cheating is caused by fake IP addresses and MAC addresses, and the massive ARP communications traffic will block the network. The MAC address from the fake source sends ARP response, attacking the high-speed cache mechanism of ARP. This usually happens to the cyber cafe users. Some or all devices in the shop experience temporal disconnection or failure of going online. It can be resolved by restarting the device; however, the problem repeats shortly after. Cafe Administrators can use arp –a command to check the ARP table. If the device IP and MAC are changed, it is the typical symptom of ARP virus attack.

Such virus program as PWSteal. lemir or its transformation is worm virus of the Trojan programs affecting Windows 95/ 98/ Me/ NT/ 2000/ XP/ 2003. There are two attack methods affecting the network connection speed: cheat on the ARP table in the device or

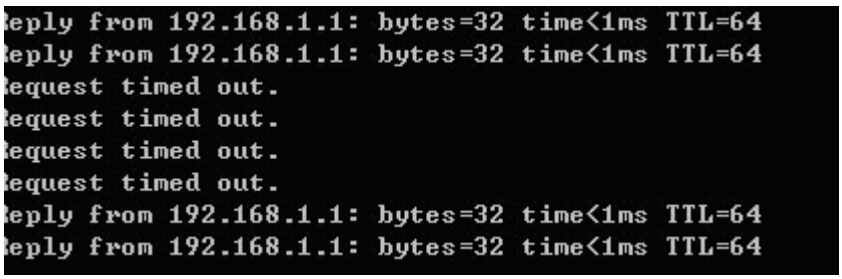
LAN PC. The former intercepts the gateway data and send ceaselessly a series of wrong MAC messages to the device, which sends out wrong MAC address. The PC thus cannot receive the messages. The later is ARP attack by fake gateways. A fake gateway is established. PC which is cheated sends data to this gateway and doesn't go online through the normal device. From the PC end, the situation is "disconnection".

For these two situations, the device and client setup must be done to prevent ARP virus attack, which is to guarantee the complete resolution of the issue. The device selection is advised to take into consideration the one with anti-ARP virus attack. Qno products come squarely with such a feature, which is very user-friendly compared to other products.

2). ARP Diagnosis

If one or more computers are affected by the ARP virus, we must learn how to diagnose and take appropriate measures. The following is experience shared by Qno technical engineers with regard to the ARP prevention.

Through the ARP working principle, it is known that if the ARP cahe is changed and the device is constantly notified with the series of error IP or if there is cheat by fake gateway, then the issue of disconnection will affect a great number of devices. This is the typical ARP attack. It is very easy to judge if there is ARP attack. Once users find the pc point where there is problem, users may enter the DOS system to conduct operation, pining the LAN ip to see the packet loss. Enter the ping 192.168.1.1 (Gateway IP address) as illustrated.



If there are cases of packet loss of the ping LAN IP and lf later there is connection, it is possible that the system is attacked by ARP. To verify the situation, we may judge by checking ARP table. Enter the ARP -a command as illustrated below.

```
Interface: 192.168.1.72 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           00-0f-3d-83-74-28     dynamic
  192.168.1.43          00-13-d3-ef-b2-0c     dynamic
  192.168.1.252         00-0f-3d-83-74-28     dynamic

C:\WINDOWS\System32>arp -a
```

It is found that the IP of 192.168.1.1 and 192.168.252 points to the same MAC address as 00-0f-3d-83-74-28. Evidently, this is a cheat by ARP.

3). ARP Solution

Now we understand ARP, ARP cheat and attack, as well as how to identify this type of attack. What comes next is to find out effective prevention measures to stop the network from being attacked. The general solution provided by Qno can be divided into the following three options:

a) Enable "Prevent ARP Virus Attack":

Enter the device IP address to log in the management webpage of the device. Enter "Firewall-> General" and find the option "Prevent ARP Virus Attack" to the right of the page. Click on the option to activate it and click "Apply" at the bottom of the page (see illustrated).

b) Bind the Gateway IP and MAC address for each PC

This prevents the ARP from cheating IP and its MAC address. First, find out the gateway IP and MAC address on the device end.

LAN Setting

MAC Address :	30 - 7e - 95 - 99 - 94 - be (Default: 30-7e-95-99-94-be)
Device IP Address :	192 . 168 . 1 . 1
Subnet Mask :	255 . 255 . 255 . 0

On every PC, start or operate cmd to enter the dos operation. Enter arp –s 192.168.1.1 0a-0f-d4-9e-fb-0b so as to finish the binding of pc01.As illustrated in Figure 7

```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\PM01>arp -s 192.168.1.1 1c-b1-80-9a-ce-20_
```

For other host devices within the network, follow the same way to enter the IP and MAC address of the corresponding device to complete the binding work. However, if this act restarts the computer, the setting will be cancelled. Therefore, this command can be regarded as a batch of processing documents placed in the activation of the operation system. The batch processing documents can be put in this way:

@echo off

arp -d

arp -s Router LAN IP Router LAN MAC

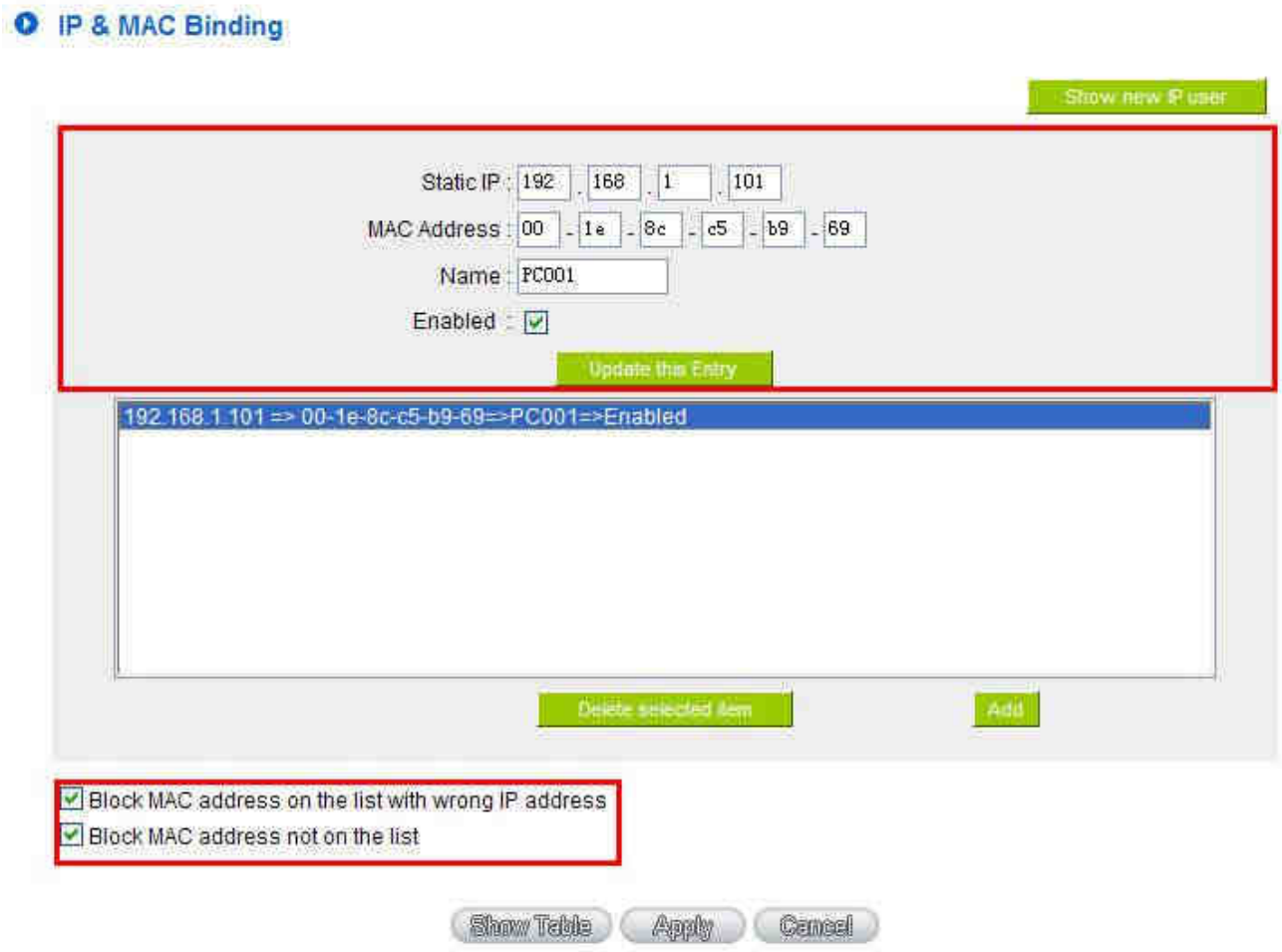
For those internal network attacked by Arp, the source must be identified. Method: If the PC fails to go online or there is packet loss of ping, in the DOS screen, input arp –a command to check if the MAC address of the gateway is the same with the device MAC address. If not, the PC corresponding to the MAC address is the source of attack.

Solutions for other device users are to make a two-way binding of the IP address and MAC address from both of the PC and device ends in order to carry out the prevention work. However, this is more complicated because the search for the IP and address and MAC increases the workload. Moreover, there is greater possibility of making errors during the operation.

c) Bind the IP/MAC Address from Device End:

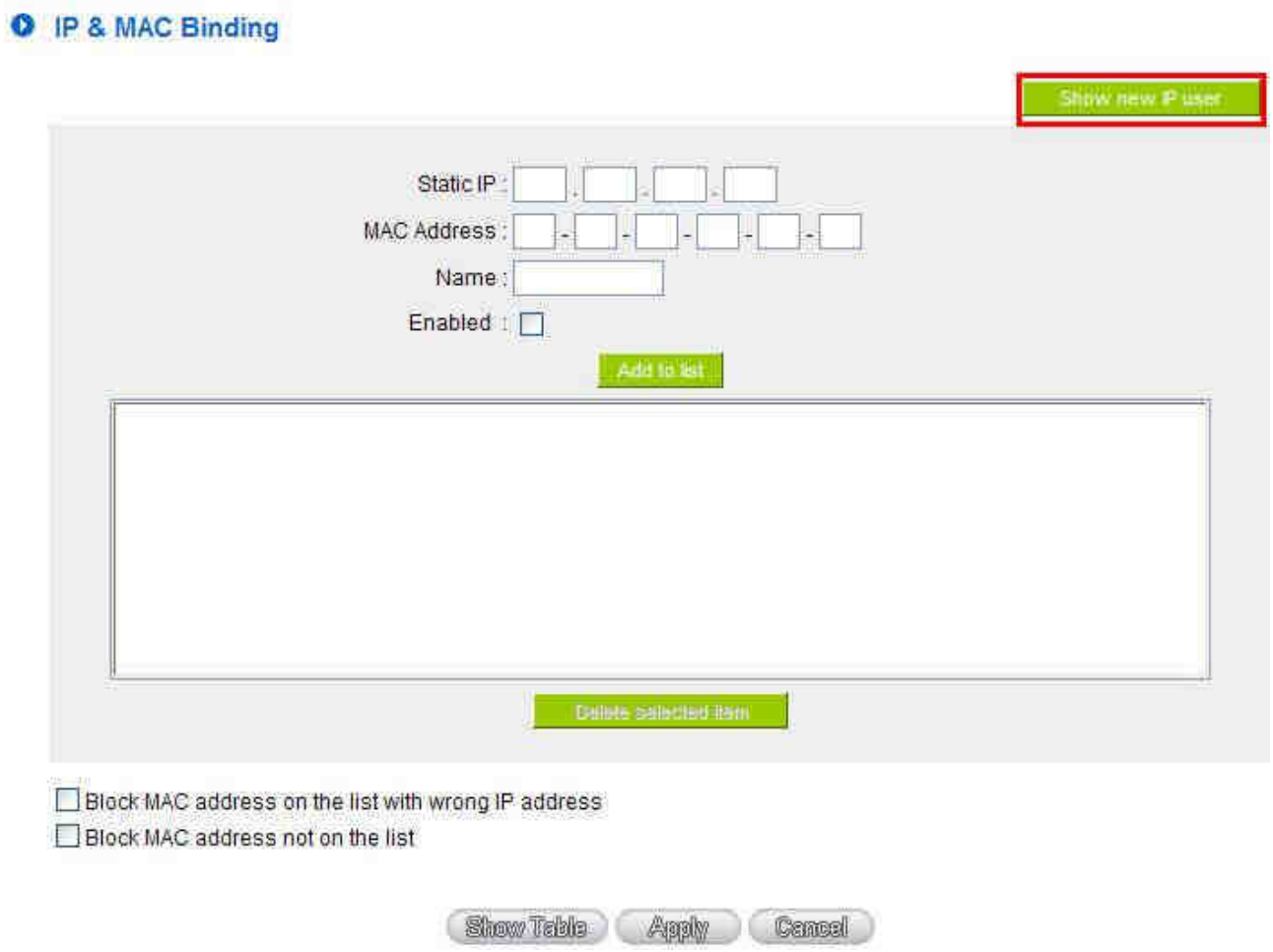
Enter "Setup" under DHCP page. On the down right corner of the screen, there is "IP

and MAC Binding," where users may create IP and MAC binding. On "Enabled," click on "√" and select "Add to List." Repeat these steps to add other IP and MAC binding, followed by clicking "Apply" at the bottom of the page.

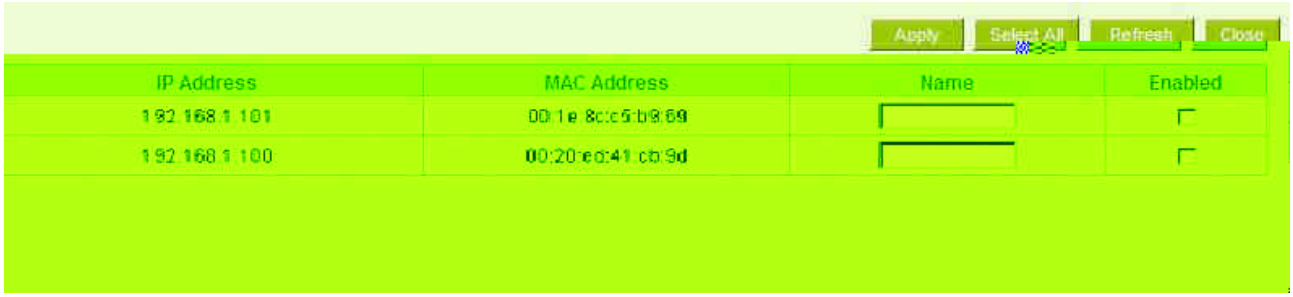


After an item is added to the list, the corresponding message will be displayed in the white block on the bottom. However, such method is not recommended because the inquiry of IP/MAC addresses of all hosts creates heavy workload. Another method to bind IP and MAC is more recommended because of easy operation, reduced workload and time efficiency. It is described in the following.

Enter "Setup" under the DHCP page and look for IP and MAC binding. On the right, there is an option of "Show new IP user" and click to enter.

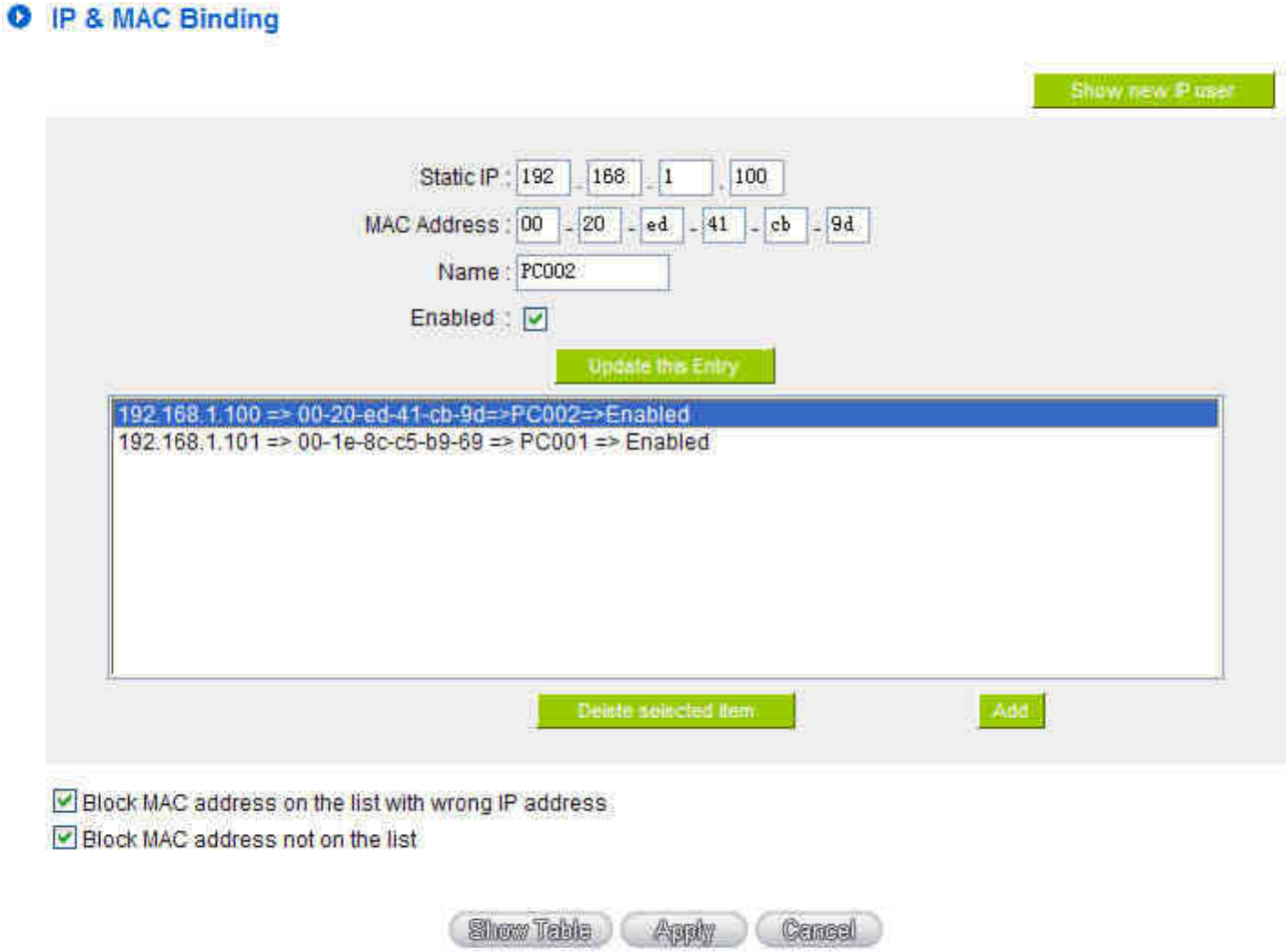


Click to display IP and MAC binding list dialog box. In this box, the unbinding IP and MAC address corresponding to the PC are displayed. Enter the "Name" of the computer and click on "**Enabled**" with the display of the **"√"** icon and push the option on the top right corner of the screen to confirm.



Now the bound options will display on the IP and MAC binding list (as illustrated in

Figure 5) and click "Apply" to finish binding.



Though these basic operations can help solve the problem but Qno's technical engineers suggest that further measures should be taken to prevent the ARP attack.

1. Deal with virus source as well as the source device affected by virus through virus killing and the system re-installation. This operation is more important because it solves the source PC which is attacked by ARP. This can better shelter the network from being attacked.

2. Cyber café administrators should check the LAN virus, install anti-virus software (Ginshan Virus/Reixin must update the virus codes) and conduct virus scanning for the device.

3. Install the patch program for the system. Through Windows Update, the system

patch program (critical update, security update and Service Pack)

4. Provide system administrators with a sophisticated and strong password for different accounts. It would be best if the password consists of a combination of more than 12 letters, digits, and symbols; Forbid and delete some redundant accounts.

5. Frequently update anti-virus software (virus data base), and set the daily upgrade that allows regular and automatic update. Install and use the network firewall software. Network firewall is important for the process of anti-virus. It can effectively avert the attack from the network and invasion of the virus. Some users of the pirate version of Windows cannot install patches successfully. Users are advised to use network firewall and other measures for protection.

6. Close some unnecessary services and some unnecessary sharing (if the condition is applicable), which includes such management sharing as C$ and D$. Single device user can directly close Server service.

7. Do not open QQ or the link messages sent by MSN online chatting tools in a causal manner. Do not open or execute any strange, suspicious documents and procedures such as the unknown attachment enclosed in E-mail and plug-in.

4). Summary

ARP attack prevention is a serious and long-term undertaking. The above methods can basically resolve the network problems caused by ARP virus attack. Moreover, clients who adopted similar methods witness good results. However, it is important that network administrators pay special attention to this problem rather than overlooking the issue. It is suggested that the above measures can be adopted to prevent ARP attack, reduce the damage, enhance the work efficiency and minimize economic loss.

Appendix 2：Qno Technical Support Information

For more information about the Qno's product and technology, please log onto the Qno's bandwidth forum, refer to the examples of the FTP server, or contact the technical department of Qno's dealers as well as the Qno's technical center.

Qno Official Web Site：http：//www.Qno.com.tw

Dealer Contact:

Users may log on to the service webpage to check the contacts of dealers:

http：//www.qno.com.tw/web/where_buy.asp

Taiwan Technical Center:

E-mail：QnoFAE@qno.com.tw