Powered by OvisLink Corp.

IGR-2500

Five-WAN Internet Gateway

User's Manual

www.airlive.com

Declaration of Conformity

We, Manufacturer/Importer

OvisLink Corp.
5F., NO.6, Lane 130, Min-Chuan Rd.,
Hsin-Tien City, Taipei County, Taiwan

Declare that the product

Five-WAN Internet Gateway

IGR-2500

is in conformity with

In accordance with 89/336 EEC-EMC Directive and 1999/5 EC-R & TTE Directive

Clause	**Description**
■ **EN 55022:1998/A1 :2000/A2:2003**	Limits and methods of measurement of radio disturbance characteristics of information technology equipment
■ **EN 61000-3-2:2000**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Harmonics"
■ **EN 61000-3-3:1995/ A1:2001**	Disturbances in supply systems caused by household appliances and similar electrical equipment "Voltage fluctuations"
■ **EN 55024:1998/A1 :2001/A2:2003**	Information Technology equipment-Immunity characteristics-Limits And methods of measurement
■ **CE marking**	CE

Manufacturer/Importer

Signature： albert Ye
Name　　: **Albert Yeh**
Position/ Title : **Vice President**

Date： **2007/8/23**

(Stamp)

AirLive IGR-2500 CE Declaration Statement

Country	Declaration	Country	Declaration
cs Česky [Czech]	OvisLink Corp. tímto prohlašuje, že tento AirLive IGR-2500 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.	**lt** Lietuvių [Lithuanian]	Šiuo OvisLink Corp. deklaruoja, kad šis AirLive IGR-2500 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
da Dansk [Danish]	Undertegnede OvisLink Corp. erklærer herved, at følgende udstyr AirLive IGR-2500 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.	**nl** Nederlands [Dutch	Hierbij verklaart OvisLink Corp. dat het toestel AirLive IGR-2500 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
de Deutsch [German]	Hiermit erklärt OvisLink Corp., dass sich das Gerät AirLive IGR-2500 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.	**mt** Malti [Maltese]	Hawnhekk, OvisLink Corp, jiddikjara li dan AirLive IGR-2500 jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
et Eesti [Estonian]	Käesolevaga kinnitab OvisLink Corp. seadme AirLive IGR-2500 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.	**hu** Magyar [Hungarian]	Az OvisLink Corporation kijelenti, hogy az AirLive IGR-2500 megfelel az 1999/05/CE irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek.
en English	Hereby, OvisLink Corp., declares that this AirLive IGR-2500 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**pl** Polski [Polish]	Niniejszym OvisLink Corp oświadcza, że AirLive IGR-2500 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
es Español [Spanish]	Por medio de la presente OvisLink Corp. declara que el AirLive IGR-2500 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.	**pt** Português [Portuguese]	OvisLink Corp declara que este AirLive IGR-2500 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ OvisLink Corp. ΔΗΛΩΝΕΙ ΟΤΙ AirLive IGR-2500 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.	**sl** Slovensko [Slovenian]	OvisLink Corp izjavlja, da je ta AirLive IGR-2500 v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
fr Français [French]	Par la présente OvisLink Corp. déclare que l'appareil AirLive IGR-2500 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**sk** Slovensky [Slovak]	OvisLink Corp týmto vyhlasuje, že AirLive IGR-2500 spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
it Italiano [Italian]	Con la presente OvisLink Corp. dichiara che questo AirLive IGR-2500 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**fi** Suomi [Finnish]	OvisLink Corp vakuuttaa täten että AirLive IGR-2500 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen
lv Latviski [Latvian]	Ar šo OvisLink Corp. deklarē, ka AirLive IGR-2500 atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.	Íslenska [Icelandic]	Hér með lýsir OvisLink Corp yfir því að AirLive IGR-2500 er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
sv Svenska [Swedish]	Härmed intygar OvisLink Corp. att denna AirLive IGR-2500 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.	**no** Norsk [Norwegian]	OvisLink Corp erklærer herved at utstyret AirLive IGR-2500 er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

A copy of the full CE report can be obtained from the following address:

OvisLink Corp.
5F, No.6 Lane 130,
Min-Chuan Rd, Hsin-Tien City,
Taipei, Taiwan, R.O.C.

This equipment may be used in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, SK, SI, ES, SE, GB, IS, LI, NO, CH, BG, RO, TR

Copyright

Trademarks

FCC Interference Statement

The **IGR-2500** has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility,
EN 55022/A1/A2, EN 61000-3-2, EN 61000-3-3/A1, EN 55024/A1/A2, Class B.

The specification is subject to change without notice.

Table of Contents

Chapter 1 Introduction

Congratulations on your purchase of this outstanding IGR-2500 Five-WAN Internet Gateway, this product is specifically designed for the office that has the need to enlarge the usage bandwidth with several narrow bandwidth connections in company.

IGR-2500 features with four 10/100 Mbps Ethernet ports (WAN port), eight 10/100 Mbps Ethernet ports (LAN port), and one 10/100 Mbps Ethernet port for DMZ. WAN port is using to connect to broadband transmission equipments such as ADSL modem or CABLE modem for user and far end to download or upload data in high speed; the LAN port works to connect to computer via cable. You can also connect LAN port with HUB/SWITCH device to extend the amount of connection device/user if necessary. Families with multiple PCs could share one ISP account and play exciting games against each other through IGR-2500. The switch function could also reduce the traffic in internal LAN. DMZ is provided to specific service device to allow the access. User can also change DMZ port as 5th WAN interface from WebUI setting.

1.1 Functions and Features

- **Web configuration tool**
- **Multiple DMZ Host (PPPoE, Static IP)**
- **Multiple Virtual Server**
- **Multiple NAT function**
- **Inbound Load Balance and Outbound Load Balance**
- **Ultra Smart Sharing**
- **Protocol Route Control (IP Binding Function, by IP & port number)**
- **Protocol Bandwidth Control (by application protocol port number)**
- **IP/URL Blocking, DoS, and Intrusion Security**
- **IM Blocking**
- **ARP Protection**
- **User Bandwidth Control Function (by user IP address)**
- **H.323 VoIP ALG included**
- **Remote Configuration Through Internet**
- **System Log**
- **Mail Alert**
- **SPI Firewall**
- **Backup / Restore Router configuration file from PC**
- **Display real time router configuration parameter**

1.2 Front Panel and Rear Panel

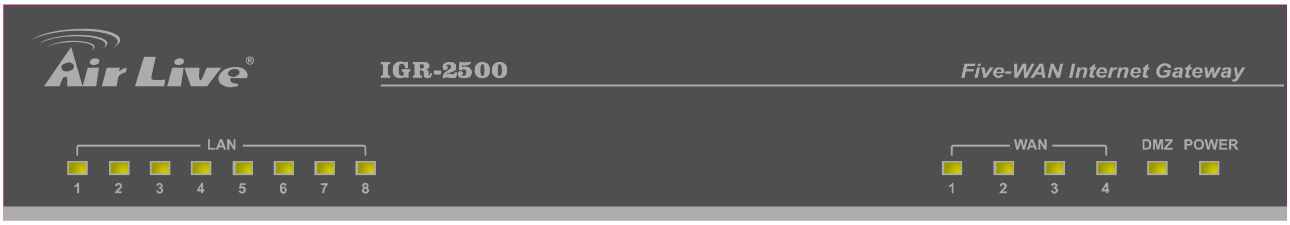


Figure 1-1 Front Panel

LED		Status	
Indicator	**Color**	**ON**	**Flashing**
Power	● Green	Initialize	Active Stage
WAN 1~4	● Red	Linked	Data Transmission
LAN 1~8	● Green	Linked	Data Transmission
DMZ	● Red	Linked	-

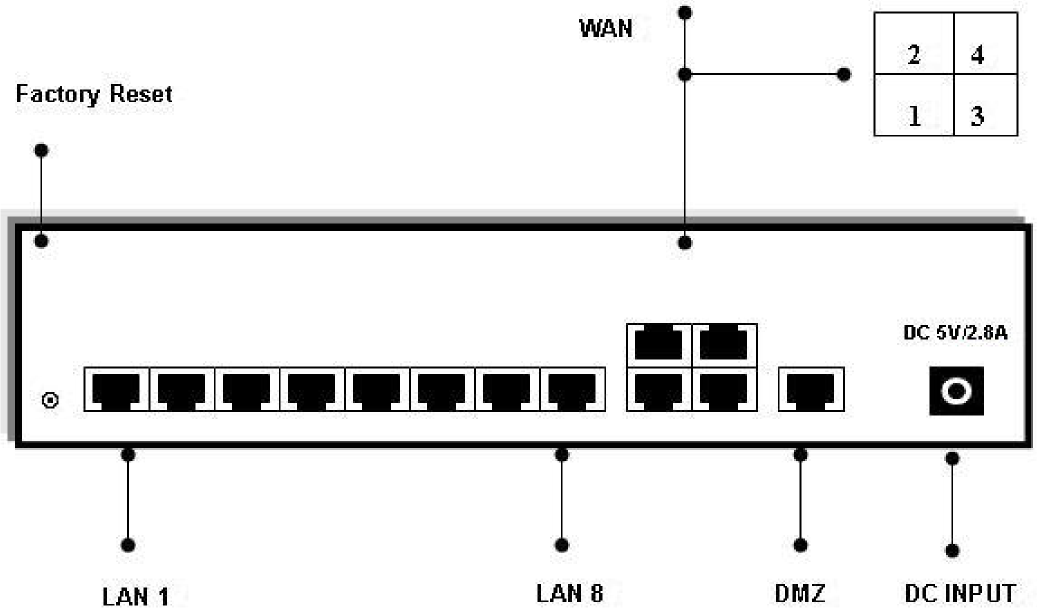


Figure 1-2 Rear Panel

Ports:

DC 5V: Connecting to AC adapter
WAN1~4 Port: Four RJ-45 type WAN ports connecting to broadband transmission equipment such as ADSL or Cable modem via RJ-45 cable.
LAN 1~8 Port: Eight RJ-45 type LAN port connecting to your network devices such as Hub/Switch via RJ-45 cable.
DMZ Port: One RJ-45 type DMZ port connecting to your network devices. It can also be configured as the 5th WAN port via software.
Factory Reset: Press **Factory Reset** button can be defined as to reload factory default value or reset back to latest configuration by software. When you finish defining the Default Button Option, just pressing Factory Reset button 2 seconds and releasing it, the router will load the default settings or back to latest configuration.

1.3 Packing List

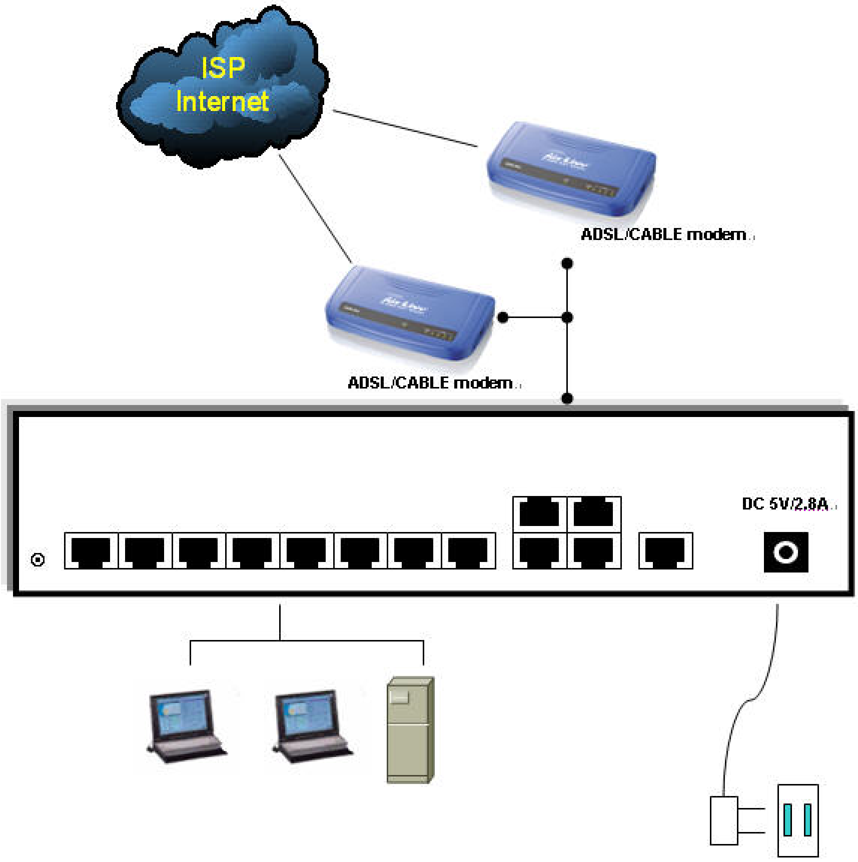
- IGR-2500 Five-WAN Internet Gateway
- Installation CD-ROM
- Quick Installation Guide
- CAT-5 UTP Fast Ethernet cable
- AC Adapter

When you open your package, make sure all of the above items are included and not damaged. If you see that any components are damaged, please notify your dealer immediately.

Chapter 2 Deployment

IGR-2500 provides one LAN port connecting to your network devices such as PC, HUB and SWITCH via RJ45 cable. Using a HUB/SWITCH will allow more PC connecting to IGR-2500. WAN ports are using to connect your ADSL or CABLE Modem to the broadband ISP.

For RJ45 cable type, both WAN/LAN port support auto MDI/MDIX Function, you can choose cross over type or straight type RJ-45 cable



Connection Procedure:

1. Plug in DC power adapter to Router.
2. Connect the Router WAN port RJ45 modular jack to ADSL/CABLE Modem Ethernet port with the RJ45 cable.
3. Connect the Router LAN port RJ45 modular jack to HUB/SWITCH LAN port by RJ45 cable.
4. Connect PC LAN card port to HUB/SWITCH LAN port.
5. Plug in AC power cord to power source

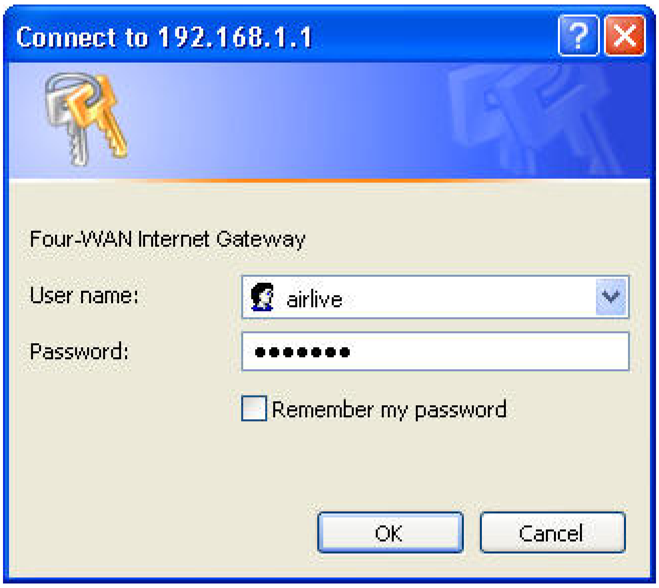
Chapter 3 Configure Router

3.1 How to start out to configure router

Step1. Connect the MIS engineer's PC and IGR-2500's LAN port to the same Hub / Switch, and launch the browser (IE or Netscape) to link the IGR-2500 appliance. The default IP address is http: //192.168.1.1

Step2. Administrator will be requested for **User Name** and **Password** when entering IGR-2500 system. (Figure 3-1)

- **User Name** : airlive
- **Password** : airlive
- Click **OK**.



Connect to 192.168.1.1

Four-WAN Internet Gateway

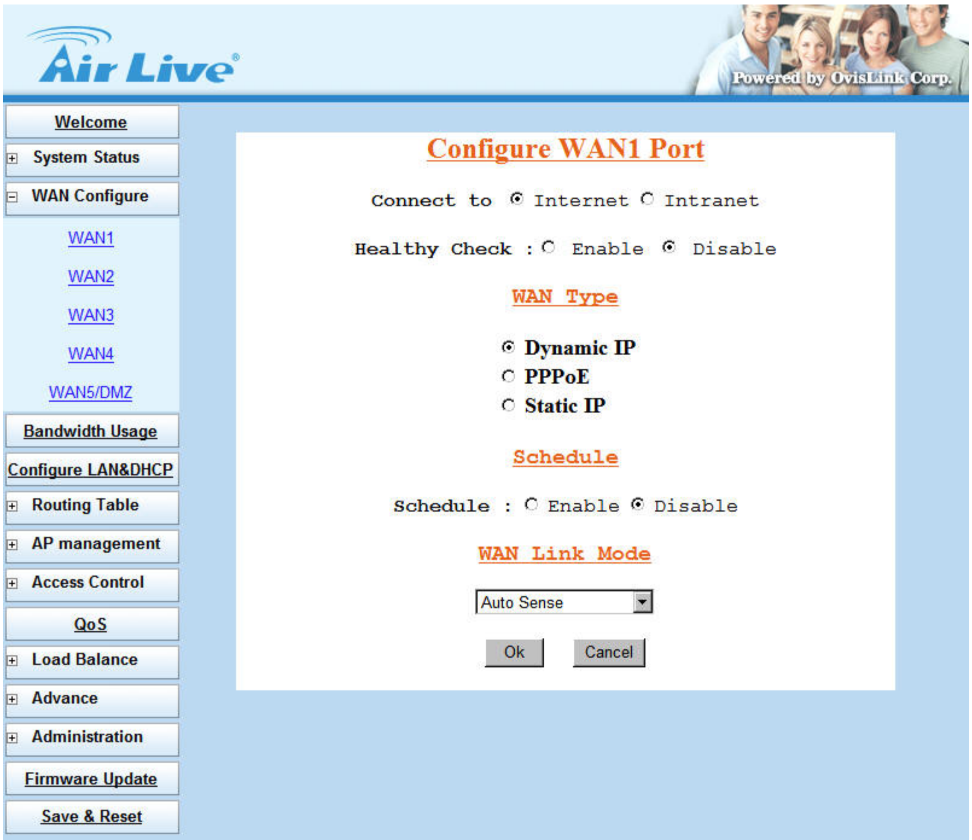
User name: airlive

Password: ●●●●●●●●

□ Remember my password

Figure 3-1 Login page

Step3. Configure each WAN port separately, and the other function you would like to use, such as Load Balance, Bandwidth Management, or else. (Figure 3-2)



Configure WAN1 Port

Connect to ● Internet ○ Intranet

Healthy Check : ○ Enable ● Disable

WAN Type

● Dynamic IP
○ PPPoE
○ Static IP

Schedule

Schedule : ○ Enable ● Disable

WAN Link Mode

Auto Sense ▾

Ok Cancel

Figure 3-2 Configure WAN port setting

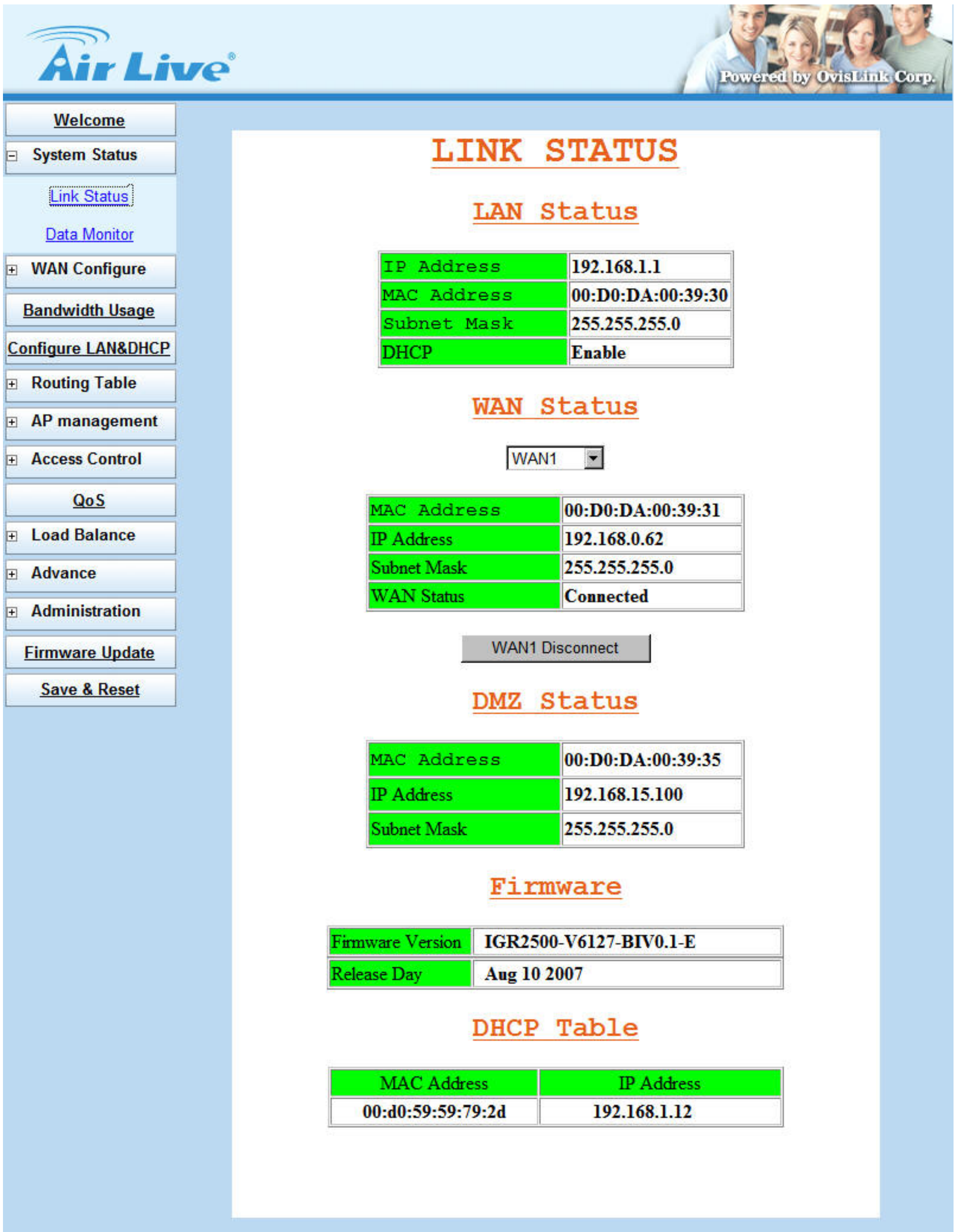
You can refer to the manual for more understanding of else router’s feature.

3.2 System Status

3.2.1 Link Status

You can get the following information in Link Status window: (Figure 3-3)

- **LAN Status**
- **WAN Status**
- **DMZ Status**
- **Firmware Version**
- **DHCP Table**



LINK STATUS

LAN Status

IP Address	192.168.1.1
MAC Address	00:D0:DA:00:39:30
Subnet Mask	255.255.255.0
DHCP	Enable

WAN Status

WAN1

MAC Address	00:D0:DA:00:39:31
IP Address	192.168.0.62
Subnet Mask	255.255.255.0
WAN Status	Connected

DMZ Status

MAC Address	00:D0:DA:00:39:35
IP Address	192.168.15.100
Subnet Mask	255.255.255.0

Firmware

Firmware Version	IGR2500-V6127-BIV0.1-E
Release Day	Aug 10 2007

DHCP Table

MAC Address	IP Address
00:d0:59:59:79:2d	192.168.1.12

Figure 3-3 Link Status

LAN Status: Shows the information of **MAC Address**, **IP Address**, **Subnet Mask** and **DHCP Status** (Enable/Disable).

WAN Status: Shows the information of **MAC Address**, **IP Address**, **Subnet Mask** and **WAN Status** on each or all **WAN** ports.

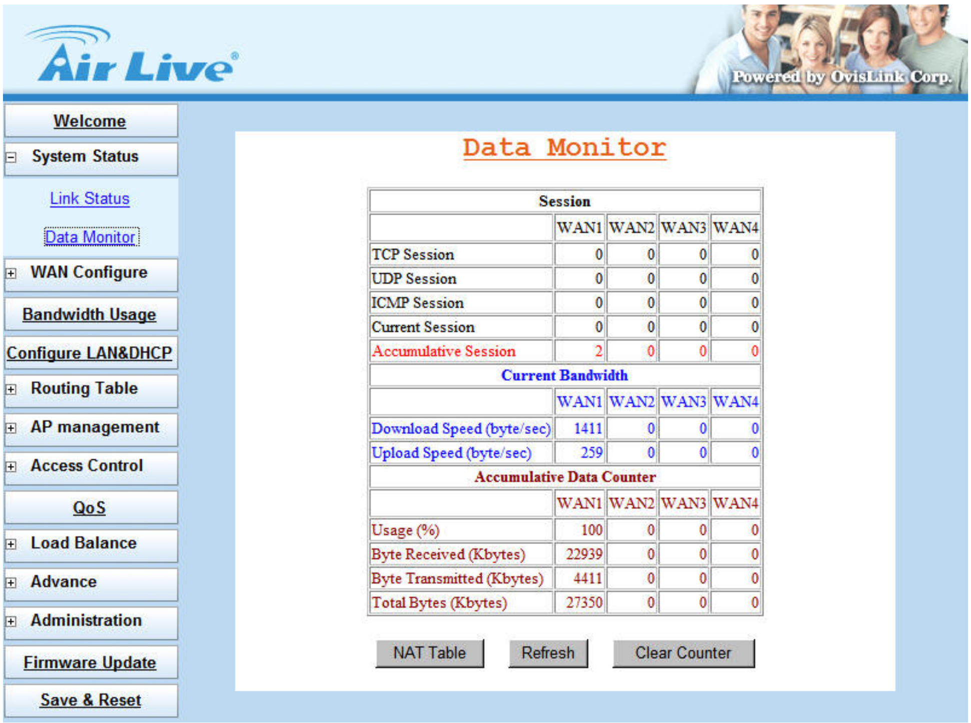
DMZ Status: Shows the information of **MAC Address**, **IP Address**, and **Subnet Mask.**

Firmware version: version of software and its released date.

DHCP Table: Shows the information of **MAC Address** and **IP Address**.

3.2.2 Data Monitor

Differ with Link Status window, Data Monitor window provides detail packet transfer status. It includes 2 kinds of real time data per each WAN port. (Figure 3-4)



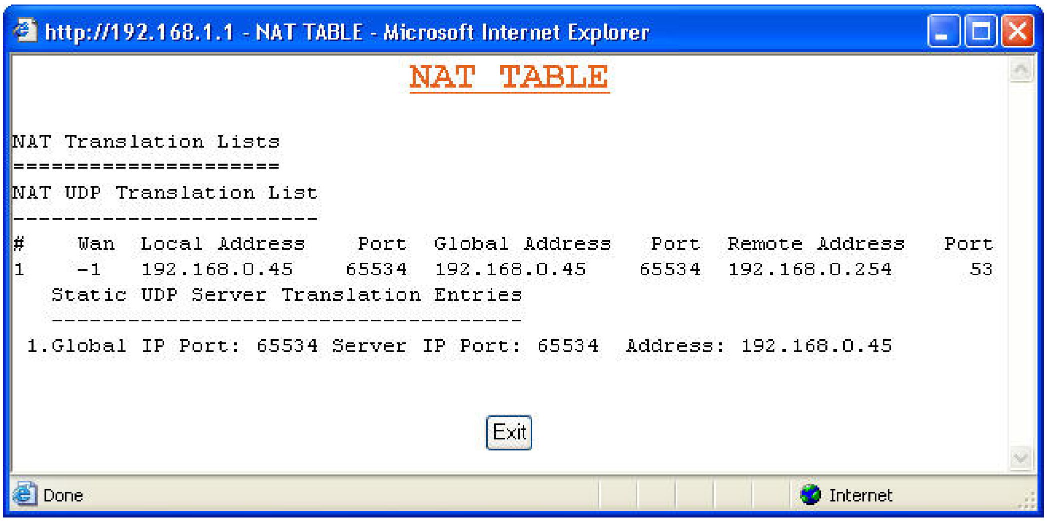
Data Monitor

Session				
	WAN1	WAN2	WAN3	WAN4
TCP Session	0	0	0	0
UDP Session	0	0	0	0
ICMP Session	0	0	0	0
Current Session	0	0	0	0
Accumulative Session	2	0	0	0
Current Bandwidth				
	WAN1	WAN2	WAN3	WAN4
Download Speed (byte/sec)	1411	0	0	0
Upload Speed (byte/sec)	259	0	0	0
Accumulative Data Counter				
	WAN1	WAN2	WAN3	WAN4
Usage (%)	100	0	0	0
Byte Received (Kbytes)	22939	0	0	0
Byte Transmitted (Kbytes)	4411	0	0	0
Total Bytes (Kbytes)	27350	0	0	0

Figure 3-4 Data Monitor

- **Current Session:**
  - TCP Session:
  - UDP Session:
  - ICMP Session:
  - Total Session:
- **Current Bandwidth:**
  - Download Speed:
  - Upload Speed
- **Accumulative Data Counter:**
  - Usage (%): For example, WAN1 usage% = $\frac{\text{WAN1 total packets}}{\text{(WAN1+WAN2) total packets}}$ %
  - Byte Received
  - Byte Transmitted
  - Total Bytes: Total packets transfer by each WAN port

- **NAT Table:** list current user detail NAT data. (Figure 3-5)
- **Refresh:** update data monitor table to display newest data
- **Clear Counter:** reset **Data Counter** data to 0, and restart to accumulate the packets.



http://192.168.1.1 - NAT TABLE - Microsoft Internet Explorer
Exit
Done
Internet

NAT TABLE

```
NAT Translation Lists
=====================
NAT UDP Translation List
------------------------
#    Wan  Local Address    Port  Global Address   Port  Remote Address    Port
1    -1   192.168.0.45     65534 192.168.0.45     65534 192.168.0.254       53
   Static UDP Server Translation Entries
   -------------------------------------
 1.Global IP Port: 65534 Server IP Port: 65534  Address: 192.168.0.45
```

Figure 3-5 NAT Table

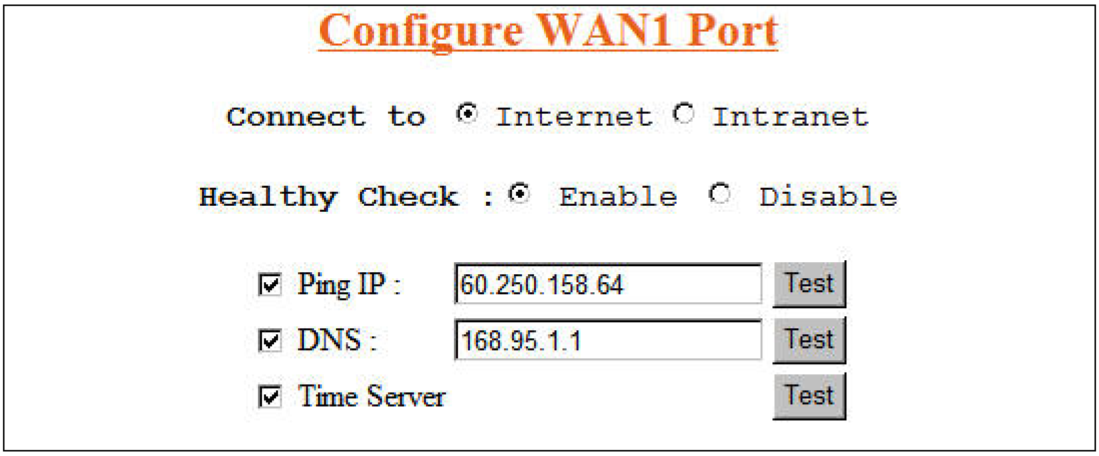
The packets start to accumulate from:

1. Router powers on
2. Clear counter
3. Counter reaches upper the limitation (4294967K), and then the counter will reset to 0 automatically.

3.3 WAN Configure

There are several **WAN** function can be made in this display, you can configure functions to each WAN port separately.

- **Connect to:**
  - **Internet:** WAN port is connected to Internet through ADSL/Cable modem
  - **Intranet:** WAN port is connected to another router LAN port, work together with "Static Route" function, can restrict specific IP packet to a dedicate route path.
- **Healthy Check:**
  - **Enable:** Enable the feature to check whether the WAN link is alive or not. System provides 3 methods to check the WAN link, **Ping IP**, **DNS**, and **Time Server**; you can choose it with each method or both. It is suggested to select at least 2 methods to check the WAN link, in order to avoid router making wrong action due to Internet Server disable. (Figure 3-6)
  - **Disable:** If "Time Server" does not exist, this function will disable automatically.



Configure WAN1 Port

Connect to ● Internet ○ Intranet

Healthy Check : ● Enable ○ Disable

☑ Ping IP : 60.250.158.64

☑ DNS : 168.95.1.1

☑ Time Server

Figure 3-6 Healthy Check

- **Dynamic IP:** Connect to Cable Modem and obtain an IP address from ISP automatically.
- **PPPoE:** Connect to Dial Up DSL
- **Static IP:** Connect to Leased DSL
- **Schedule:** This function allows you to control each WAN port link up/down time by daily/weekly.
  - **Start Time: (hh:mm)**
  - **End Time: (hh:mm)**
  - **Weekly:** choose by day

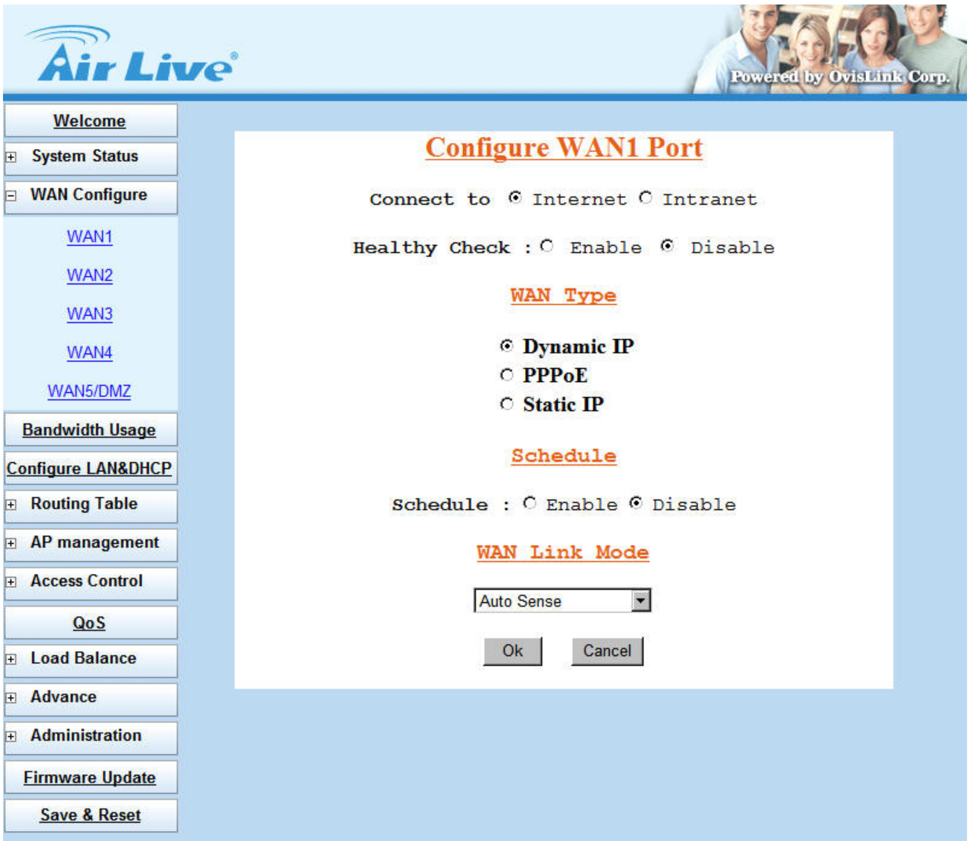
When you enable Schedule function, the WAN connection will follow the Schedule to link up or down, no matter DOD (Dial-on-demand) function is enabled or disabled.

- **WAN Link Mode:** You can choose the WAN interface type in order to follow the connecting type of ISP.
    - **Auto Sense**
    - **10Mbps Half Duplex**
    - **10Mbps Full Duplex**
    - **100Mbps Half Duplex**
    - **100Mbps Full Duplex**

3.3.1 WAN Type – Dynamic IP

Usually it's used to connect CABLE modem. You won't need to assign IP address, and the IGR-2500 will get the IP address from ISP automatically. (Figure 3-7)

When you choose Dynamic IP, you only need to save this selection, and reboot router when you finish configuring all parameter.



Configure WAN1 Port

Connect to ● Internet ○ Intranet

Healthy Check : ○ Enable ● Disable

WAN Type

● Dynamic IP
○ PPPoE
○ Static IP

Schedule

Schedule : ○ Enable ● Disable

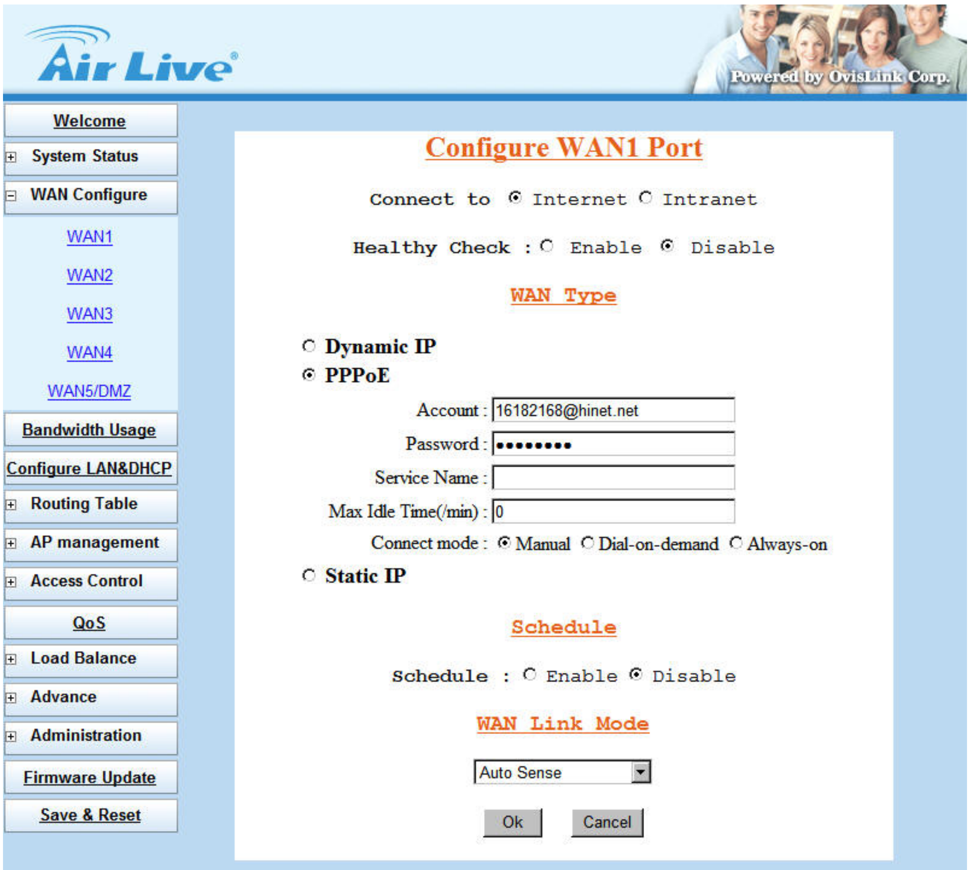
WAN Link Mode

Auto Sense

Figure 3-7 Dynamic IP

3.3.2 WAN Type – PPPoE

Connect to ISP via dial-up connecting, ISP will assign a legal IP to you after the user Id and password had been passed. (The user Id and password here are provided by your ISP.) (Figure 3-8)



Configure WAN1 Port

Connect to ● Internet ○ Intranet

Healthy Check : ○ Enable ● Disable

WAN Type

○ Dynamic IP

● PPPoE

Account : 16182168@hinet.net

Password : ••••••••

Service Name :

Max Idle Time(/min) : 0

Connect mode : ● Manual ○ Dial-on-demand ○ Always-on

○ Static IP

Schedule

Schedule : ○ Enable ● Disable

WAN Link Mode

Auto Sense

Ok Cancel

Figure 3-8 PPPoE

- **Account:** The user name provided by ISP, the character can be entered up to 60.
- **Password:** The password provided by ISP, the character can be entered up to 60.
- **Service Name:** This is optional. The Service name is needed if ISP requires for it.
- **Max. Idle Time (min):** The default value is 0, means not to check the idle time, so the connection will remain connecting unless user disconnects it by manually.
- **Dial On Demand:** Auto connect function
  - **Manual:** You need to initiate WAN connection manually, by clicking **WAN1 connect** or **WAN2 connect** button in **System Status** → **Link Status** menu. However, power up or reset also can initiate the WAN connection.
  - **Dial-on-demand:** Whenever a user is trying to access the Internet from his computer, this WAN port will start connection automatically if it is disconnected.
  - **Always-on:** The WAN port will try to establish the connection as long as it is disconnected, no matter this port is used or not.

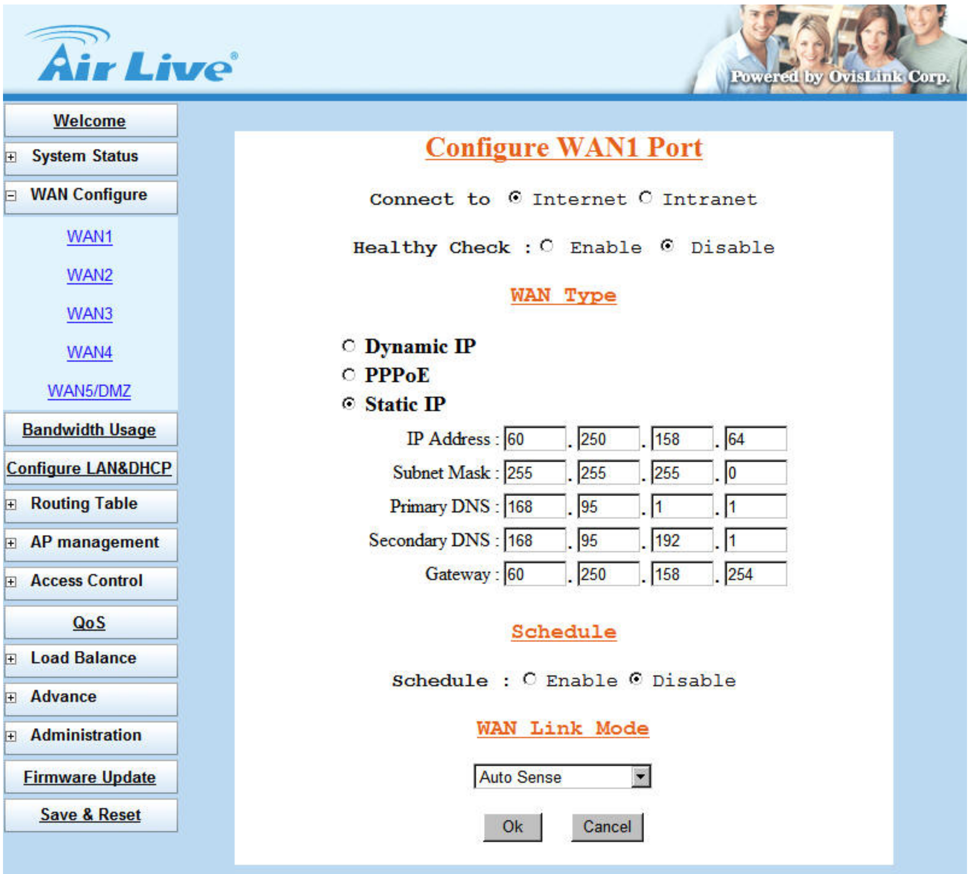
About “Always-on” function, normally you need to combine "Healthy Check" function together, then "Always-on" can work more perfectly because there is an ADSL modem between router & ISP equipment. In physical layer, if ADSL line fails but ADSL modem is still alive, and router can not detect the line status unless ISP sends a disconnected packet to router. So if ADSL line is in abnormal up-down, sometimes router can not get disconnect packet from ISP. Maybe in ISP side, it treats line as disconnected status, but router seems like to be still in "connecting" status.

If you enable "Healthy Check" in each line, then router can automatically send packet out through WAN to detect whether line is active or not. (1 packet per 30 sec) This function will be helpful to judge the line status, and provide correct information to router for the Link Status.

It's better to enable at least 2 options in "Healthy Check", in order to avoid misjudgments when only 1 option is selected and the option server fails to respond the request.

3.3.3 WAN Type – Static IP

When user applied the leased line from ISP, the service provider will offer user the real IP, Subnet Mask, Gateway and DNS. You need to indicate the static IP manually. (Figure 3-9)



Configure WAN1 Port

Connect to ● Internet ○ Intranet

Healthy Check : ○ Enable ● Disable

WAN Type

○ Dynamic IP
○ PPPoE
● Static IP

IP Address :	60	250	158	64
Subnet Mask :	255	255	255	0
Primary DNS :	168	95	1	1
Secondary DNS :	168	95	192	1
Gateway :	60	250	158	254

Schedule

Schedule : ○ Enable ● Disable

WAN Link Mode

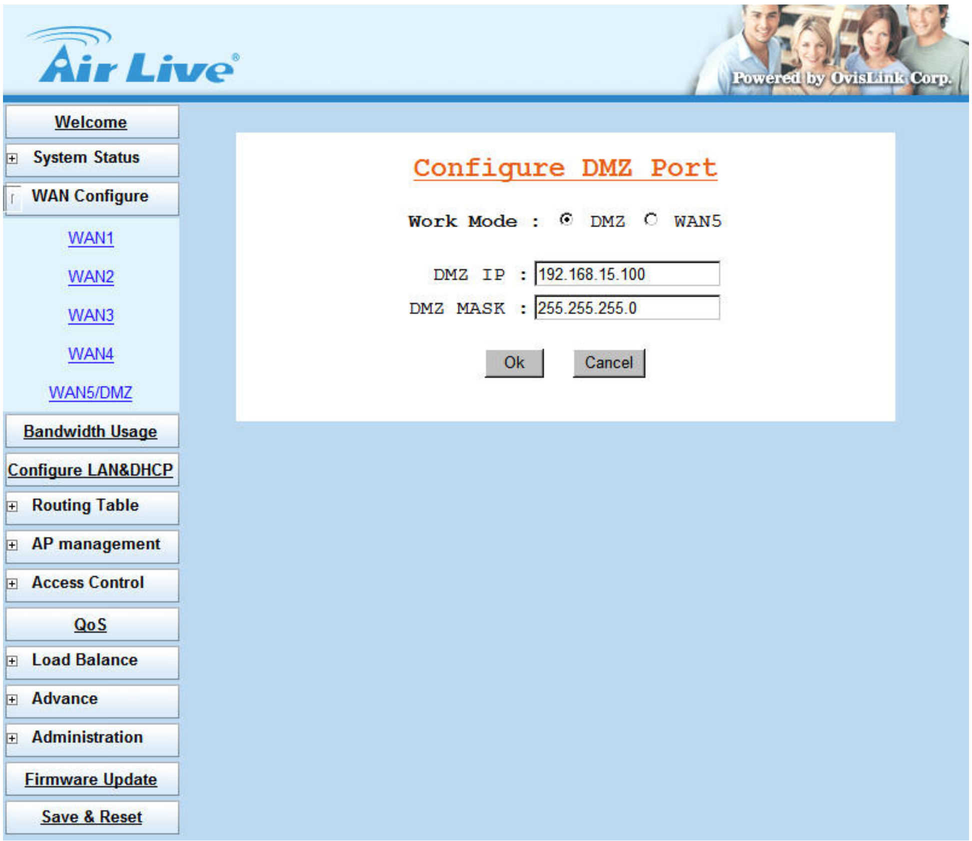
Auto Sense

Figure 3-9 Static IP

3.3.4 WAN Type – WAN5/DMZ

The hardware DMZ can be defined as DMZ function or 5th WAN port. If you select to define the interface as 5th WAN port, its setting is the same as else WAN interface.

When you select to define the interface as DMZ port, the default IP address of DMZ interface is 192.168.15.100. You can configure the DMZ setting with three different types, **Dynamic IP DMZ**, **Multi-DMZ**, and **Public DMZ**. For more detail information for the DMZ configuration please refers to the section 3.10.4 **DMZ Host**. (Figure 3-10)



Configure DMZ Port

Work Mode : ● DMZ ○ WAN5

DMZ IP : 192.168.15.100

DMZ MASK : 255.255.255.0

Ok Cancel

Figure 3-10 WAN5/DMZ

3.4 Bandwidth Usage

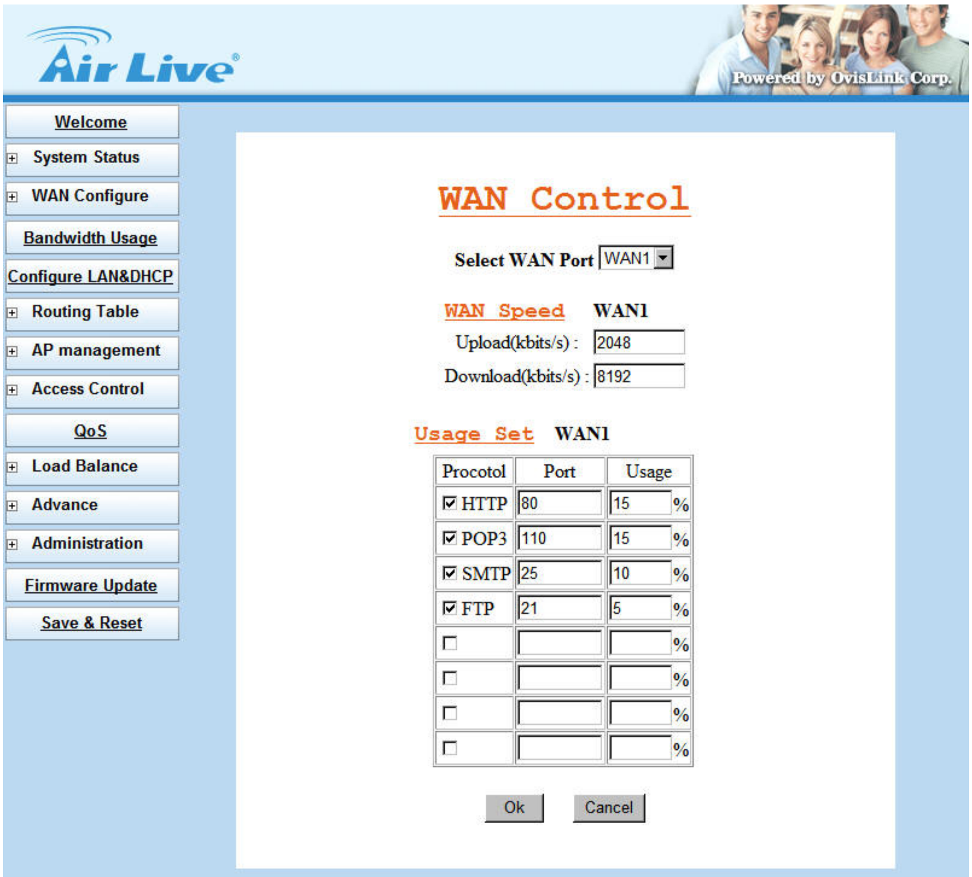
This is a very useful function, it can let you to control WAN port bandwidth usage by each protocol. Like FTP, when someone uses FTP to transfer file, it will occupy heavy loading by using this function, so you can limit the dedicated application bandwidth as you want to.

For example:

In following display, FTP, HTTP & Mail bandwidth will be limited in certain percentage. This router provides 3 most often use protocol in the table, and you just need to fill in port number and % usage for each application:

- **Select WAN Port:** Select the WAN interface for the bandwidth definition
- **WAN Speed:** Enter the upload and download speed provided by ISP
  - **Upload** (kbits/s)
  - **Download** (kbits/s)
- **Usage Set:**
  - **Protocol:** name of protocol data packet will be limited.
  - **Port:** protocol port number
  - **Usage %:** The usage percentage of WAN speed

    (Figure 3-11)



WAN Control

Select WAN Port WAN1

WAN Speed WAN1

Upload(kbits/s) : 2048

Download(kbits/s) : 8192

Usage Set WAN1

Procotol	Port	Usage
☑ HTTP	80	15 %
☑ POP3	110	15 %
☑ SMTP	25	10 %
☑ FTP	21	5 %
□		%
□		%
□		%
□		%

Figure 3-11 Bandwidth Usage

The totally amount of protocol usage percentage can not exceed 100% for each WAN port.

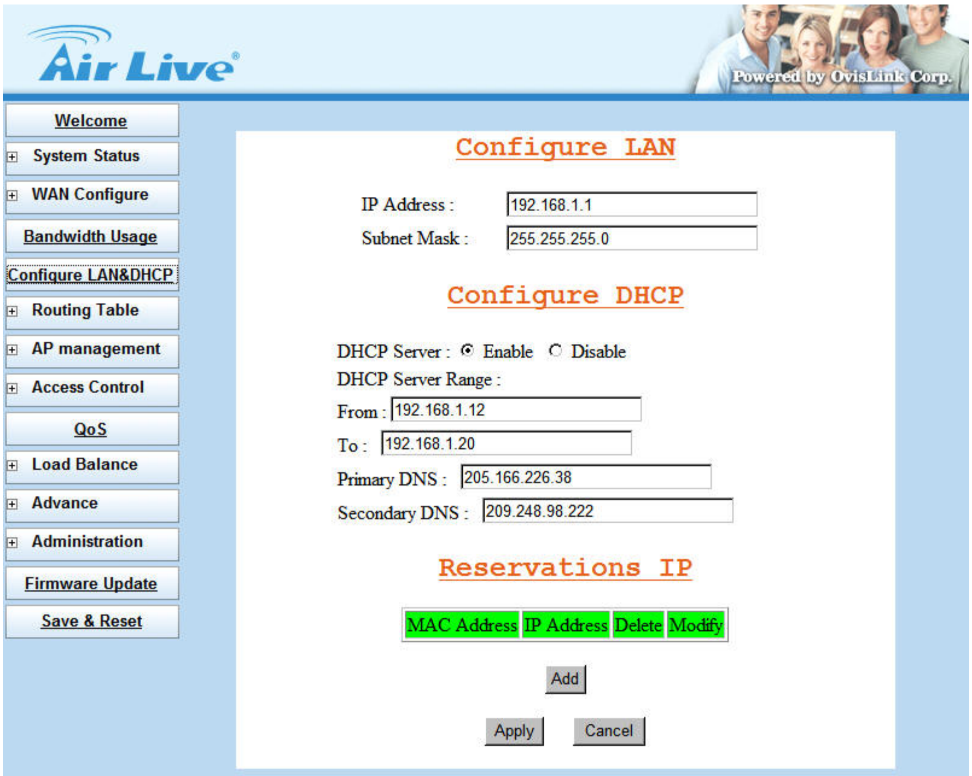
Router provides another 4 self-defined port number, user just needs to fill in port number for each protocol.

3.5 Configure LAN & DHCP

This function configures the LAN ports **IP address**, **Subnet Mask**, and **DHCP server**.

You can choose using DHCP server or disable it, the Dynamic Host Configuration Protocol (DHCP) allows the Broadband Router to dynamically assign IP addresses to network devices. Dynamic IP assignment alleviates the need for the network administrator to maintain and monitor IP address assignments and simplifies IP use because the IP addresses are automatically and dynamically assigned when a station powers-on. You will need to indicate the range of DHCP server and DNS address if you enable DHCP server function.
(Figure 3-12)

You can also reserve some IP's to specific computers. You need to enter the name (MAC address) of the network card installed in your computer to assign a particular IP to it. Enter the relative values and then click **Add**. (Figure 3-13)



Configure LAN

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0

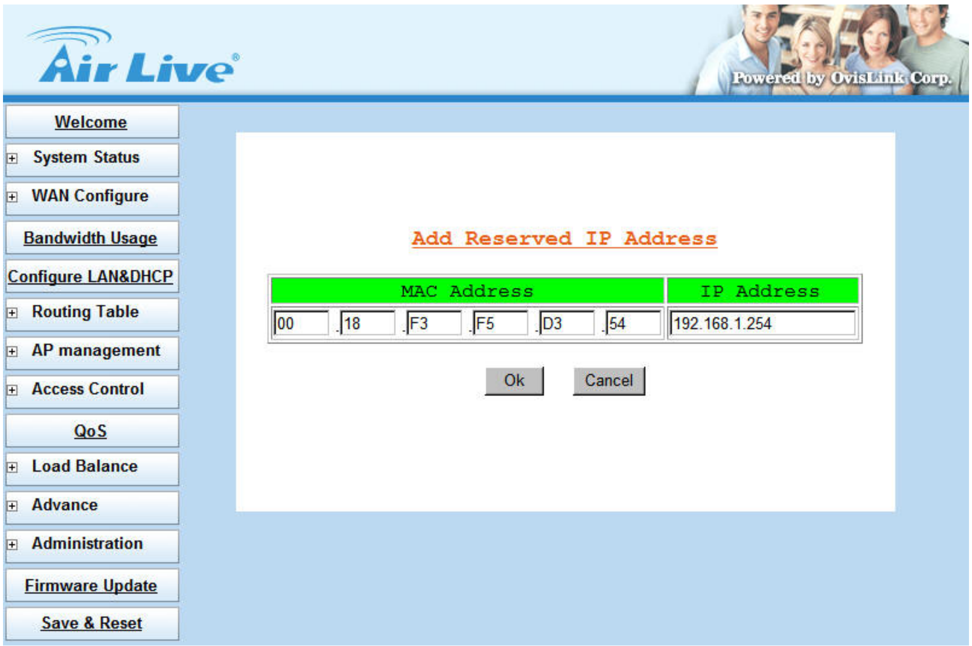
Configure DHCP

DHCP Server : ● Enable ○ Disable
DHCP Server Range :
From : 192.168.1.12
To : 192.168.1.20
Primary DNS : 205.166.226.38
Secondary DNS : 209.248.98.222

Reservations IP

MAC Address	IP Address	Delete	Modify

Figure 3-12 Configure LAN & DHCP



Add Reserved IP Address

MAC Address	IP Address
00 . 18 . F3 . F5 . D3 . 54	192.168.1.254

Figure 3-13 Add Reserved IP Address

When enable DHCP Server in “From”, ”TO” field, you can reserve up to **253** IP address to DHCP server.

Fill in local DNS Server IP address in “**DNS Address”** field, the DNS IP information will also assign to DHCP client.

3.6 Routing Table

3.6.1 Configure

This function allows manually defined by users as the only path to the destination. Users can configure the static routing path to IGR-2500.

- **Static Routing**

There have one pc with two interfaces in this area, one interface is connected to IGR-2500 (domain A), and the other connected to another Server (domain B). Users need to set the static routing path in IGR-2500 in order to recognize another domain in this area. These settings enable the packets from domain A to the destination in domain B via the gateway configured in IGR-2500. (Figure 3-14, 3-15)

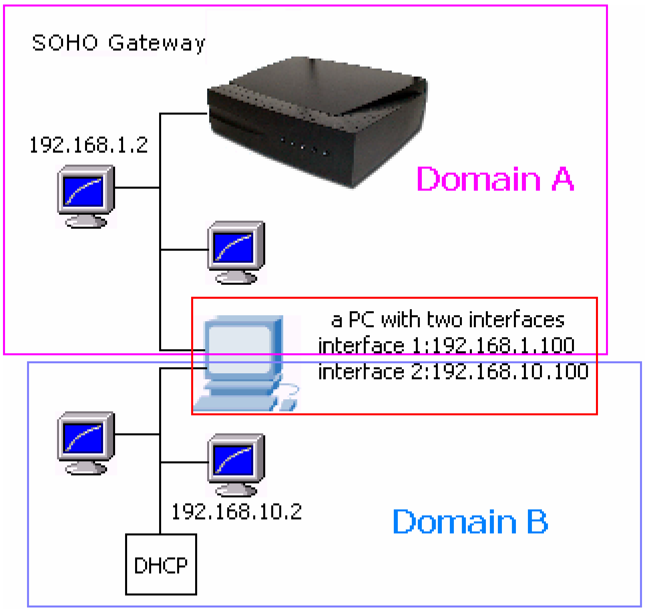
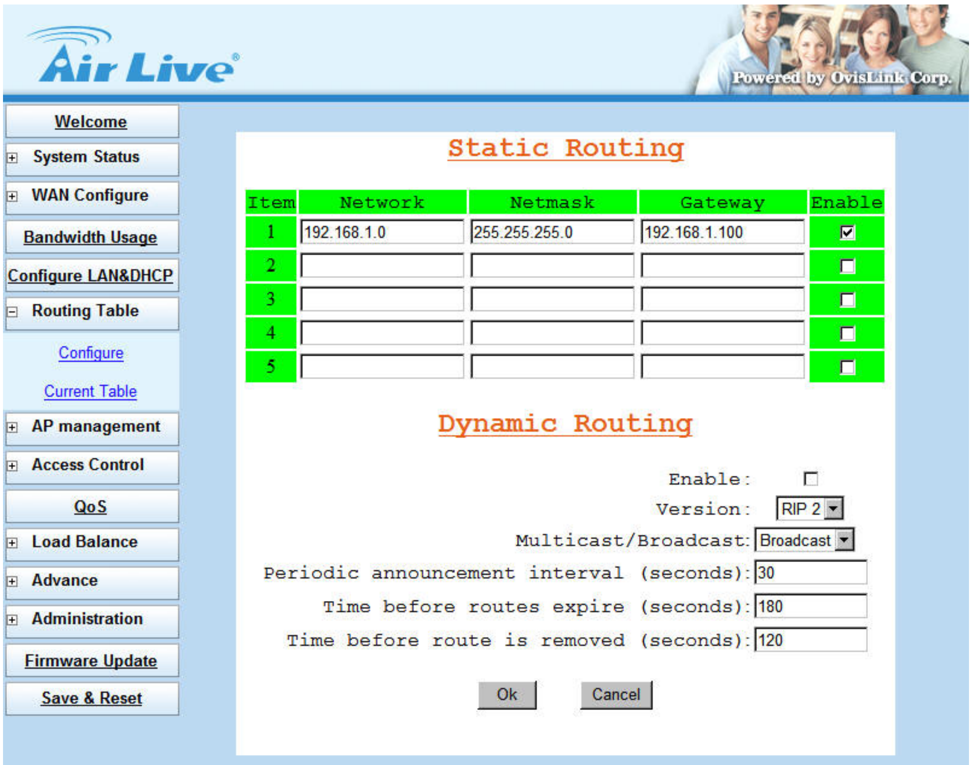


Figure 3-14 Static Routing



Static Routing

Item	Network	Netmask	Gateway	Enable
1	192.168.1.0	255.255.255.0	192.168.1.100	☑
2				□
3				□
4				□
5				□

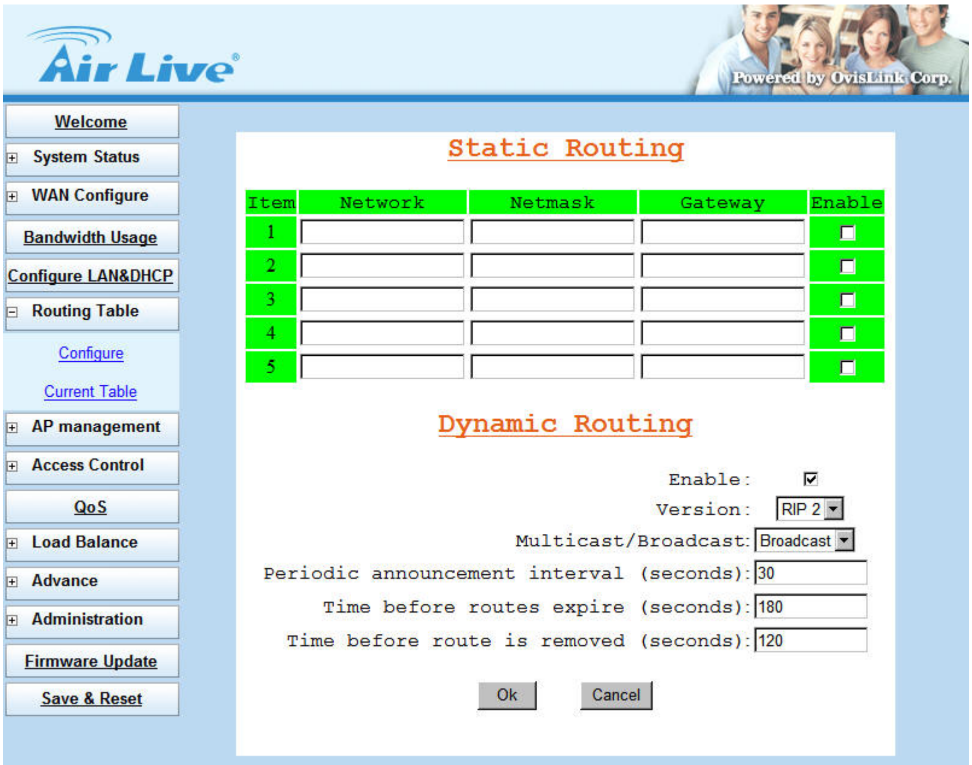
Dynamic Routing

Enable:	□
Version:	RIP 2
Multicast/Broadcast:	Broadcast
Periodic announcement interval (seconds):	30
Time before routes expire (seconds):	180
Time before route is removed (seconds):	120

Figure 3-15 Static Routing

■ Dynamic Routing

Dynamic Routing allows router learning the path to destination by receiving periodic updates from others. The protocol used in communication between routers is RIP v1 and v2. (Routing Information Protocol). RIP1 supports only to broadcast mode while RIP2 supports broadcast and multicast mode. (Figure 3-16)



Static Routing

Item	Network	Netmask	Gateway	Enable
1				□
2				□
3				□
4				□
5				□

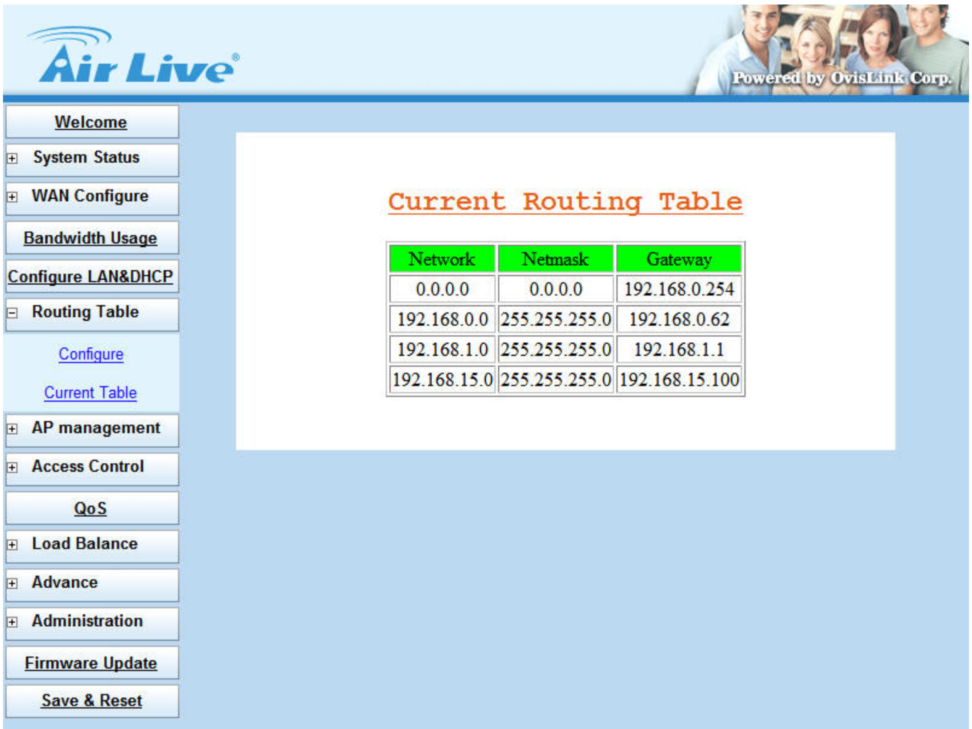
Dynamic Routing

Enable:	☑
Version:	RIP 2
Multicast/Broadcast:	Broadcast
Periodic announcement interval (seconds):	30
Time before routes expire (seconds):	180
Time before route is removed (seconds):	120

Figure 3-16 Dynamic Routing

3.6.2 Current Table

This display shows the valid routing paths in IGR-2500. Users can view the information about current routing paths. (Figure 3-17)



Current Routing Table

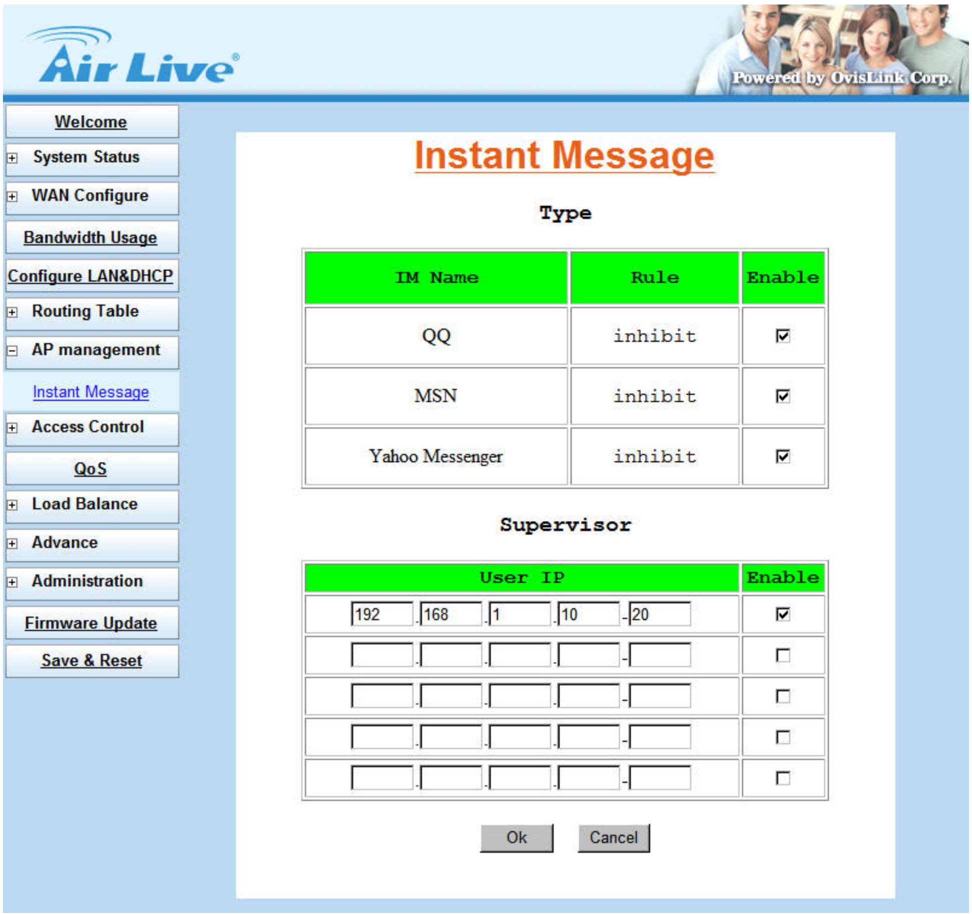
Network	Netmask	Gateway
0.0.0.0	0.0.0.0	192.168.0.254
192.168.0.0	255.255.255.0	192.168.0.62
192.168.1.0	255.255.255.0	192.168.1.1
192.168.15.0	255.255.255.0	192.168.15.100

Figure 3-17 Current Table

3.7 AP Management

AirLive IGR-2500 supports to block several Instant Message programs, such as QQ, MSN, and Yahoo Messenger. User can also define the supervisor IP address to be the privilege user who will not be restricted the access of IM program. (Figure 3-18)

- **Type:** Select to enable QQ, MSN, and Yahoo Messenger IM program inhibiting.
- **Supervisor:** Define the specific IP address or IP range that is able to access IM program.



Instant Message

Type

IM Name	Rule	Enable
QQ	inhibit	☑
MSN	inhibit	☑
Yahoo Messenger	inhibit	☑

Supervisor

User IP	Enable
192 . 168 . 1 . 10 - 20	☑
. . . -	☐
. . . -	☐
. . . -	☐
. . . -	☐

Figure 3-18 AP Management for IM

3.8 Access Control

3.8.1 Local IP Filtering

AirLive IGR-2500 allows you to define the accessed restriction about to block or allow outgoing IP packets per protocol (port number).

You may restrict specific IP to perform limited protocols or allow them to execute partial protocols. And the first thing you have to know is the port numbers and their usages.

Local IP Filtering can be defined 10 items and item 1 has the highest priority. In principle, the same IP should not list in different items. If IP settings are conflicted, the higher priority item will be the obeyed rules.

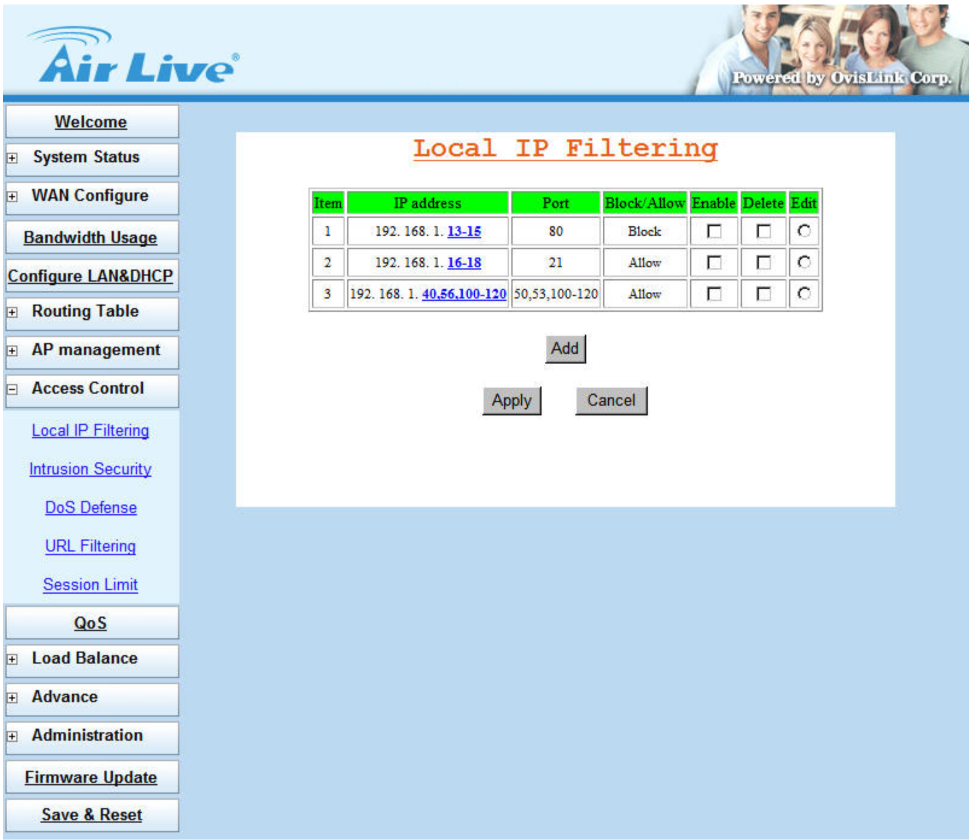
You can reserve dedicate IP address to dedicated user from **Configure LAN & DHCP → Reservations IP** function, by using this function, user can have dedicated IP address match to their computer NIC MAC address.

There are ten items in this function. You can allow or restrict specific IP(s) to access some port numbers.

Example 1:
If you restrict the PC of IP 192.168.1.13-192.168.1.15 to access HTTP, the settings are:
Item 1: Enable
Filter entry: Block
Port Number: 80
IP address: 192.168.1.13-192.168.1.15

Example 2:
If you allow the PC of IP 192.168.1.16-192.168.1.18 to access FTP only, the settings are:
Item 2: Enable
Filter entry: Allow
Port Number: 21
IP address: 192.168.1.16-192.168.1.18

Example 3:
If you allow the PC of IP 192.168.1.40, 192.168.1.56, 192.168.1.100-192.168.1.120 to access port 50, port 53, port 100-120 only, the settings are:
Item 3: Enable
Filter entry: Allow
Port Number: 50, 53, 100-120
IP address: 192.168.1.40, 192.168.1.56, 192.168.1.100-120 (Figure 3-19)



Local IP Filtering

Item	IP address	Port	Block/Allow	Enable	Delete	Edit
1	192. 168. 1. 13-15	80	Block	□	□	○
2	192. 168. 1. 16-18	21	Allow	□	□	○
3	192. 168. 1. 40,56,100-120	50,53,100-120	Allow	□	□	○

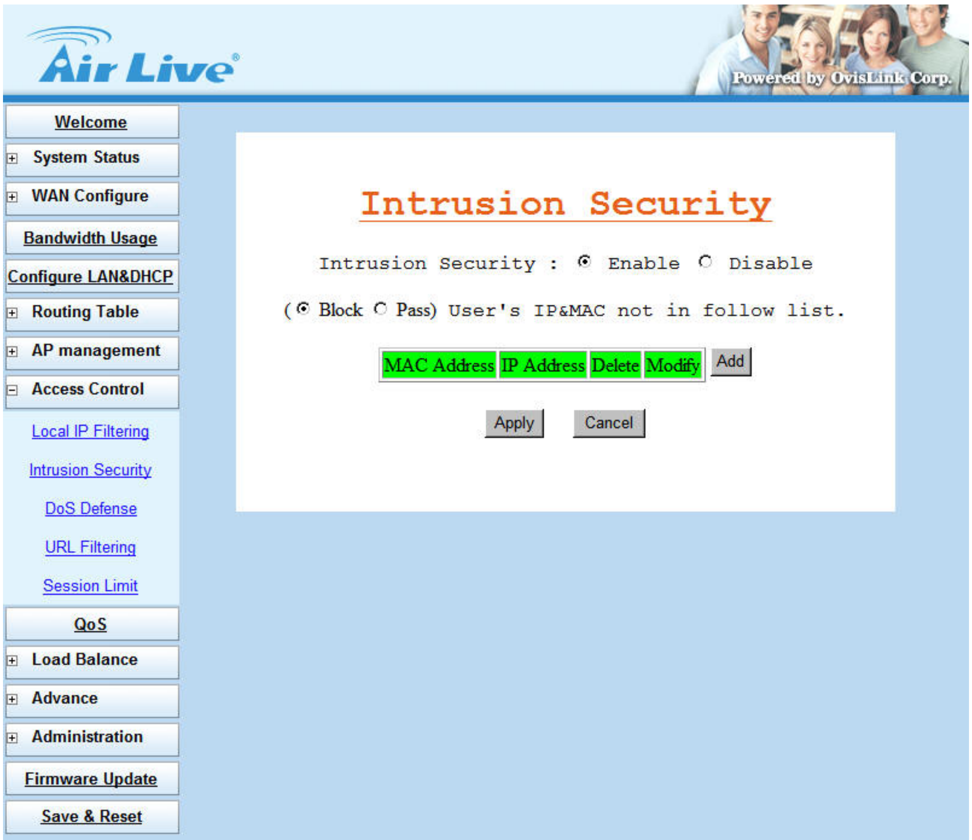
Figure 3-19 Local IP Filtering Example Setting

- **Protocol Port Number List**

Protocol	Service	Port no.	Protocol	Service	Port no.
TCP	FTP	21	TCP	LADP	389
TCP	SSH	22	TCP	HTTPS	443
TCP	TELNET	23	UDP	IKE	500
TCP	SMTP	25	TCP	RLOGIN	513
UDP	DNS	53	UDP	SYSLOG	514
UDP	TFTP	69	UDP	TALK	517,518
TCP	GOTHER	70	UDP	RIP	520
TCP	FINGER	79	TCP	AFPOWERTCP	548
TCP	HTTP	80	TCP	Net-Meeting	1503,1702
TCP	POP3	110	TCP	L2TP	1701
UDP	NFS	111	TCP	PPTP	1723
TCP	NNTP	119	TCP	AOL	5190~5194
UDP	NTP	123	UDP	PC Anywhere	5631~5632
TCP	IMAP	143	TCP	XWINDOW	6000-6063
UDP	SNMP	161	TCP	IRC	6660~6669
TCP	BGP	179	TCP	Real-Media	7070
TCP	WAIS	210	TCP		6000-6063

3.8.2 Intrusion Security

AirLive IGR-2500 features Intrusion Security, to allow user setting as “BLOCK” or “PASS” function following by the table content. The restricted user can be defined with its IP and MAC address.
(Figure 3-20)



Intrusion Security

Intrusion Security : ● Enable ○ Disable

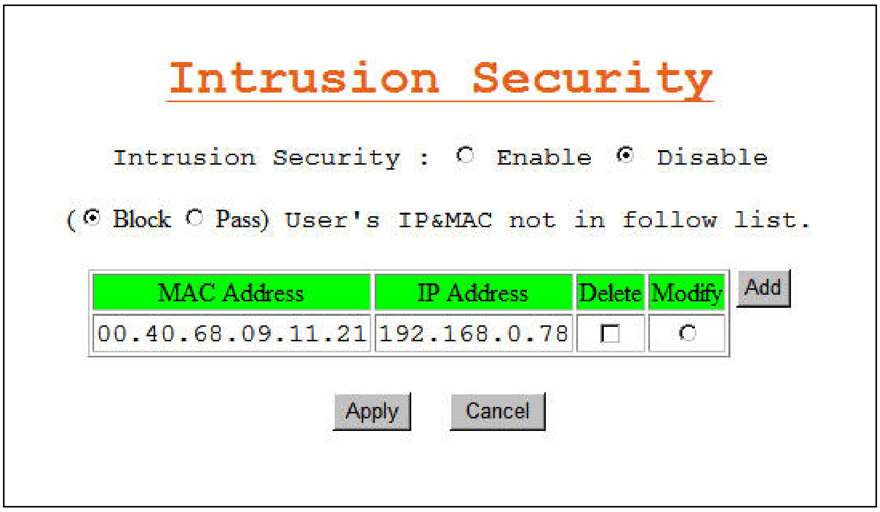
(● Block ○ Pass) User's IP&MAC not in follow list.

MAC Address	IP Address	Delete	Modify

Figure 3-20 Intrusion Security

- **Intrusion Security:** select **Enable** to enable Intrusion Security function.

Block or Pass User’s IP&MAC not in follow list: user can define an IP list, and decide the operating rule for the list to block or pass the connection. (Figure 3-21)



Intrusion Security

Intrusion Security : ○ Enable ● Disable

(● Block ○ Pass) User's IP&MAC not in follow list.

MAC Address	IP Address	Delete	Modify
00.40.68.09.11.21	192.168.0.78	□	○

Figure 3-21 Intrusion Security IP list

3.8.3 DoS Defense

AirLive IGR-2500 also provides DoS (Denial of Service Defense) function to protect your network servers, hosts, routers and other devices from the attacking of villain using mass data transmission. (Figure 3-22)

The default value in the display is the optimize parameter for Router. (Figure 3-23)

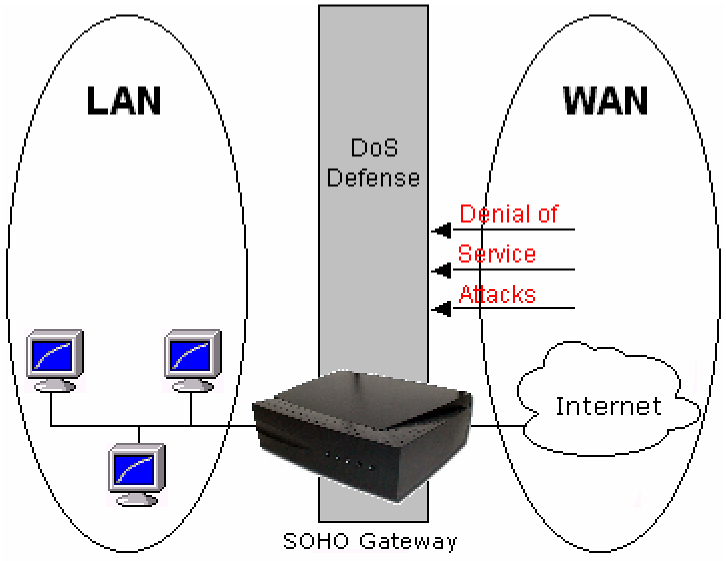
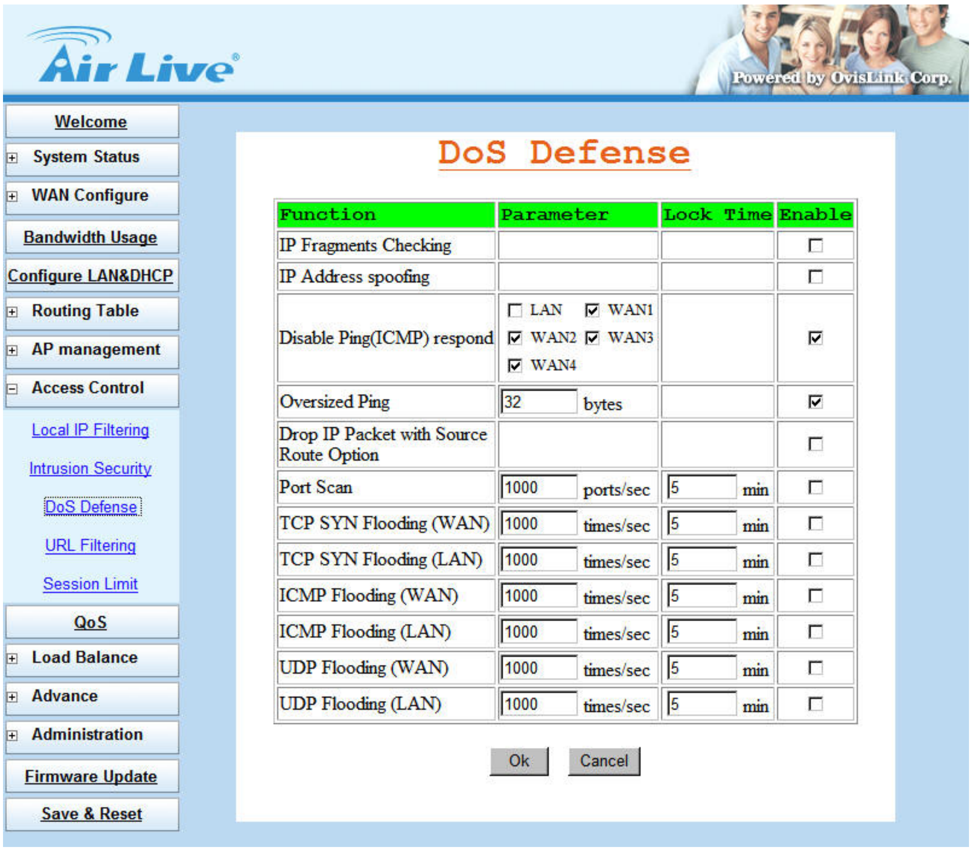


Figure 3-22 DoS Defense

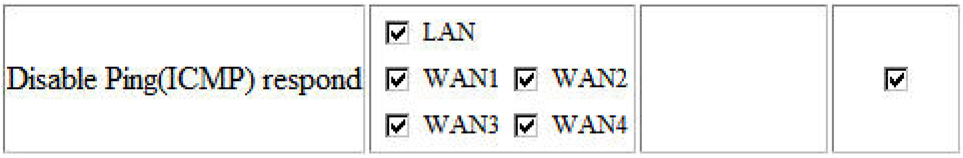


DoS Defense

Function	Parameter	Lock Time	Enable
IP Fragments Checking			□
IP Address spoofing			□
Disable Ping(ICMP) respond	□ LAN ☑ WAN1 ☑ WAN2 ☑ WAN3 ☑ WAN4		☑
Oversized Ping	32 bytes		☑
Drop IP Packet with Source Route Option			□
Port Scan	1000 ports/sec	5 min	□
TCP SYN Flooding (WAN)	1000 times/sec	5 min	□
TCP SYN Flooding (LAN)	1000 times/sec	5 min	□
ICMP Flooding (WAN)	1000 times/sec	5 min	□
ICMP Flooding (LAN)	1000 times/sec	5 min	□
UDP Flooding (WAN)	1000 times/sec	5 min	□
UDP Flooding (LAN)	1000 times/sec	5 min	□

Figure 3-23 Default Setting of DoS Defense

Some virus are using “PING” command to attack network, AirLive IGR-2500 can be defined as accept or reject “PING” command from WAN or LAN. (Figure 3-24)



Disable Ping(ICMP) respond	☑ LAN ☑ WAN1 ☑ WAN2 ☑ WAN3 ☑ WAN4		☑

Figure 3-24 Disable Ping respond

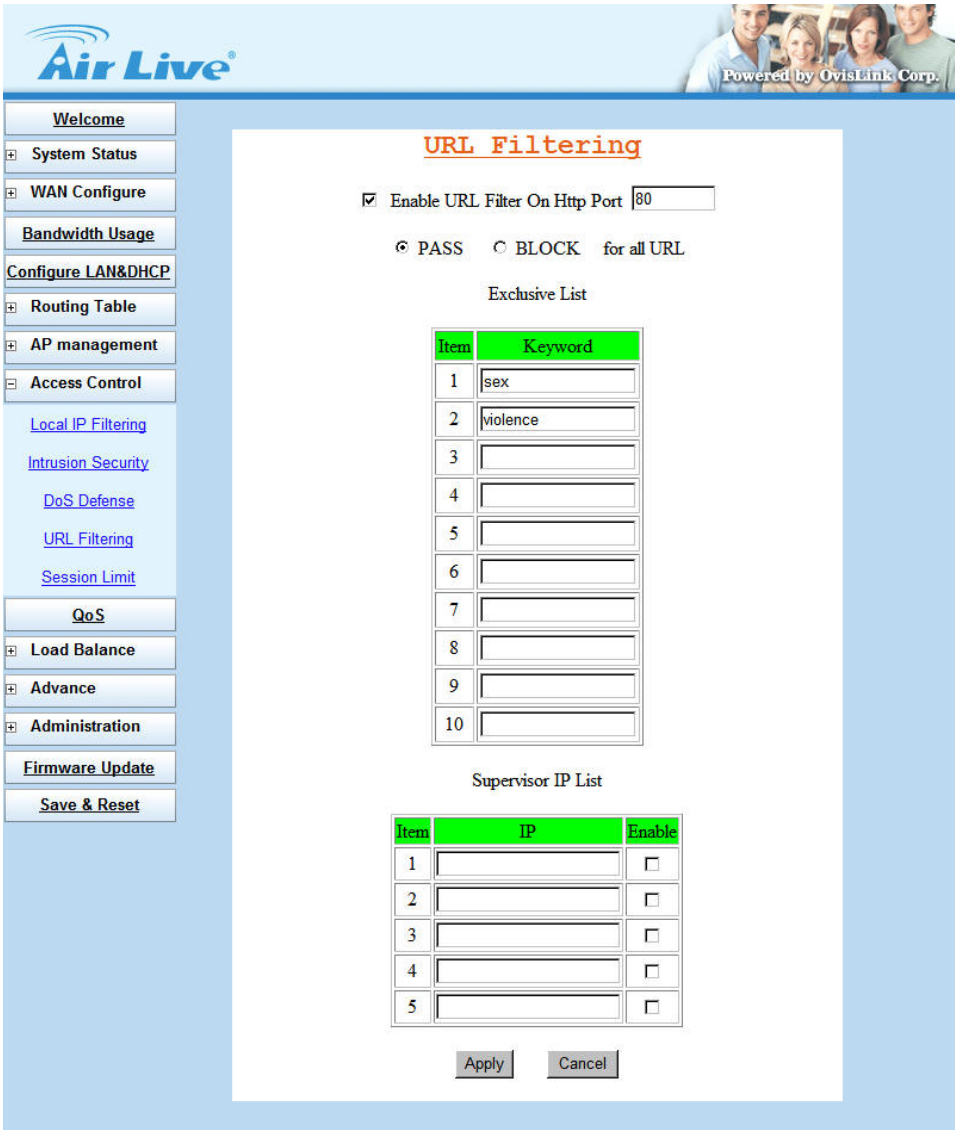
Function	Description
IP Fragments Checking	Checking the IP fragments. When it finds someone from WAN side tries to attack your network using overlap IP fragments in a bad attention, this function will check over these packets and drop them.
IP Address spoofing	Finding out whether the source address(s) and destination address(s) are legal IP’s or not. If they are illegal IP’s or multicast addresses, this function will cast these packets away.
Oversized Ping	Dropping the packets of “ping” which exceed the size you set. The default value is 32 bytes.
Drop IP Packet with Source Route Option	Casing a packet away when it contains source route option(s) in its IP.
Port Scan	When an IP from Internet tries to scan the IP of IGR-2500 up to 10000ports/sec (default value), this function will drop all the packets from this IP within 5 minutes (default value).
TCP SYN Flooding (WAN)	When a destination address and destination port of IGR-2500 receives TCP SYN packet from WAN over 10000 times (default value) in one second, IGR-2500 will close this address and port for 5 minutes (default value) temporarily.
TCP SYN Flooding (LAN)	When an IP in LAN of IGR-2500 tries to send TCP SYN packet over 10000 times (default value) in one second, IGR-2500 will close this source address for 5 minutes (default value) temporarily.
ICMP Flooding (WAN)	When a destination address of IGR-2500 receives ICMP from WAN over 10000 times (default value) in one second, IGR-2500 will close this address for 5 minutes (default value) temporarily.
ICMP Flooding (LAN)	When an IP in LAN of IGR-2500 tries to send ICMP over 10000 times (default value) in one second, IGR-2500 will close this source address for 5 minutes (default value) temporarily.
UDP Flooding (WAN)	When a destination address of IGR-2500 receives UDP from WAN over 10000 times (default value) in one second, IGR-2500 will close this address for 5 minutes (default value) temporarily.
UDP Flooding (LAN)	When an IP in LAN of IGR-2500 tries to send UDP over 10000 times (default value) in one second, IGR-2500 will close this source address for 5 minutes (default value) temporarily.

3.8.4 URL Filtering

Besides restrict users by local/destination IP, AirLive IGR-2500 provides you to do accessed restriction for user by URL as well.

You may restrict some URL address that are not allowed to reach

- **Enable URL Filter On Http Port:** You can define the port number for URL Filtering, and select to enable the rule.
- **PASS or BLOCK for all URL:** Select a basic rule as the foundation, and then to define the **Exclusive List**.
- **Exclusive List:** Define specific keyword as the Exclusive List.
  - **Keyword:** destination URL that prohibit users to reach
- **Supervisor IP List**: Specify IP address that will not be filtered with URL filtering rule. (Figure 3-25)



URL Filtering

☑ Enable URL Filter On Http Port 80

● PASS ○ BLOCK for all URL

Exclusive List

Item	Keyword
1	sex
2	violence
3	
4	
5	
6	
7	
8	
9	
10	

Supervisor IP List

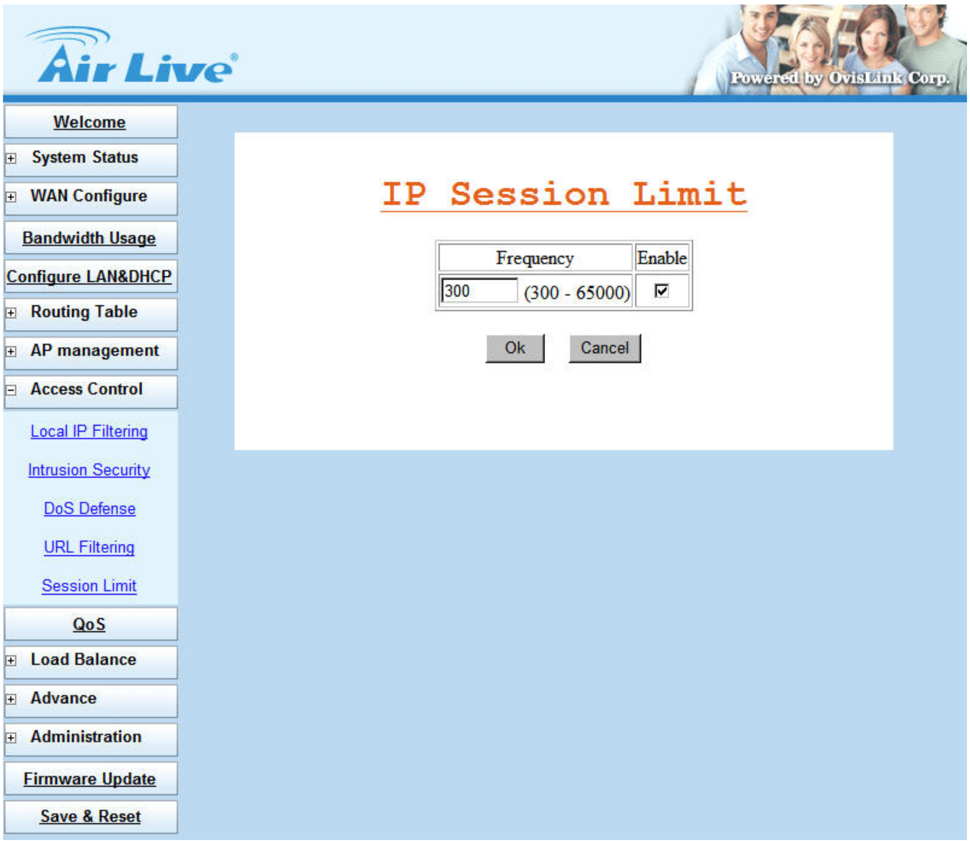
Item	IP	Enable
1		□
2		□
3		□
4		□
5		□

Figure 3-25 Disable Ping respond

3.8.5 Session Limit

AirLive IGR-2500 features Session Limit to restrict each IP connection’s session. This feature can assure the network performance from being attacked by infected PC, which can create and spread out lots of session in a short time.

- **Frequency:** The maximum session number of connection. The available range is 300 ~ 65500. (Figure 3-26)



IP Session Limit

Frequency	Enable
300 (300 - 65000)	☑

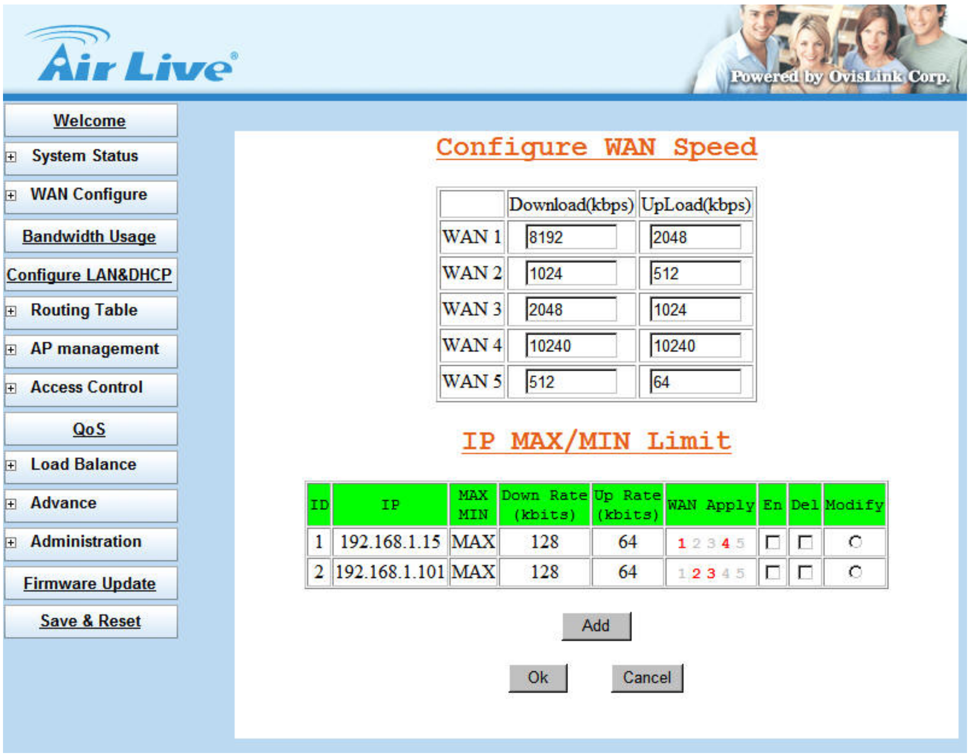
Ok Cancel

Figure 3-26 Session Limit

3.9 QoS

With QoS function, you can set up **user bandwidth** with Maximum & Minimum bandwidth value.

- **Configure WAN Speed:** The WAN speeds must be configured for the QoS configuration to take effect.
- **IP MAX/MIN Limit:** Allocate bandwidth to users:
    - **IP:** IP address of specified user
    - **MAX:** Bandwidth limitation to this user
    - **MIN:** Minimal Bandwidth keeps for this user before allocating any bandwidth from this user to others
    - **Down Rate:** Download speed
    - **Up Rate:** Upload speed
    - **WAN Apply:** Which WAN you want the allocation to take effect. (Do not use this option to specify which WAN to use for this user.) (Figure 3-27)



Configure WAN Speed

	Download(kbps)	UpLoad(kbps)
WAN 1	8192	2048
WAN 2	1024	512
WAN 3	2048	1024
WAN 4	10240	10240
WAN 5	512	64

IP MAX/MIN Limit

ID	IP	MAX MIN	Down Rate (kbits)	Up Rate (kbits)	WAN Apply	En	Del	Modify
1	192.168.1.15	MAX	128	64	**1** 2 3 **4** 5	□	□	○
2	192.168.1.101	MAX	128	64	1 **2** **3** 4 5	□	□	○

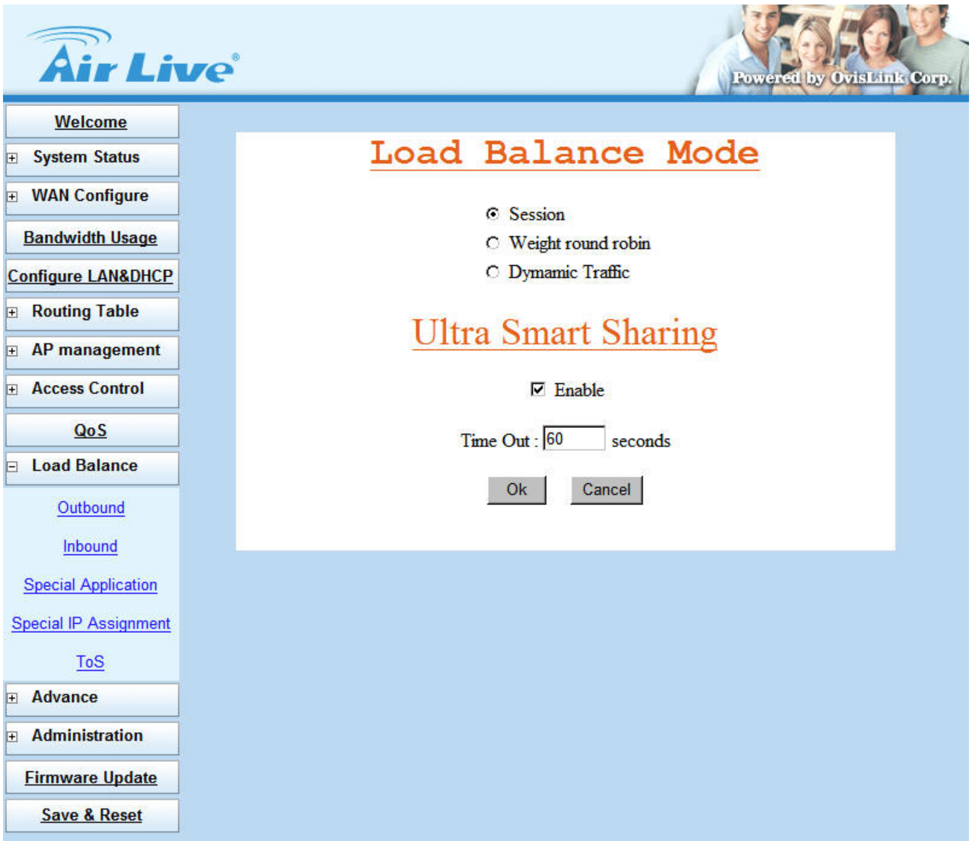
Figure 3-27 QoS Setting

3.10 Load Balance

3.10.1 Outbound Load Balance

AirLive IGR-2500 provides three kinds of work mode for **Outbound Load Balance**, and **Ultra Smart Sharing** feature to offer intelligent connection solution for banking system and Internet on-line game server. The load balance types include **Session**, **Weight round robin**, and **Dynamic Traffic**.

- **Session:** When user chooses this mode, the router will assign each coming session to each WAN port one by one, no matter how traffic loading is on each WAN port. All the enabled WAN ports have the same bandwidth rate (1:1). (Figure 3-28)



Load Balance Mode

● Session
○ Weight round robin
○ Dymamic Traffic

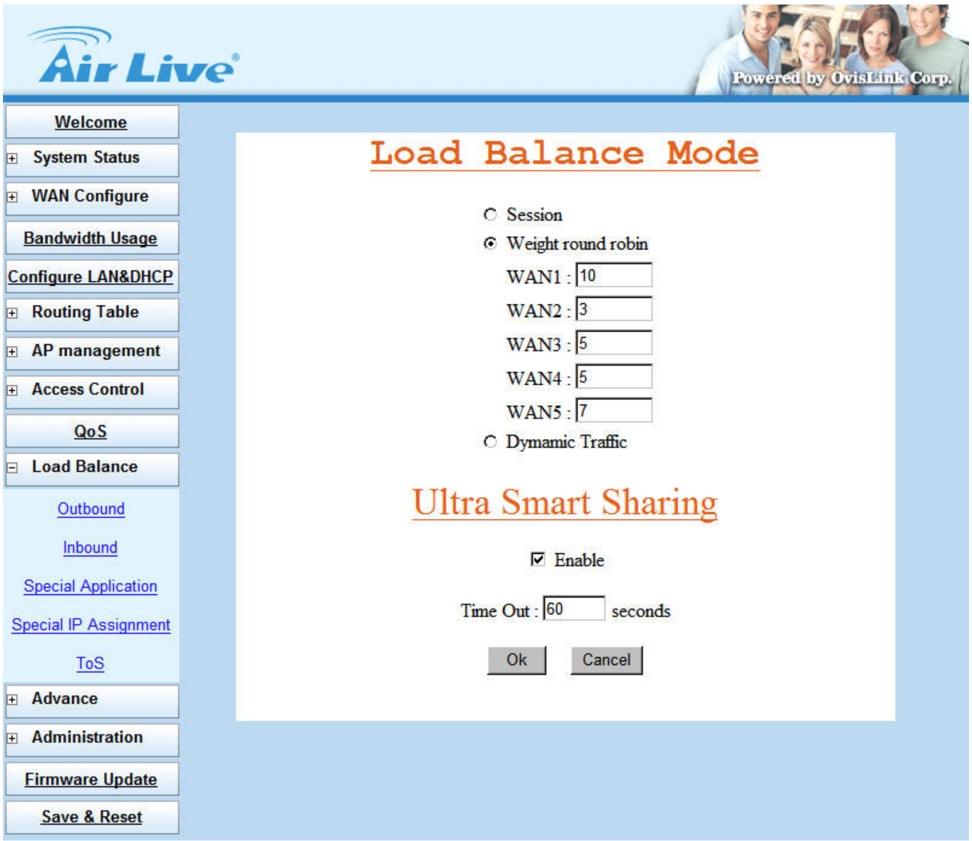
Ultra Smart Sharing

☑ Enable

Time Out : 60 seconds

Figure 3-28 Outbound Load Balance – Session

- **Weight round robin:** Configure the WAN ports bandwidth rate manually, means you can distribute each coming session from users to each WAN port, following the rate that you assign in each WAN port. The session number in each WAN can be numbered from **1 to 100**, the suggest number is under 1 ~10. If rate is 1:1 for each WAN port, the router function will act like Session mode. (Figure 3-29)



Load Balance Mode

○ Session

● Weight round robin

WAN1 : 10

WAN2 : 3

WAN3 : 5

WAN4 : 5

WAN5 : 7

○ Dymamic Traffic

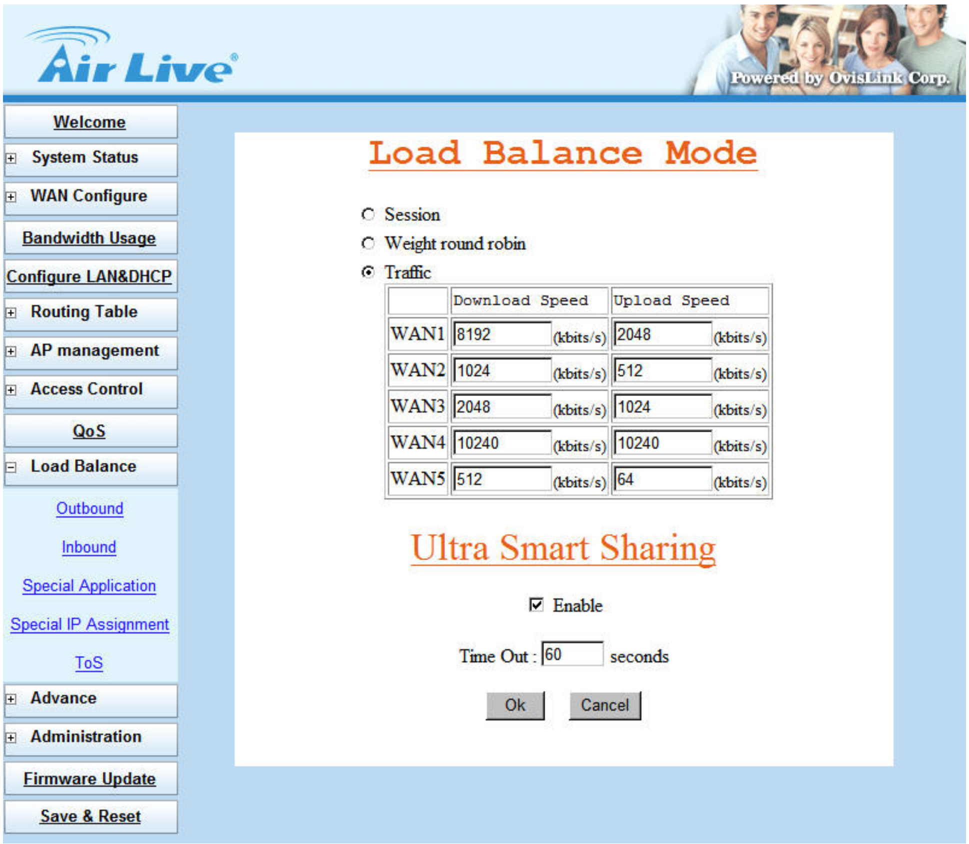
Ultra Smart Sharing

☑ Enable

Time Out : 60 seconds

Figure 3-29 Outbound Load Balance – Weight round robin

- **Traffic:** Router will find the lowest loading WAN port to transmit and receive data automatically. You need to enter correct ADSL/CABLE WAN speed in here. (Figure 3-30)



Load Balance Mode

○ Session

○ Weight round robin

● Traffic

	Download Speed	Upload Speed
WAN1	8192 (kbits/s)	2048 (kbits/s)
WAN2	1024 (kbits/s)	512 (kbits/s)
WAN3	2048 (kbits/s)	1024 (kbits/s)
WAN4	10240 (kbits/s)	10240 (kbits/s)
WAN5	512 (kbits/s)	64 (kbits/s)

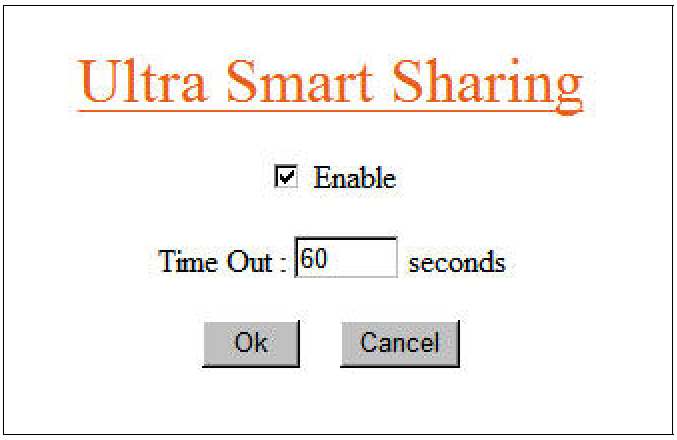
Ultra Smart Sharing

☑ Enable

Time Out : 60 seconds

Figure 3-30 Outbound Load Balance – Dynamic Traffic

- **Ultra Smart Sharing:** When user enables this function, IGR-2500 will lock user packet at dedicated WAN port, the dedicated WAN port will be selected base on 1st user packet (This feature is suitable for Game, VoIP, banking system …etc). (Figure 3-31)
  - **Time out Timer:** Default is 60 second, range from 30 ~255. User will be removed from WAN user list if no user packet RX/TX passes through the dedicated WAN port after timer expired.



Ultra Smart Sharing

☑ Enable

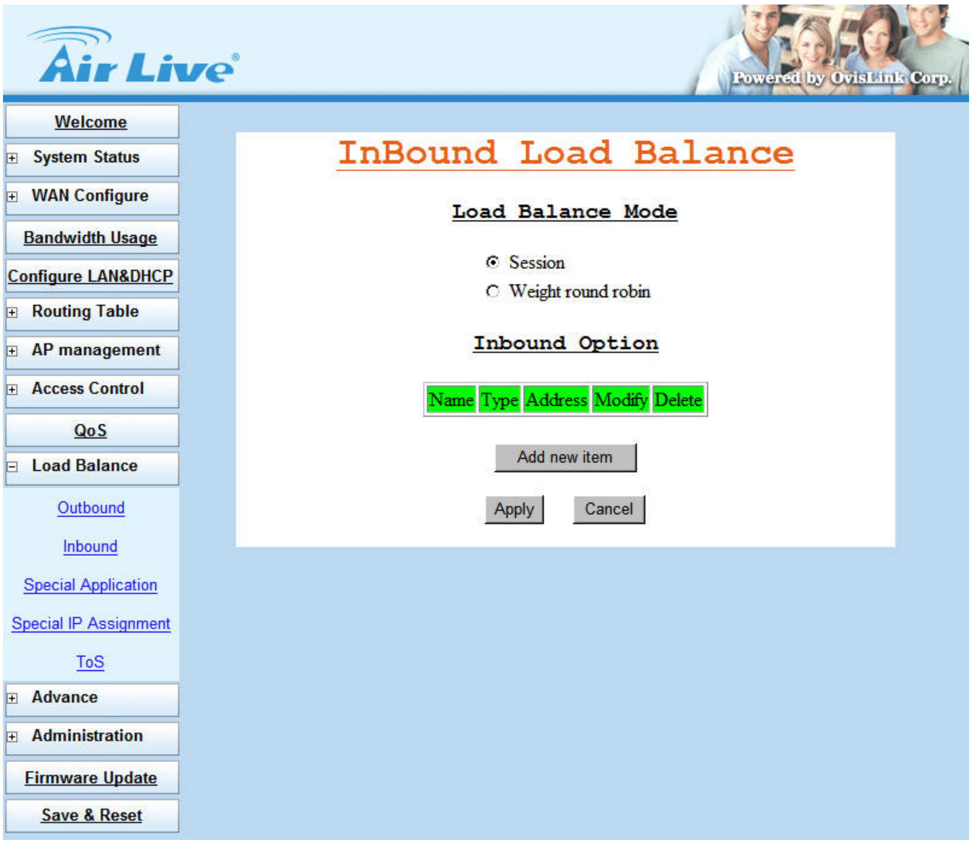
Time Out : 60 seconds

Figure 3-31 Outbound Load Balance – Ultra Smart Sharing

3.10.2 Inbound Load Balance

Inbound function can let you load sharing traffic that coming from Internet to access you intranet server via each WAN link, this function can increase WAN utilization. (Figure 3-32)

For more detail usage, please refer to **Appendix A**.



InBound Load Balance

Load Balance Mode

● Session
○ Weight round robin

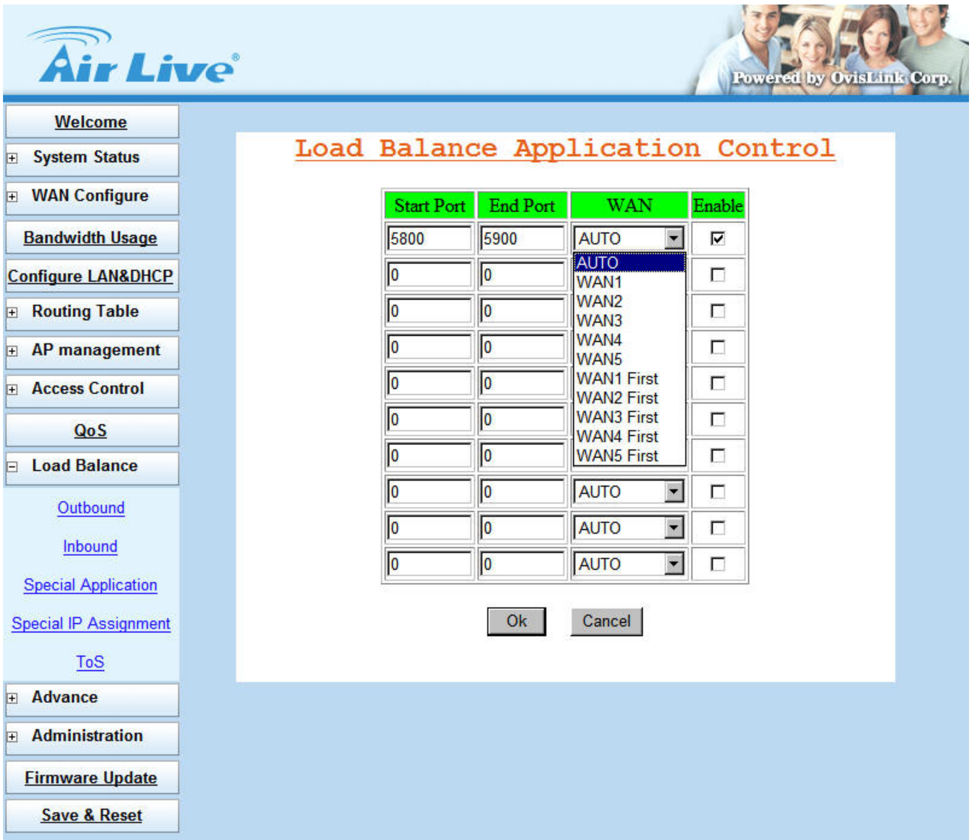
Inbound Option

Name	Type	Address	Modify	Delete

Figure 3-32 Inbound Load Balance

3.10.3 Special Application

Some Internet WEB server do not allow access with multi WAN address, also these WEB server was using dynamic IP address, in this case, AirLive IGR-2500 can let you just define dedicated port number allocated with dedicated WAN port, and the dedicated port was used to access these special WEB Server. (Figure 3-33)



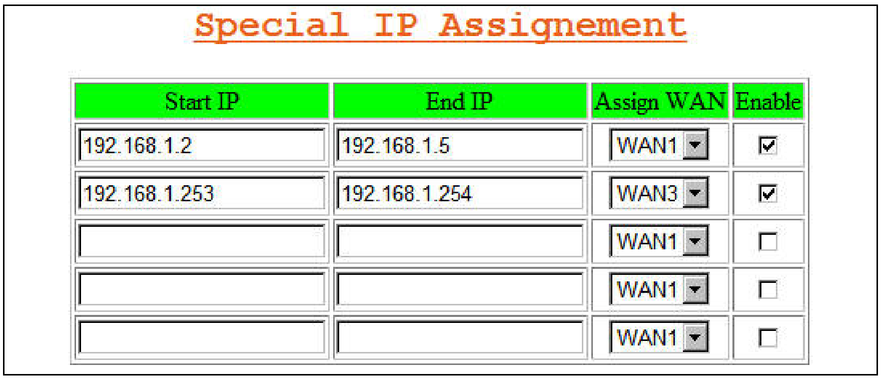
Load Balance Application Control

Start Port	End Port	WAN	Enable
5800	5900	AUTO	☑
0	0		☐
0	0		☐
0	0		☐
0	0		☐
0	0		☐
0	0		☐
0	0	AUTO	☐
0	0	AUTO	☐
0	0	AUTO	☐

Figure 3-33 Special Application

3.10.4 Special IP Assignment

Same as above mentioned, AirLive IGR-2500 can let you defined dedicated IP address (destination IP address or Source IP address) allocated with dedicated WAN port. (Figure 3-34)



Special IP Assignement

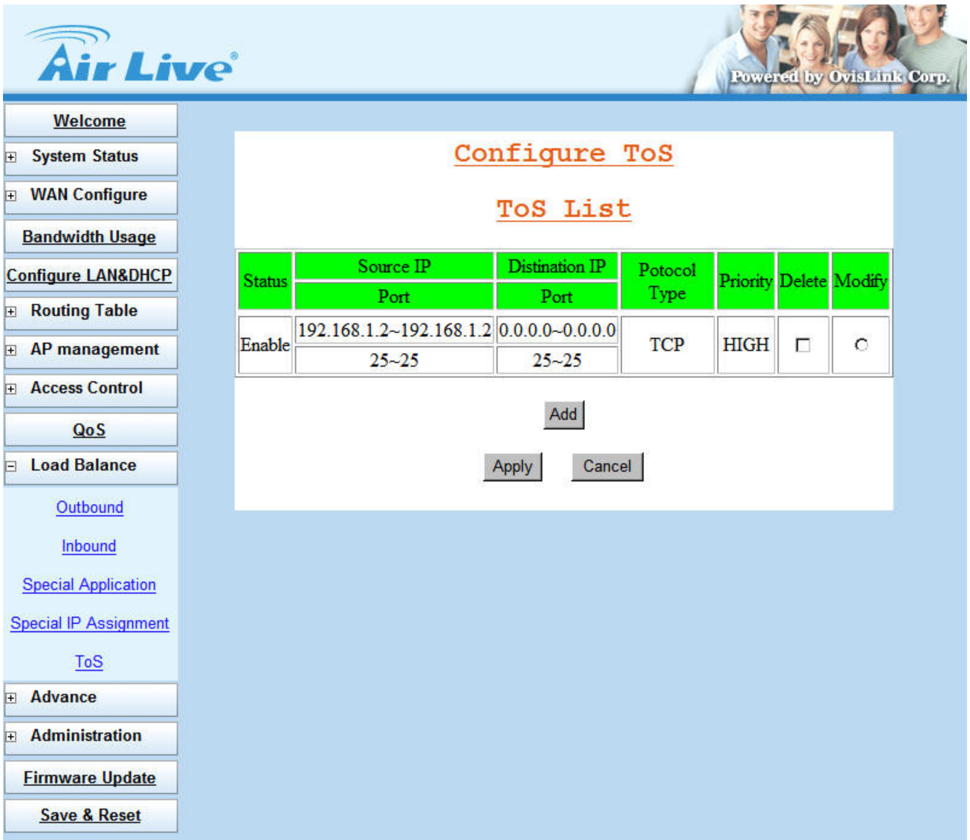
Start IP	End IP	Assign WAN	Enable
192.168.1.2	192.168.1.5	WAN1	☑
192.168.1.253	192.168.1.254	WAN3	☑
		WAN1	☐
		WAN1	☐
		WAN1	☐

Figure 3-34 Special IP Assignment

3.10.5 TOS

TOS function can let you setting the priority for dedicated packet. (Figure 3-35)

User can specify the **Source IP**, **Destination IP**, **Protocol type**, **Source port number**, **Destination port number** and **Priority** for TOS feature. (Figure 3-36)

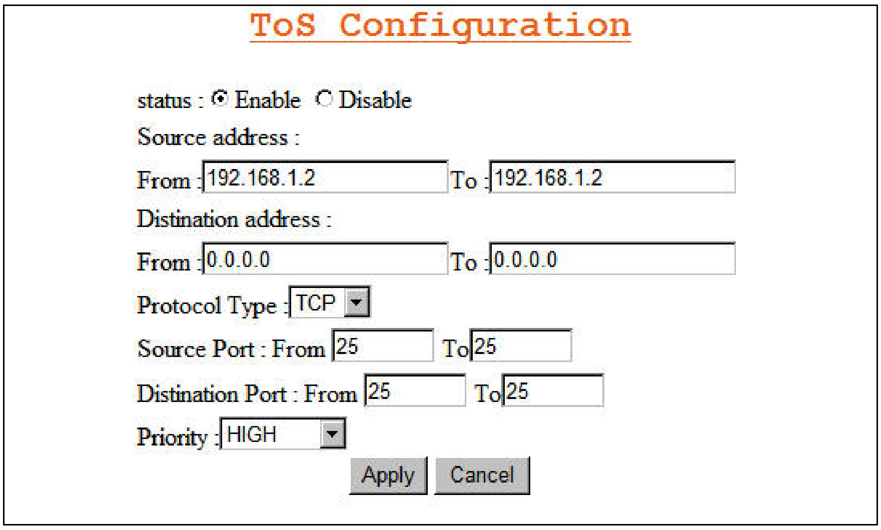


Configure ToS

ToS List

Status	Source IP	Distination IP	Potocol Type	Priority	Delete	Modify
	Port	Port				
Enable	192.168.1.2~192.168.1.2	0.0.0.0~0.0.0.0	TCP	HIGH	□	○
	25~25	25~25				

Figure 3-35 TOS



ToS Configuration

status : ● Enable ○ Disable

Source address :

From : 192.168.1.2 To : 192.168.1.2

Distination address :

From : 0.0.0.0 To : 0.0.0.0

Protocol Type : TCP

Source Port : From 25 To 25

Distination Port : From 25 To 25

Priority : HIGH

Figure 3-36 TOS Configuration

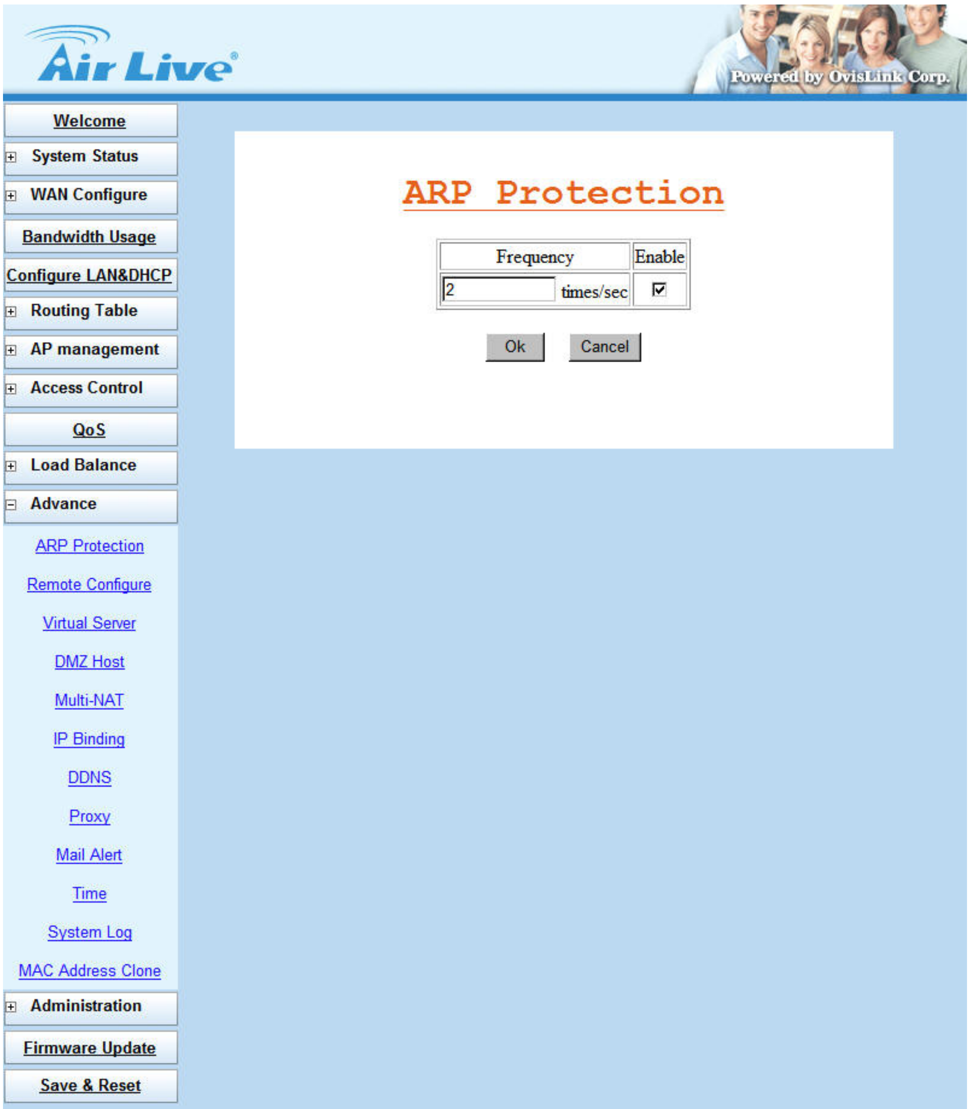
3.11 Advance

3.11.1 ARP Protection

To prevent the ARP cheating from virus, AirLive IGR-2500 offers you a feature named ARP protection; it will spread out router's IP and MAC address to LAN user in every specific time.

- **Frequency times/sec:** User can define the time for ARP protection service. For example, if you define the Frequency to 2, IGR-2500 will broadcast its MAC address twice to LAN users in every second.

(Figure 3-37)



ARP Protection

Frequency	Enable
2 times/sec	☑

Figure 3-37 TOS Configuration

3.11.2 Remote Configure

The AirLive IGR-2500 can be managed from any PC from Internet. If enable “Remote Configure” function, remote user can access the Web-based from router’s WAN interface via Internet; If “Remote Configure” does not enable, the access is only available to PCs from LAN. The accessed port number is changeable. (Figure 3-38)

- **Assigning Remote IP:** Specific dedicated PC can access IGR-2500 remotely.
    - Leaving these fields blank will allow access by all PCs
    - If enter specific IP address, only this address PC can access device remotely.
    - The address must be public IP addresses.

Example: If the local user:

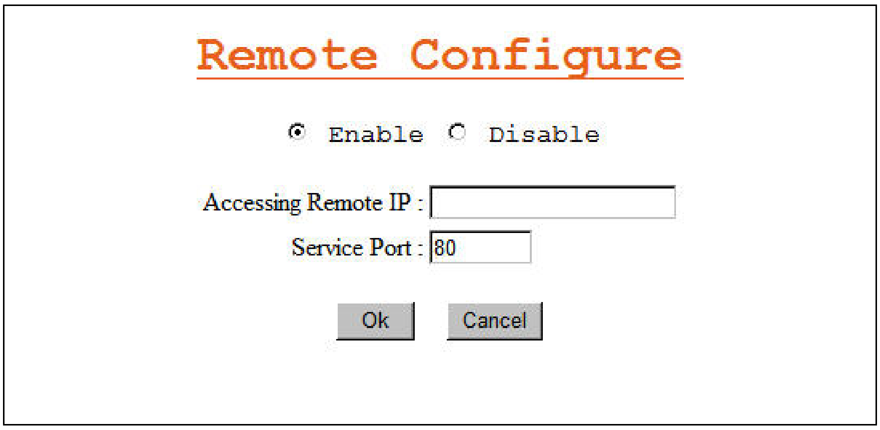
Enable the remote configure function

Remote port is ***80*** **(default is 80, can be different port number)**

Remote IP is blank.

ROUTER WAN port IP is ***110.111.112.1***

When the user of remote side wants to access IGR-2500 web configure, the remote user only needs to enter ***http:// 110.111.112.1***



Remote Configure

● Enable ○ Disable

Accessing Remote IP :

Service Port : 80

Figure 3-38 Remote Configure

3.11.3 Virtual Server

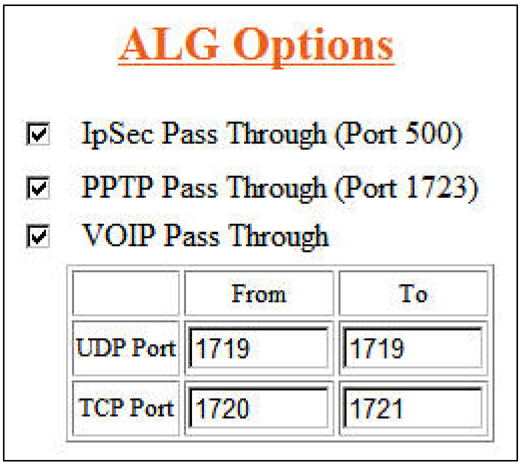
AirLive IGR-2500 ALG Options to allow IPSec, PPTP and VoIP pass-through, user can also define the port number for ALG Options.

You may have FTP, MAIL, VPN or other server on your LAN. If you would like to allow the global users access some servers providing special services on your LAN. This function can help you to do this.
Provide with global port & local port mapping function, let you easily configure internal server with same port number mapping to WAN IP different port number.

ALG Options:

- **VPN Pass Through:** For IPSec and PPTP
- **VoIP Pass Through:** VoIP Gateway can be connected directly to IGR-2500 LAN port, and open the corresponded VoIP port number.

(Figure 3-39)



ALG Options

☑ IpSec Pass Through (Port 500)

☑ PPTP Pass Through (Port 1723)

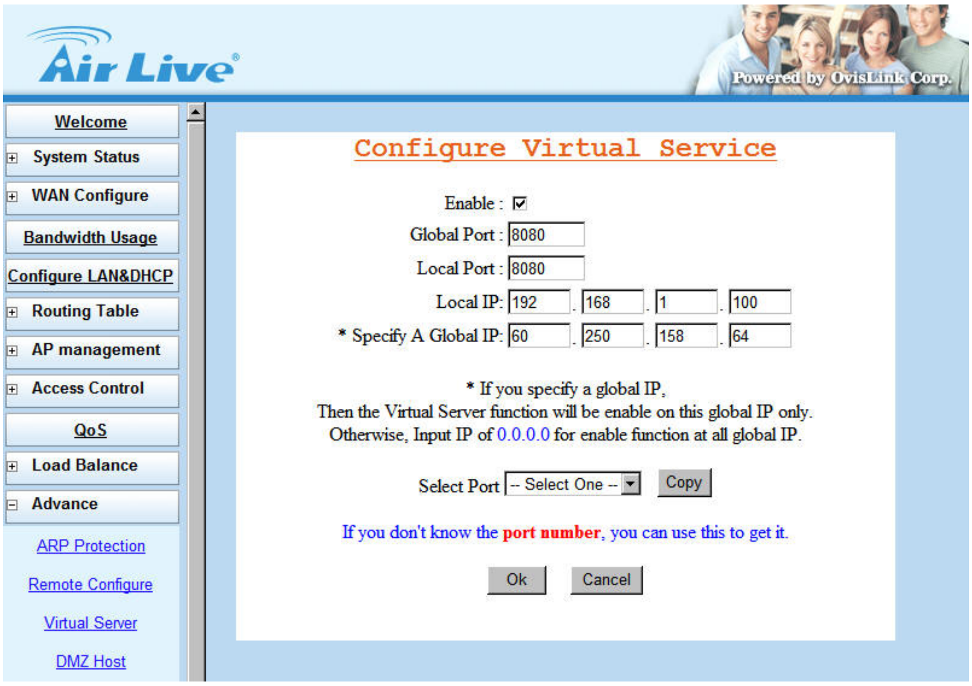
☑ VOIP Pass Through

	From	To
UDP Port	1719	1719
TCP Port	1720	1721

Figure 3-39 ALG Options and Pass Through

Virtual Server: (Figure 3-40)

- **Global port:** WAN virtual protocol number
- **Local port:** used by internal server port number
- **Local IP:** local server IP address
- **Specify A Global IP:** You can select to define one IP address from IGR-2500 several WAN ports setting. If you specify Global IP address with 0.0.0.0, the Internet user will be able to access virtual server from all the WAN port IP addresses.
- **Select Port:** If you don’t know the port number, you can use this feature to select the service you want to define.



Configure Virtual Service

Enable : ☑

Global Port : 8080

Local Port : 8080

Local IP: 192 . 168 . 1 . 100

* Specify A Global IP: 60 . 250 . 158 . 64

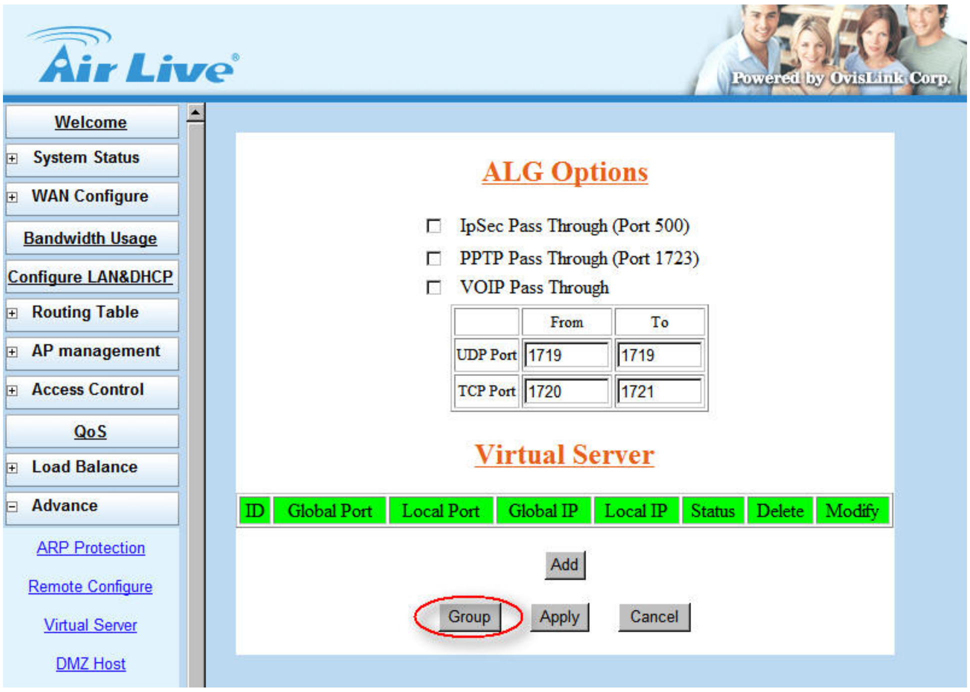
* If you specify a global IP,
Then the Virtual Server function will be enable on this global IP only.
Otherwise, Input IP of 0.0.0.0 for enable function at all global IP.

Select Port -- Select One --

If you don't know the **port number**, you can use this to get it.

Figure 3-40 Virtual Server

Group Virtual Server: If you would like to define more than one service port number into a virtual server rule, you can use **Group Virtual Server**. (Figure 3-41)



ALG Options

□ IpSec Pass Through (Port 500)

□ PPTP Pass Through (Port 1723)

□ VOIP Pass Through

	From	To
UDP Port	1719	1719
TCP Port	1720	1721

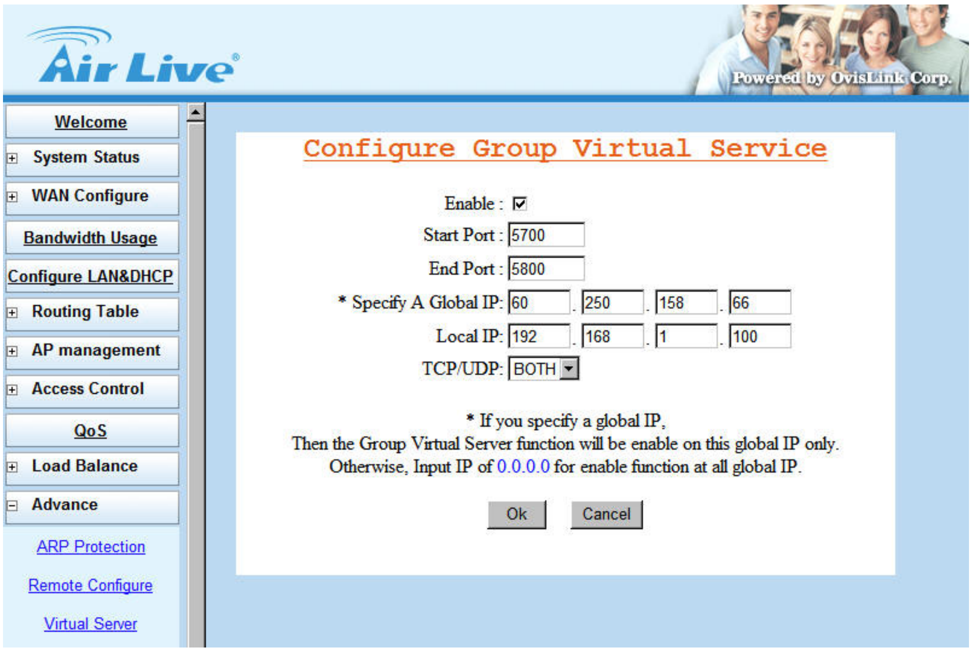
Virtual Server

ID	Global Port	Local Port	Global IP	Local IP	Status	Delete	Modify

Figure 3-41 Group Virtual Server

- **Start port:** The start port number of the port range.
- **End port:** The end port number of the port range.
- **Specify A Global IP:** User can select to define one IP address from IGR-2500 several WAN ports setting. If you specify Global IP address with 0.0.0.0, the Internet user will be able to access virtual server from all the WAN port IP addresses.
- **Local IP:** local server IP address
- **TCP/UDP:** The item is selected to define the port number type with TCP, UDP, or both.

(Figure 3-42)



Configure Group Virtual Service

Enable : ☑
Start Port : 5700
End Port : 5800
* Specify A Global IP: 60 . 250 . 158 . 66
Local IP: 192 . 168 . 1 . 100
TCP/UDP: BOTH

* If you specify a global IP,
Then the Group Virtual Server function will be enable on this global IP only.
Otherwise, Input IP of 0.0.0.0 for enable function at all global IP.

Figure 3-42 Group Virtual Server Setting

For example: (Figure 3-43)

Suppose you want to install servers dedicated with specific WAN port as following:

1. Internet user can access FTP server from WAN1

2. Internet user can access VNC from WAN 2.

3. Internet user can ERP server from all the WAN port.

Environment:

WAN1 IP address: Static IP address 60.250.158.64

WAN2 IP address: Static IP address 230.74.69.15

WAN3 IP address: Dynamic IP

WAN4 IP address: PPPoE

LAN server:

FTP server (TCP 21): 192.168.1.10

VNC client (TCP 5800, 5900): 192.168.1.50

ERP server (TCP 1394 ~ TCP 1400): 192.168.1.120

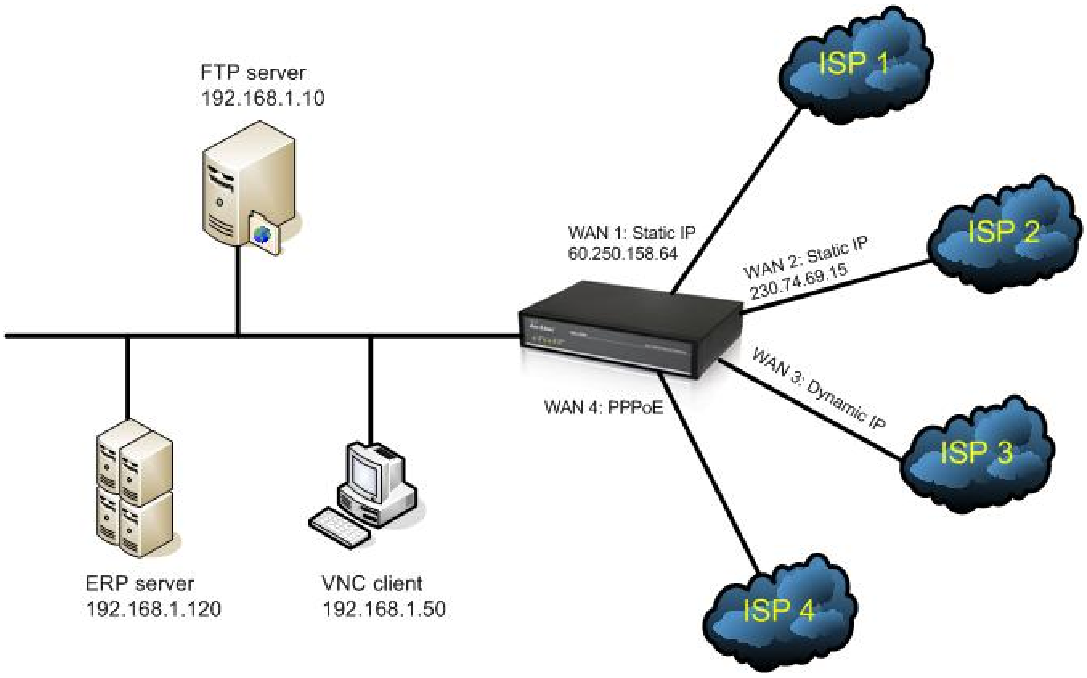
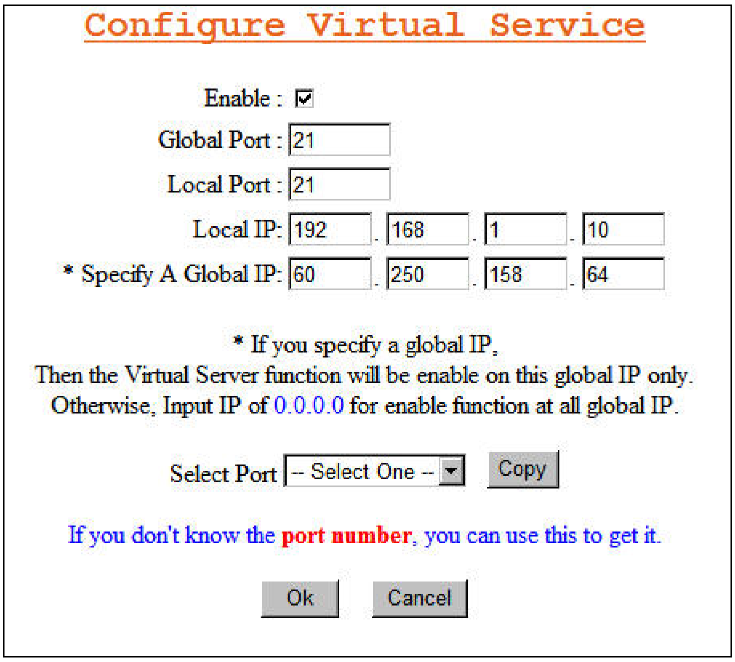


Figure 3-43 Example Topology

Example 1: Define Virtual server to allow FTP service (TCP 21) packets from Internet to LAN FTP server via WAN1. (Figure 3-44)



Configure Virtual Service

Enable : ☑

Global Port : 21

Local Port : 21

Local IP: 192 . 168 . 1 . 10

* Specify A Global IP: 60 . 250 . 158 . 64

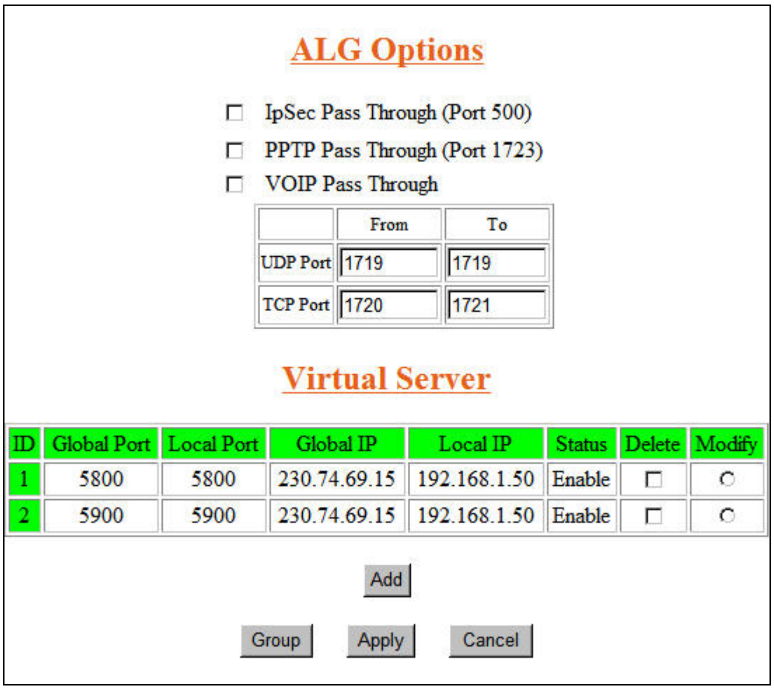
* If you specify a global IP,
Then the Virtual Server function will be enable on this global IP only.
Otherwise, Input IP of 0.0.0.0 for enable function at all global IP.

Select Port -- Select One -- Copy

If you don't know the **port number**, you can use this to get it.

Figure 3-44 Example1 setting

Example 2: Define Virtual server to allow VNC service (TCP 5800, TCP 5900) packets from Internet to LAN VNC client via WAN2. (Figure 3-45)



ALG Options

□ IpSec Pass Through (Port 500)

□ PPTP Pass Through (Port 1723)

□ VOIP Pass Through

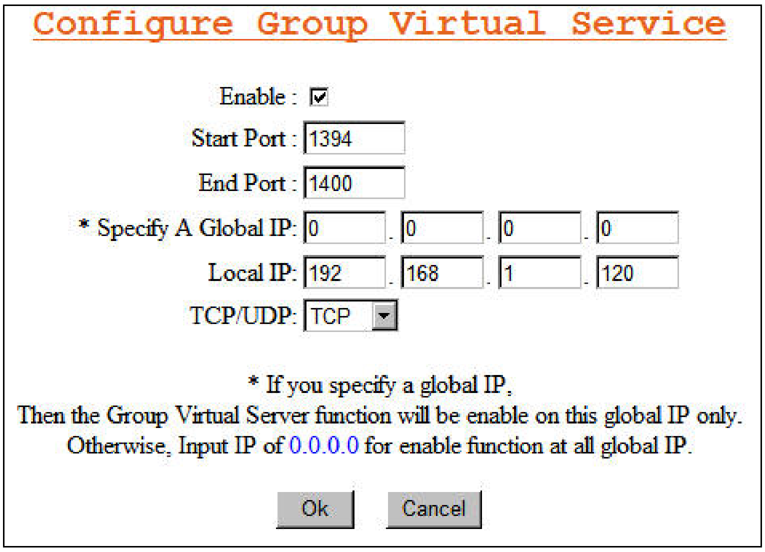
	From	To
UDP Port	1719	1719
TCP Port	1720	1721

Virtual Server

ID	Global Port	Local Port	Global IP	Local IP	Status	Delete	Modify
1	5800	5800	230.74.69.15	192.168.1.50	Enable	□	○
2	5900	5900	230.74.69.15	192.168.1.50	Enable	□	○

Figure 3-45 Example2 setting

Example 3: Define Virtual server to allow packets TCP 1394 ~ 1400 from Internet to ERP server via all the WAN interfaces. (Figure 3-46)



Configure Group Virtual Service

Enable : ☑

Start Port : 1394

End Port : 1400

* Specify A Global IP: 0 . 0 . 0 . 0

Local IP: 192 . 168 . 1 . 120

TCP/UDP: TCP

* If you specify a global IP,
Then the Group Virtual Server function will be enable on this global IP only.
Otherwise, Input IP of 0.0.0.0 for enable function at all global IP.

Figure 3-46 Example3 setting

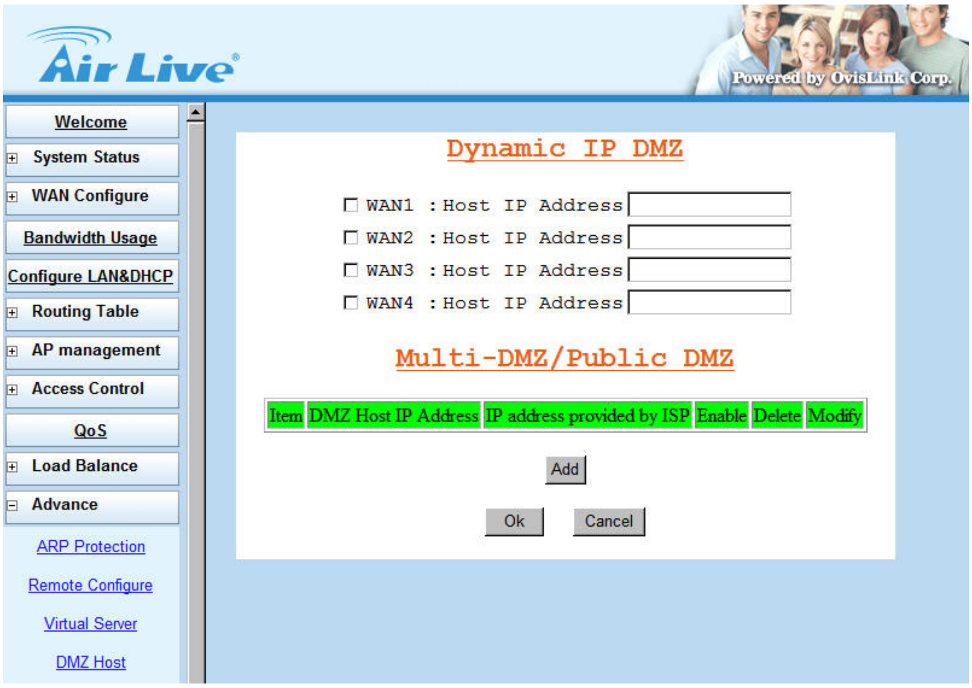
3.11.3 DMZ Host

The **Demilitarized Zone (DMZ)** function provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, and from the LAN to the DMZ, but traffic from the DMZ to the LAN is denied. Internet users can access to host servers configured in DMZ Host list, but can not access to the LAN, unless special filter rules were configured to permit the access by the administrator or the user who is an authorized remote user.

It is highly recommended that you keep all sensitive information off of the public servers, and store sensitive information in computers on LAN.

If you would like to grant remote users the right to access one of your computers on LAN to perform some actions such as Internet games, you must enable the function of DMZ. When remote users access your legal IP(s), IGR-2500 will transmit these packets to the corresponding virtual IP(s).
(Figure 3-47)



Dynamic IP DMZ

□ WAN1 : Host IP Address

□ WAN2 : Host IP Address

□ WAN3 : Host IP Address

□ WAN4 : Host IP Address

Multi-DMZ/Public DMZ

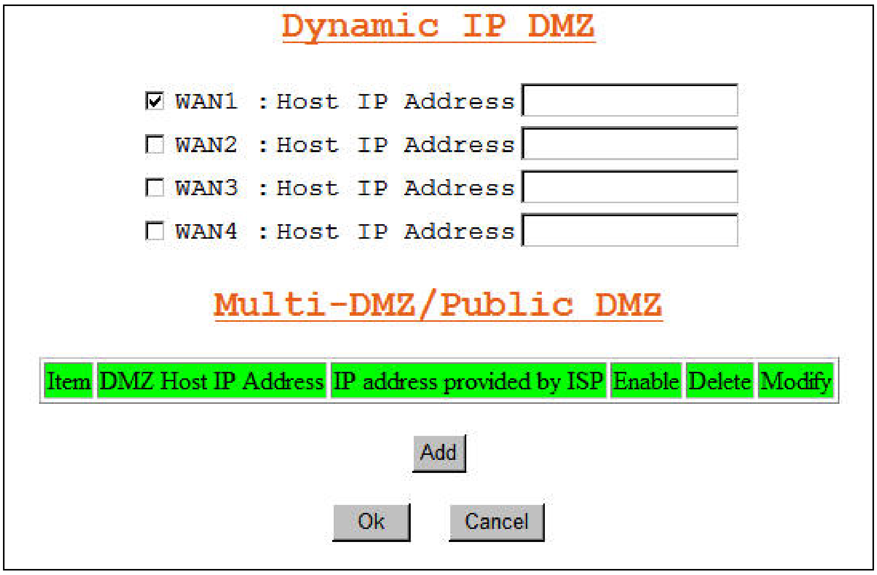
Item	DMZ Host IP Address	IP address provided by ISP	Enable	Delete	Modify

Figure 3-47 Dynamic IP DMZ

- **Dynamic IP DMZ:**

When a WAN port IP is assigned by ISP and obtained by PPPoE or Dynamic IP, you can use this section to specify the DMZ host disregarding the exact WAN IP address. Tick the WAN port option and fill in the IP address of the DMZ host inside the network, the IGR-2500 will map the corresponding WAN IP to the internal DMZ host automatically. When a remote computer wants to access the internal LAN through this WAN, if the accessed port number is not specified by Virtual Server Host, it will be mapped into this internal DMZ host. For example, if your WAN1 uses PPPoE connection to obtain a public IP address, the IGR-2500 will let data packet with destination address point to WAN1, and pass through into DMZ Host when the port number of the packet does not exist in Virtual Server Host table.

(Figure 3-48)



Dynamic IP DMZ

☑ WAN1 : Host IP Address

☐ WAN2 : Host IP Address

☐ WAN3 : Host IP Address

☐ WAN4 : Host IP Address

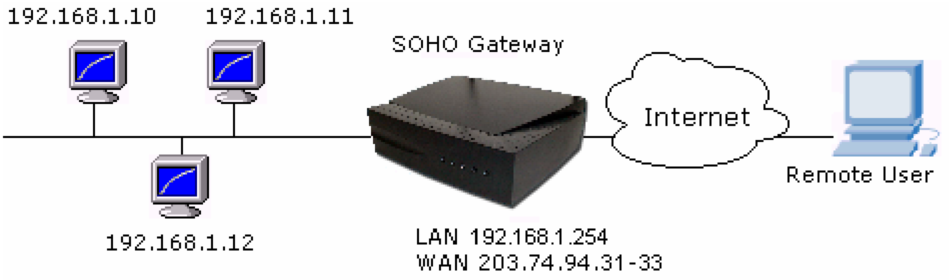
Multi-DMZ/Public DMZ

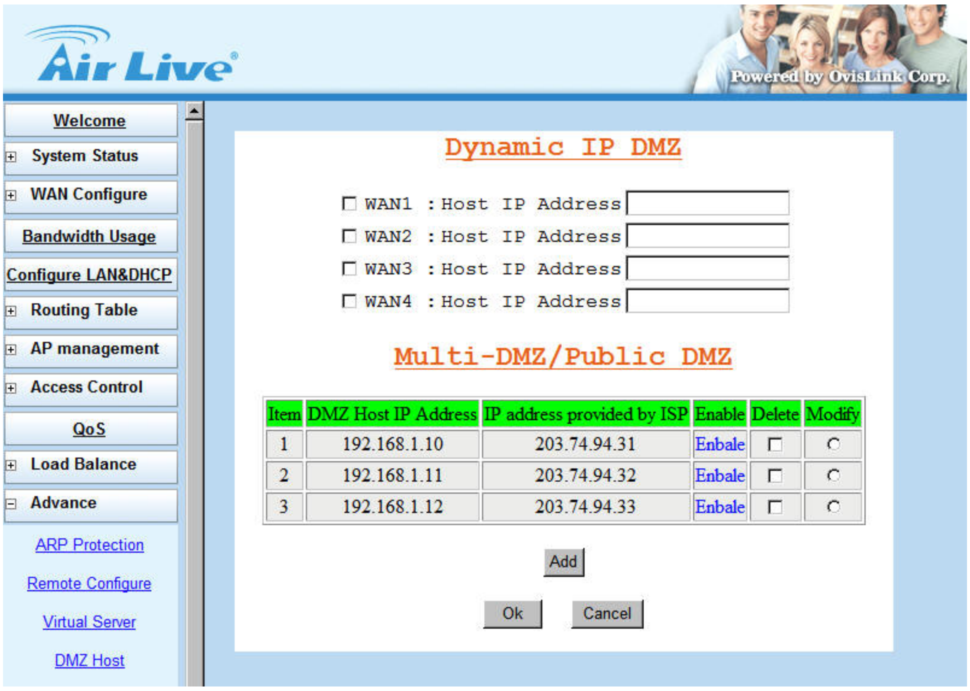
Item	DMZ Host IP Address	IP address provided by ISP	Enable	Delete	Modify

Figure 3-48 Dynamic IP DMZ

- **Multi-DMZ:**

If you use fixed WAN IP address assigned by your ISP, you can use this section to specifically assign the WAN IP address to corresponding DMZ host. If you own several legal WAN IPs, you can assign which WAN IP correspond to which IP on your LAN. This assignment will let most protocol to access the assigned IP on the LAN. The following figure is an example: (Figure 3-49)





Dynamic IP DMZ

□ WAN1 : Host IP Address

□ WAN2 : Host IP Address

□ WAN3 : Host IP Address

□ WAN4 : Host IP Address

Multi-DMZ/Public DMZ

Item	DMZ Host IP Address	IP address provided by ISP	Enable	Delete	Modify
1	192.168.1.10	203.74.94.31	Enbale	□	○
2	192.168.1.11	203.74.94.32	Enbale	□	○
3	192.168.1.12	203.74.94.33	Enbale	□	○

Figure 3-49 Multi-DMZ

- **Public DMZ: Public IP Mapping**

This AirLive IGR-2500 provides “Public IP Mapping” function. With this function you can map legal IP between ROUTER WAN & LAN interface. This application will be very useful to let you connect GAME Server or VOIP gateway inside the LAN, because most GAME SERVER or VOIP gateway needs legal IP address to operation.

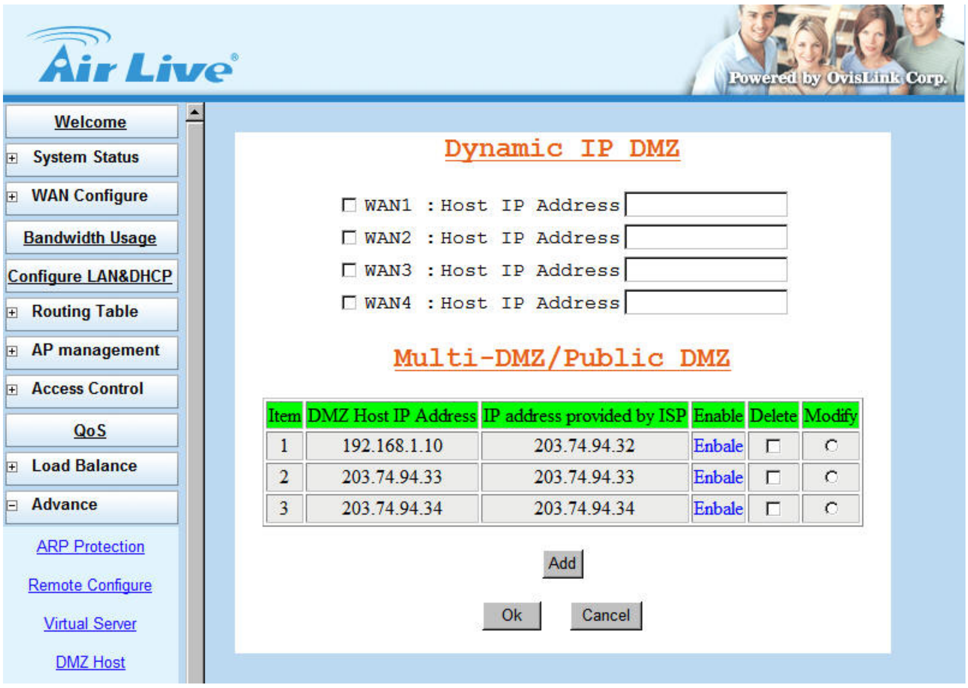
For Example:

ISP provides following legal IP address to your office. (Static IP 203.74.94.31 ~ 34)

By using DMZ function, you can configure DMZ host as follow.

DMZ Host IP Address	IP address provided by ISP	
192.168.1.10	203.74.94.32	(private DMZ host)
203.74.94.33	203.74.94.33	(for GAME SERVER)
203.74.94.34	203.74.94.34	(for VOIP gateway)

After configure IGR-2500 as above DMZ HOST table, the IGR-2500 will redirect the packets which destination address points to 203.74.94.33/34 into GAME SRVER and VOIP gateway .It also allows LAN user (ex. 192.168.1.xx) to access GAME SERVER or VOIP gateway. (Figure 3-50)



Dynamic IP DMZ

□ WAN1 : Host IP Address

□ WAN2 : Host IP Address

□ WAN3 : Host IP Address

□ WAN4 : Host IP Address

Multi-DMZ/Public DMZ

Item	DMZ Host IP Address	IP address provided by ISP	Enable	Delete	Modify
1	192.168.1.10	203.74.94.32	Enbale	□	○
2	203.74.94.33	203.74.94.33	Enbale	□	○
3	203.74.94.34	203.74.94.34	Enbale	□	○

Figure 3-50 Public DMZ

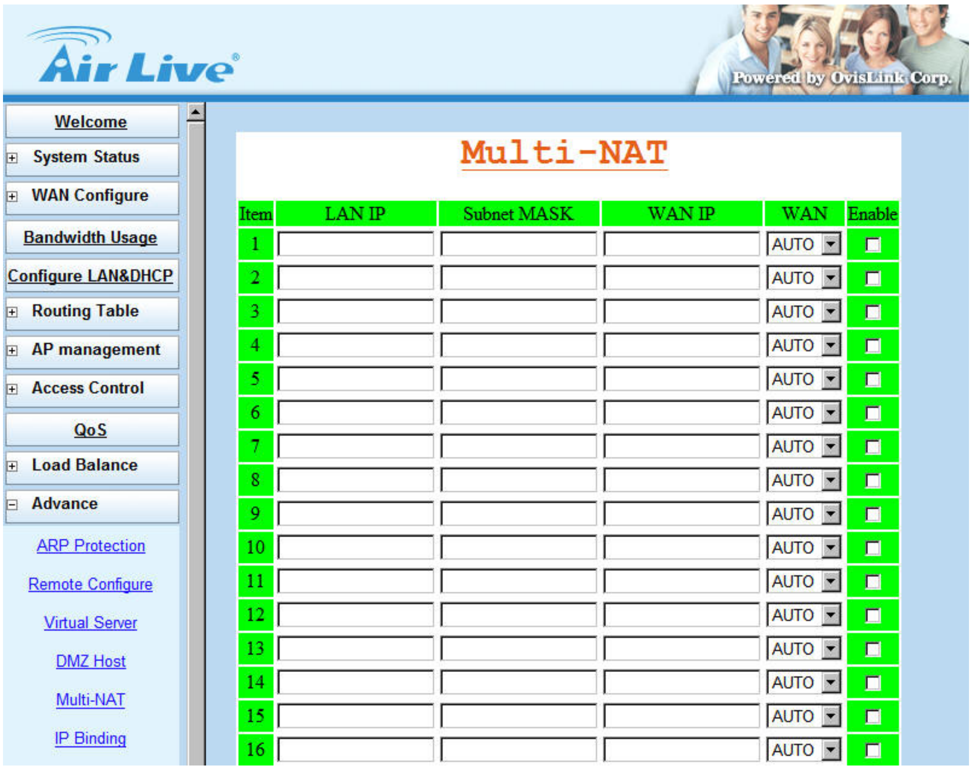
If user configures “Public IP Mapping” function, the GAME SERVER & VOIP gateway will not have DoS function protected by IGR-2500.

When hardware DMZ is enabled, the entire DMZ rule will be re-directed to the device that is connected to hardware DMZ port.

3.11.4 Multi-NAT

Multi-NAT function allows you to configure multiple LAN IP domain to each WAN port (total 10 LAN IP can be defined), after configure multiple NAT function it will act like virtual router, all traffic between each LAN IP domain will be accessed through IGR-2500. It will provide following benefit:

- Restrict broadcast storm in single IP domain.
- Check each packet with DoS function enable.



Multi-NAT

Item	LAN IP	Subnet MASK	WAN IP	WAN	Enable
1				AUTO	□
2				AUTO	□
3				AUTO	□
4				AUTO	□
5				AUTO	□
6				AUTO	□
7				AUTO	□
8				AUTO	□
9				AUTO	□
10				AUTO	□
11				AUTO	□
12				AUTO	□
13				AUTO	□
14				AUTO	□
15				AUTO	□
16				AUTO	□

Figure 3-51 Multi-NAT

- **LAN IP:** separated LAN IP domain
- **Subnet Mask:** mask for IP domain
- **WAN IP:** specific WAN IP address matched to LAN IP domain.
  - You can leave it **blank** in this field for PPPoE connection.
  - Write down specific WAN IP address, if WAN port had defined multiple IP address on it (DMZ used).
  - Blank: router will send packet follow by WAN filed selected.
- **WAN:** AUTO, WAN1, WAN2, WAN3, WAN4, WAN5
  - WAN1/2/3/4: router will route packet to correspond LAN/WAN
  - AUTO: router will route packet follow by “load balance” function selected

(Figure 3-51)

3.11.5 IP Binding

In Internet world, there have some Game Server, SSL protocol user or Personal Server have special request for connection, these special request include:

- **Use special port number to perform specific function**
- **Not allow user connect with multiple WAN IP address**

For Example, if user uses load Balance function provided by router to connect Server, Server might respond with many login requests back to user, because each session comes different WAN port with different IP address, Server treats it like different request

When user enables IP Binding function, he can specify the IP packet with dedicated WAN port to reach dedicated destination server, so it will show only 1 IP address.

That means when user wants to reach destination server, the packet will only go through dedicated WAN port, so load balance function will not be available.

- **Remote IP:** Destination server IP address. It will be restrict the access via dedicated WAN port. If you do not specify destination Host IP address in this field, the specific port number in the port number field will be limited to transfer packet via dedicated WAN port.
- **Start Port / End Port:** The protocol port number starts from 0 to 65535, you can decide the port number range to be restricted.
    - **Start Port / End Port: 0 –** all packet will be restricted to dedicated WAN port
    - **Start Port / End Port: blank –** all packet will be restricted to dedicated WAN port
    - **Start Port / End Port: 80 –** only packet type of port 80 will be restricted, the rest type packets will not be restricted, and can be spread out with Load Balance function.
    - **Start Port / End Port: 1 ~ 21 –** only packet type from port 1 to port 21 will be restricted, the rest type packets will not be restricted, and can be spread out with load balance function.
- **WAN:** select WAN port for transferring the dedicated destination packet

Example:

IP Address	***Start port***	***End Port***	***WAN***
210.3.1.23	0	65535	WAN1

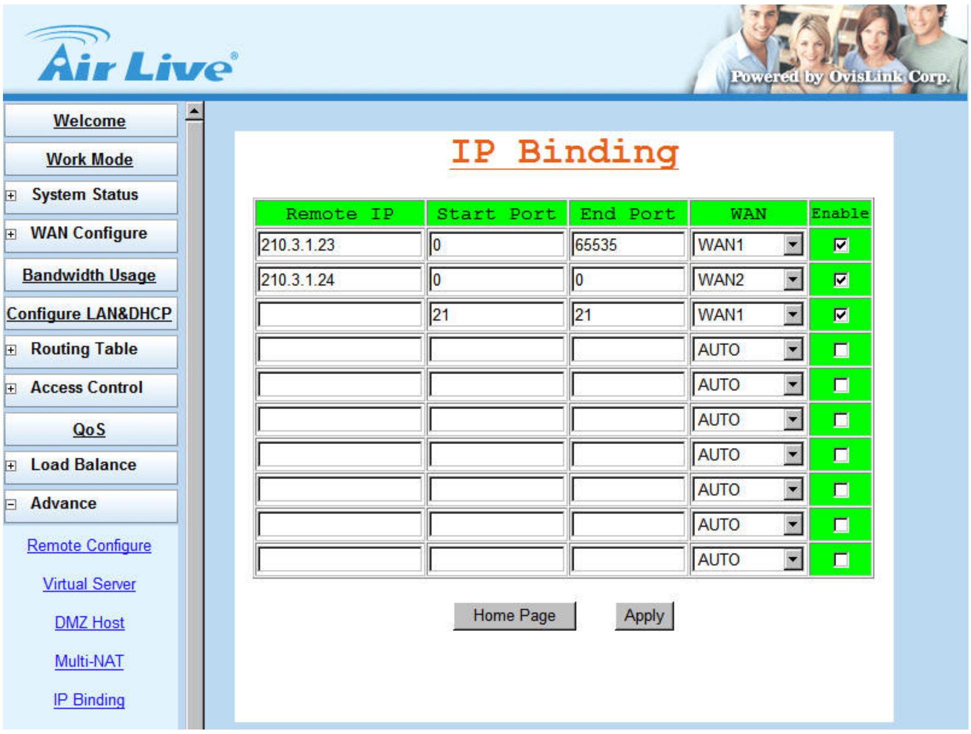
All packets go to Internet Host with IP 210.3.1.23 will be restricted to dedicated WAN 1

IP Address	***Start port***	***End Port***	***WAN***
210.3.1.24	23	23	WAN2

Packet type belong to protocol 23 that goes to Internet Host with IP 210.3.1.24 will be restricted to dedicated WAN2

IP Address	***Start port***	***End Port***	***WAN***
Blank	21	21	WAN1

Packet type belong to protocol 21 (FTP) that goes to any of Internet Host will be restricted to dedicated WAN1. (Figure 3-52)



IP Binding

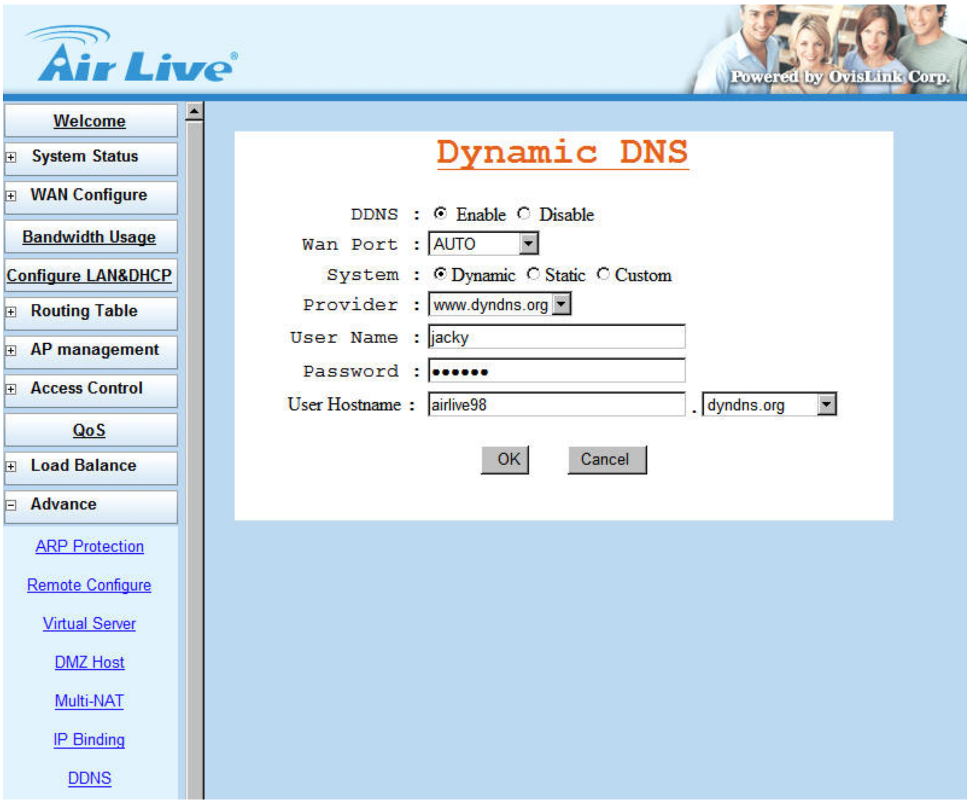
Remote IP	Start Port	End Port	WAN	Enable
210.3.1.23	0	65535	WAN1	☑
210.3.1.24	0	0	WAN2	☑
	21	21	WAN1	☑
			AUTO	□
			AUTO	□
			AUTO	□
			AUTO	□
			AUTO	□
			AUTO	□
			AUTO	□

Figure 3-52 IP Binding

3.11.6 DDNS

You need to apply for a free DNS domain name from www.dyndns.org or the other DDNS service provider, AirLive IGR-2500 will update the WAN IP address to DDNS database once the WAN port was connected to Internet if DDNS function is enabled. And the users in Internet can find out the IGR-2500 via this domain name. (Figure 3-53)

- **DDNS:** select to enable DDNS service
- **WAN Port:** select the dedicated WAN port for DDNS service
- **Provider:** select the DDNS service provider that you want to apply the DDNS service, IGR-2500 provides www.oray.net, www.88ip.com, www.dyndns.org, and www.dtdns.com DDNS service provider.
    - **System:** IGR-2500 supports to define Dyndns DDNS service as DDNS resolved Dynamic IP, DDNS resolved Static IP, or DDNS resolved Custom IP.
- **User Name:** Enter the user name applied from DDNS service provider
- **Password:** Enter the password applied from DDNS service provider
- **User Hostname:** Enter the host name applied from DDNS service provider



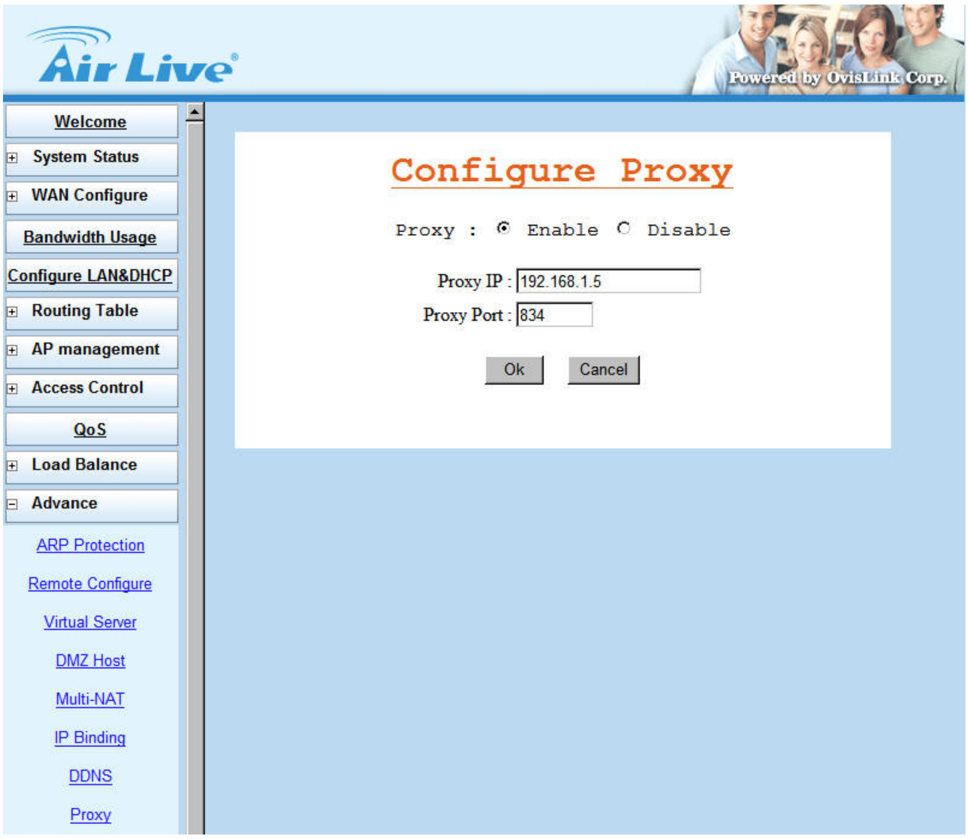
Dynamic DNS

DDNS : ● Enable ○ Disable
Wan Port : AUTO
System : ● Dynamic ○ Static ○ Custom
Provider : www.dyndns.org
User Name : jacky
Password : ••••••
User Hostname : airlive98 . dyndns.org

Figure 3-53 DDNS

3.11.7 Proxy

This function works together with **Mail Alert** function, if there have Proxy Server in your local LAN, please fill in necessary Proxy information in this display. (Figure 3-54)



Configure Proxy

Proxy : ● Enable ○ Disable

Proxy IP : 192.168.1.5

Proxy Port : 834

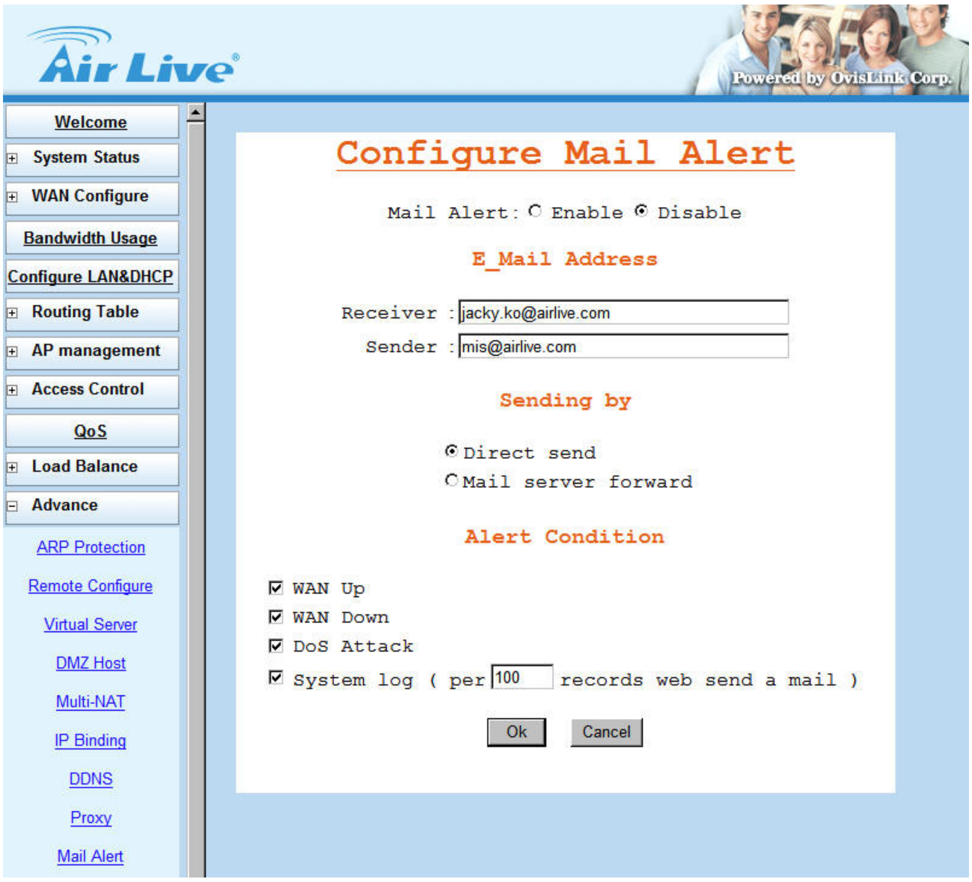
Figure 3-54 Proxy

3.11.8 Mail Alert

Enter the **Receiver/ Sender** e-mail Address in the fields and check the items you want. System will send e-mails to **Receiver** address once the conditions meets the setting. (Figure 3-55)

- **Receiver mail address:** The mail address that will receive alert mail
- **Sender mail address:** The mail address that send out alert mail, you should fill in a legal format address
- **Alert Condition:** IGR-2500 provides four condition selections:

WAN Up	System will send the mail, once WAN port(s) is connected to Internet.
WAN Down	System will send the mail, once WAN port(s) is disconnected from Internet.
DoS Attack	System will send the mail, once the selected conditions in DoS occurred. (need to enable DoS function)
System log	System will send the mail of log information, once the log records conform to your setting.



Configure Mail Alert

Mail Alert: ○ Enable ● Disable

E_Mail Address

Receiver : jacky.ko@airlive.com

Sender : mis@airlive.com

Sending by

● Direct send

○ Mail server forward

Alert Condition

☑ WAN Up

☑ WAN Down

☑ DoS Attack

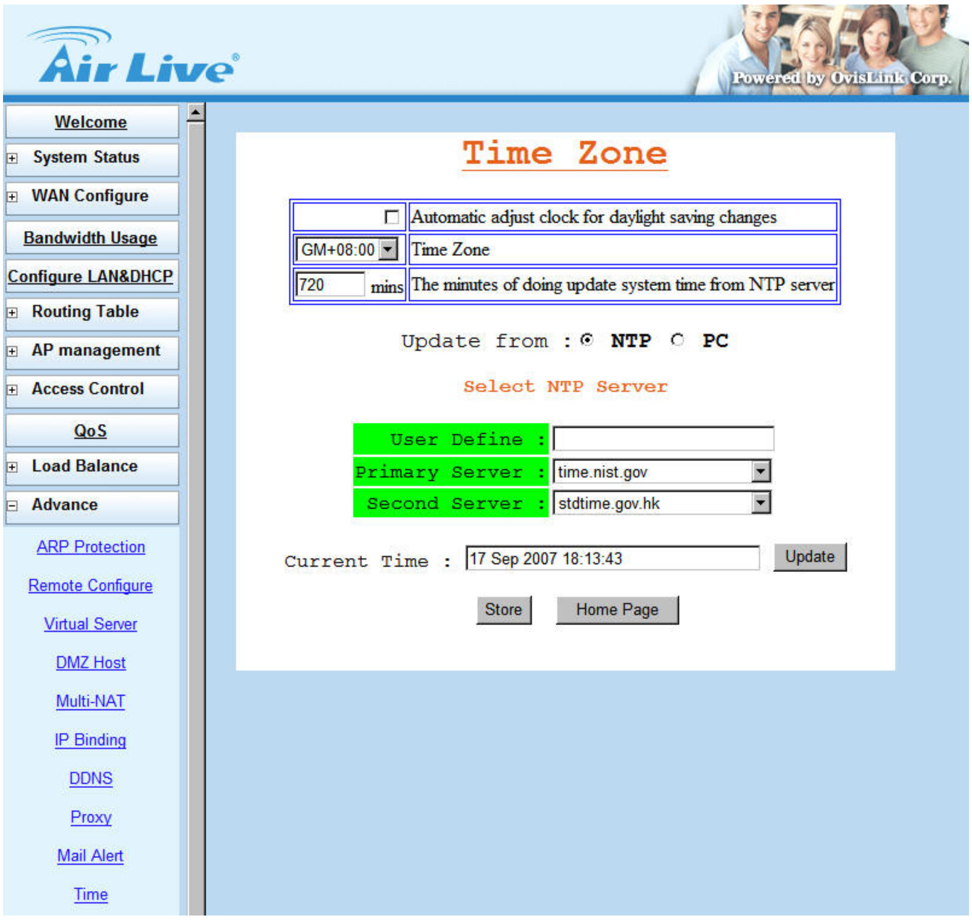
☑ System log (per 100 records web send a mail)

Figure 3-55 Mail Alert

3.11.9 Time

AirLive IGR-2500 will obtain the GMT (Greenwich Mean Time) after connected to Internet. You need to indicate the local time so that the system could operate with the correct time. For example, Taiwan's local time is GMT + 8 hours.

Select "Automatic adjust clock for daylight saving changes" will display the time one hour earlier than local time. (Figure 3-56)



Time Zone

□	Automatic adjust clock for daylight saving changes
GM+08:00	Time Zone
720 mins	The minutes of doing update system time from NTP server

Update from : ● NTP ○ PC

Select NTP Server

User Define :

Primary Server : time.nist.gov

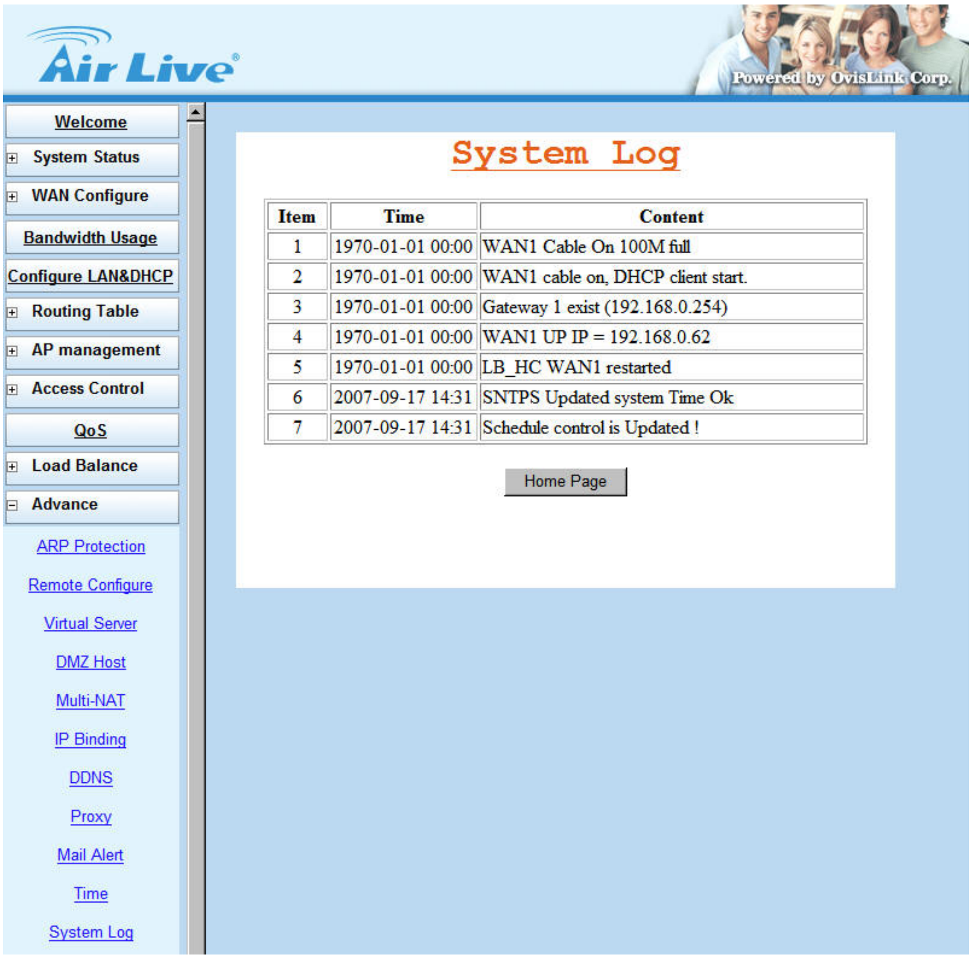
Second Server : stdtime.gov.hk

Current Time : 17 Sep 2007 18:13:43

Figure 3-56 Time

3.11.10 System Log

Show all the records after IGR-2500 Power on, such as WAN port up/down, WAN IP address, the obtained time, DDNS current corresponding WAN IP address and so forth. You can also save these data to files. (Figure 3-57)



System Log

Item	Time	Content
1	1970-01-01 00:00	WAN1 Cable On 100M full
2	1970-01-01 00:00	WAN1 cable on, DHCP client start.
3	1970-01-01 00:00	Gateway 1 exist (192.168.0.254)
4	1970-01-01 00:00	WAN1 UP IP = 192.168.0.62
5	1970-01-01 00:00	LB_HC WAN1 restarted
6	2007-09-17 14:31	SNTPS Updated system Time Ok
7	2007-09-17 14:31	Schedule control is Updated !

Figure 3-57 System Log

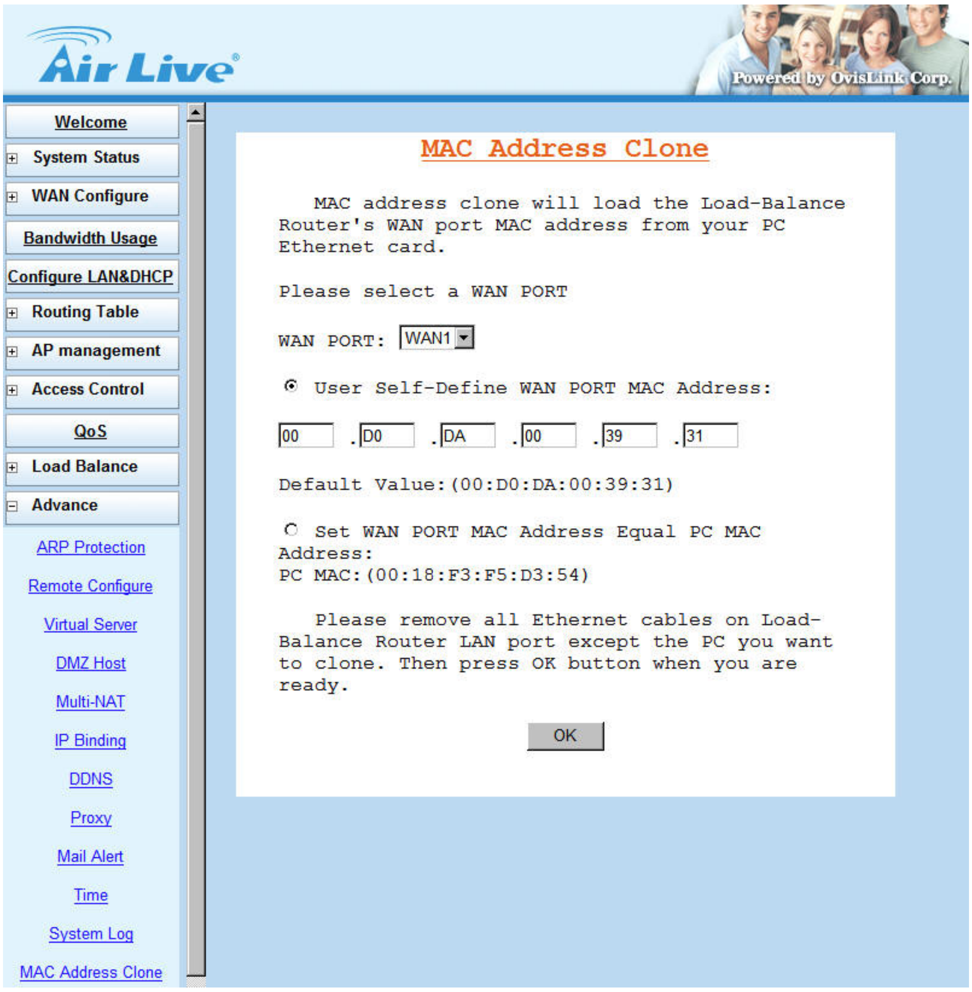
3.11.11 MAC Address Clone

If your ISP blocked the MAC address of a network card, you may use MAC Address Clone to duplicate the MAC address to the Mac address in each WAN port.

Remove all Ethernet cable on IGR-2500 LAN port except for the PC you want to clone. Then press **Ok** when you ready. (Figure 3-58)

- **User Self-Define WAN Port MAC Address:** type in a MAC Address to define WAN MAC Address.
- **Set WAN Port MAC Address Equal PC MAC Address:** select to clone WAN MAC Address from LAN PC MAC Address.

You need to **reboot** IGR-2500 after finished cloning to make new MAC address takes effects.



MAC Address Clone

MAC address clone will load the Load-Balance Router's WAN port MAC address from your PC Ethernet card.

Please select a WAN PORT

WAN PORT: WAN1

● User Self-Define WAN PORT MAC Address:

00 . D0 . DA . 00 . 39 . 31

Default Value:(00:D0:DA:00:39:31)

○ Set WAN PORT MAC Address Equal PC MAC Address:
PC MAC:(00:18:F3:F5:D3:54)

Please remove all Ethernet cables on Load-Balance Router LAN port except the PC you want to clone. Then press OK button when you are ready.

OK

Figure 3-58 MAC Address Clone

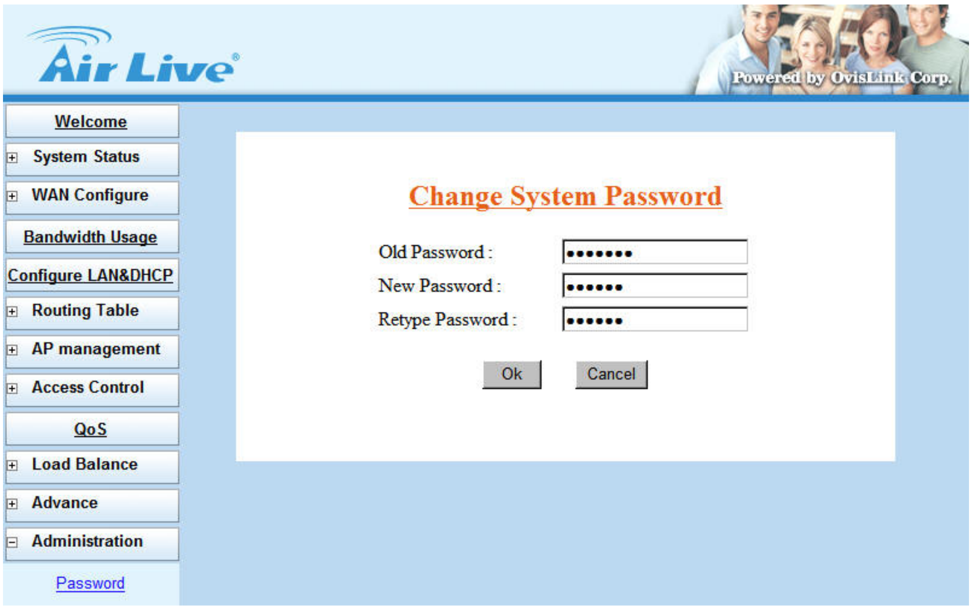
3.12 Administrator

3.12.1 Password

Use this function to change the **Password** that is used for access the web configuration. Type in the **Old Password, New Password** and **Retype Password** in their respective fields and then click **Ok**, the password will be changed to new one after re-boot. (Figure 3-59)

Password length can be up to 30 alphanumeric characters with case sensitive.

WE SUGGESTED YOU TO CHANGE ROUTER PASSWORD AND KEEP IT IN SAFETY PLACE AFTER YOU RECEIVED ROUTER AND FINISH ALL ROUTER PARAMETER SETTING.



Change System Password

Old Password : •••••••

New Password : ••••••

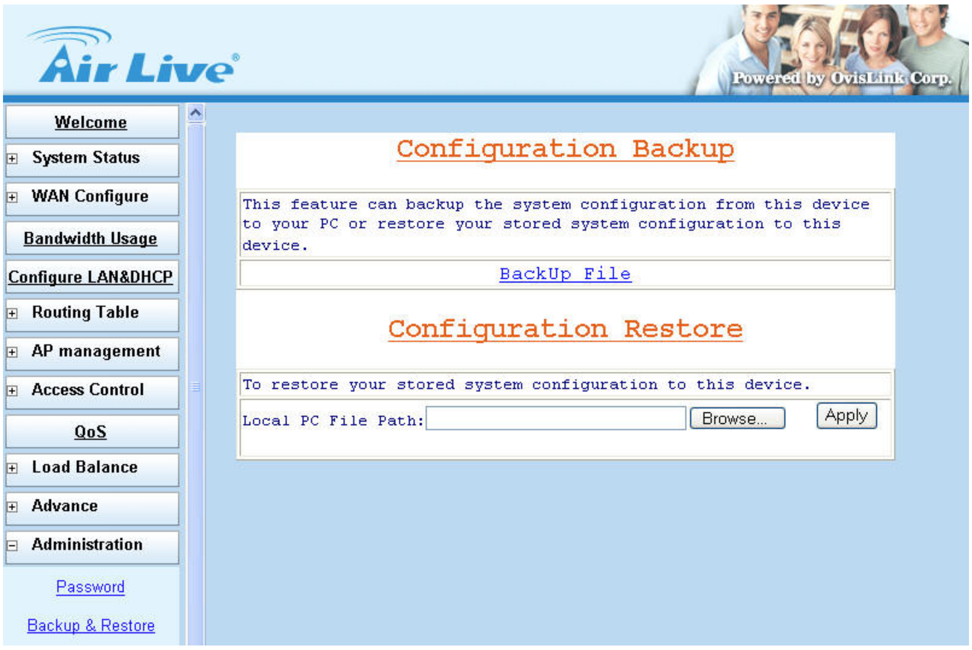
Retype Password : ••••••

Ok Cancel

Figure 3-59 Change Password

3.12.2 Backup & Restore

Use **Backup & Restore** function to save all the settings parameters to PC for safety issue, in order to avoid all parameter lose when system crushes. (Figure 3-60)



Configuration Backup

This feature can backup the system configuration from this device to your PC or restore your stored system configuration to this device.

BackUp File

Configuration Restore

To restore your stored system configuration to this device.

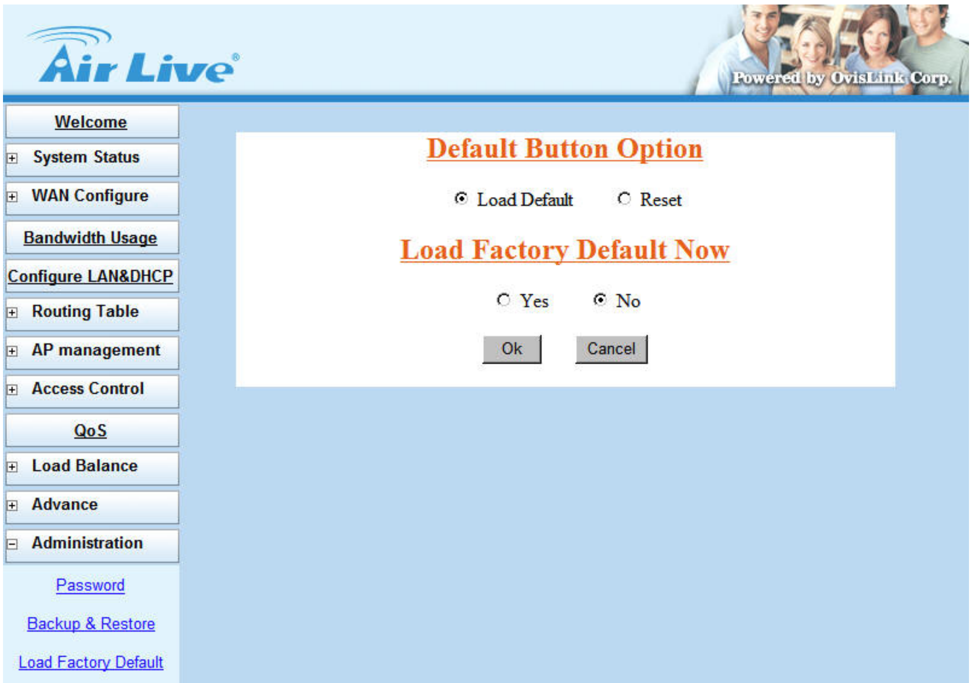
Local PC File Path: Browse... Apply

Figure 3-60 Backup & Restore

3.12.3 Load Factory Default

User can use this function to define the feature of reset button, or load the latest configuration file back to device. Click OK after the selection, the IGR-2500 will restart automatically. (Figure 3-61)

- ■ **Reset Button Option:** This option is used to define Default button on the back penal of the router.
  - ◆ **Load Default:** press Reset button, the factory default configuration will be loaded.
  - ◆ **Reset:** press Reset button, IGR-2500 will reboot and load the latest configuration.
- ■ **Load Factory Default:** Tick “**Yes**” option then click “**Ok**”, you can load the factory default value immediately. If you only want to submit new setting for Default Button Option without load the factory default, tick the “**No**” option before click Ok.



Default Button Option

● Load Default ○ Reset

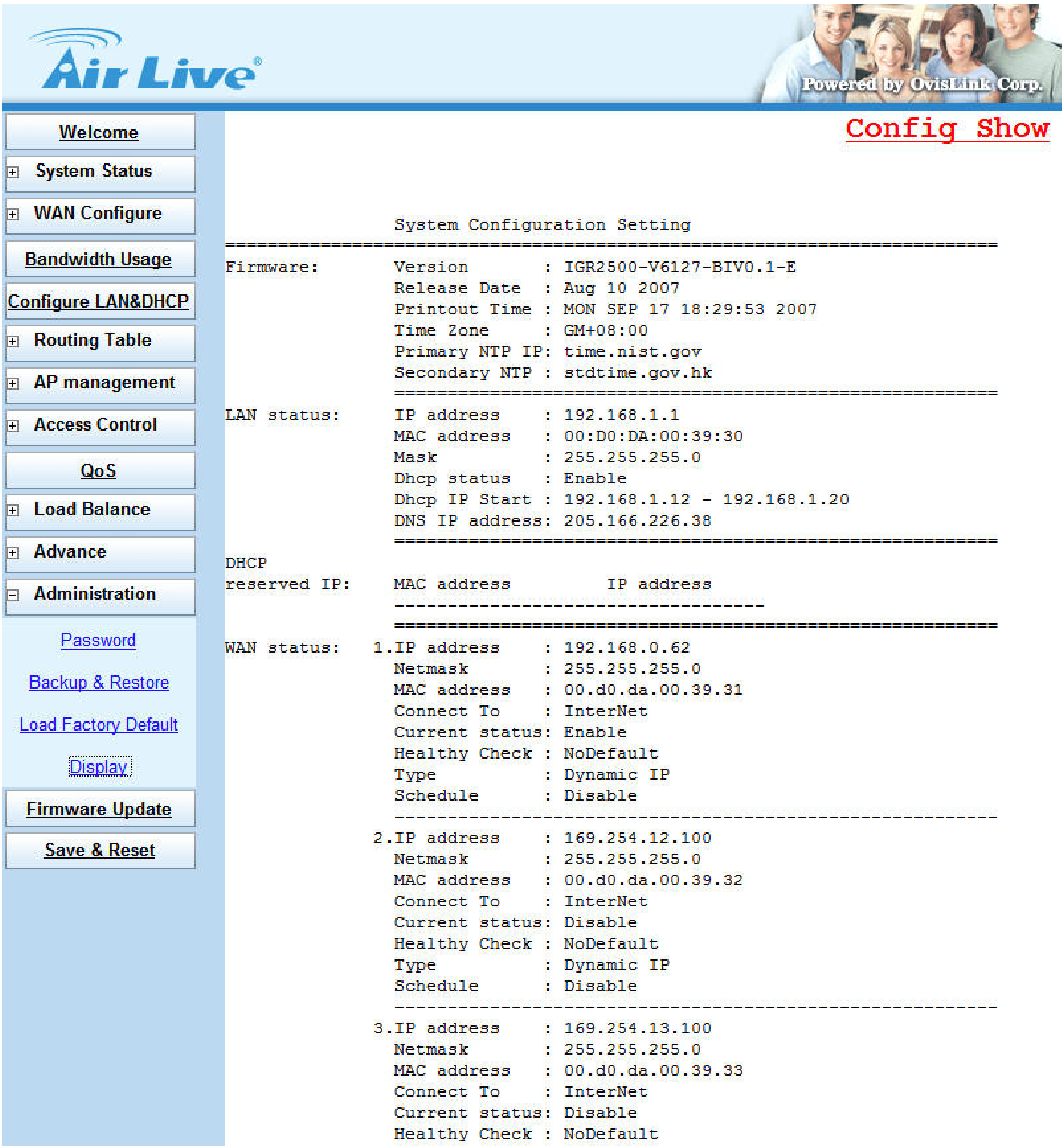
Load Factory Default Now

○ Yes ● No

Figure 3-61 Load Factory Default

3.12.4 Display

You can use this function to check all the parameter setting in this router, in order to save time to check every display. (Figure 3-62)



```
                System Configuration Setting
==========================================================================
Firmware:       Version        : IGR2500-V6127-BIV0.1-E
                Release Date   : Aug 10 2007
                Printout Time  : MON SEP 17 18:29:53 2007
                Time Zone      : GM+08:00
                Primary NTP IP: time.nist.gov
                Secondary NTP  : stdtime.gov.hk
                ==========================================================
LAN status:     IP address     : 192.168.1.1
                MAC address    : 00:D0:DA:00:39:30
                Mask           : 255.255.255.0
                Dhcp status    : Enable
                Dhcp IP Start  : 192.168.1.12 - 192.168.1.20
                DNS IP address: 205.166.226.38
                ==========================================================
DHCP
reserved IP:    MAC address          IP address
                -----------------------------------
                ==========================================================
WAN status:   1.IP address     : 192.168.0.62
                Netmask        : 255.255.255.0
                MAC address    : 00.d0.da.00.39.31
                Connect To     : InterNet
                Current status: Enable
                Healthy Check  : NoDefault
                Type           : Dynamic IP
                Schedule       : Disable
                ----------------------------------------------------------
              2.IP address     : 169.254.12.100
                Netmask        : 255.255.255.0
                MAC address    : 00.d0.da.00.39.32
                Connect To     : InterNet
                Current status: Disable
                Healthy Check  : NoDefault
                Type           : Dynamic IP
                Schedule       : Disable
                ----------------------------------------------------------
              3.IP address     : 169.254.13.100
                Netmask        : 255.255.255.0
                MAC address    : 00.d0.da.00.39.33
                Connect To     : InterNet
                Current status: Disable
                Healthy Check  : NoDefault
```

Figure 3-62 Display

3.13 Firmware Upgrade

AirLive IGR-2500 allows you to easily update the embedded firmware.

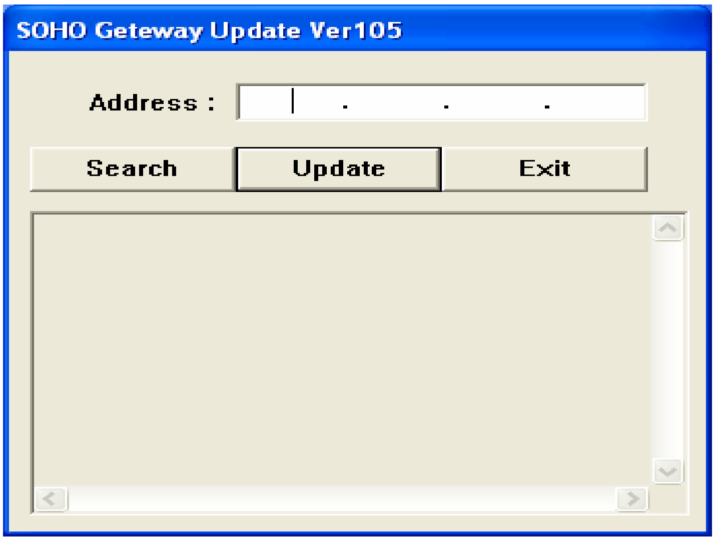
We will occasionally provide new firmware on the web site to help you updating the firmware of your IGR-2500.

Follow the procedure to update your firmware after downloaded the new code.

Method 1:

Double click the executable file (the file with exe extension file name) you downloaded. Here we take **v105.exe** as the example of new version file.

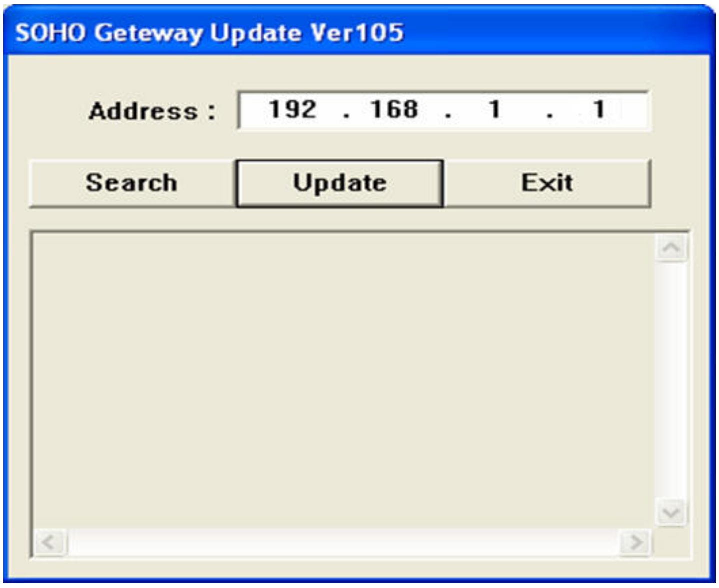
Step 1: Click **Search** to find the IP of router.



SOHO Geteway Update Ver105

Address : . . .

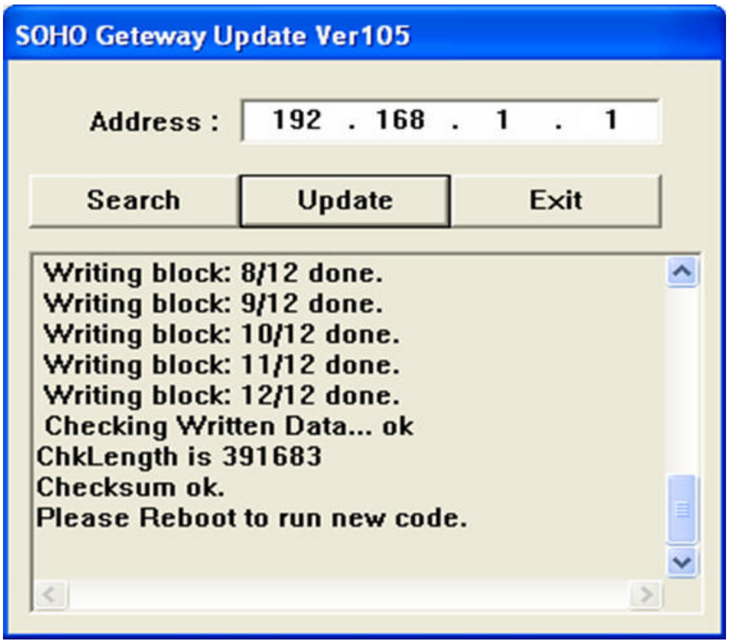
Step 2: The IP address of IGR-2500 is **192.168.1.1 (default value)**.



SOHO Geteway Update Ver105

Address : 192 . 168 . 1 . 1

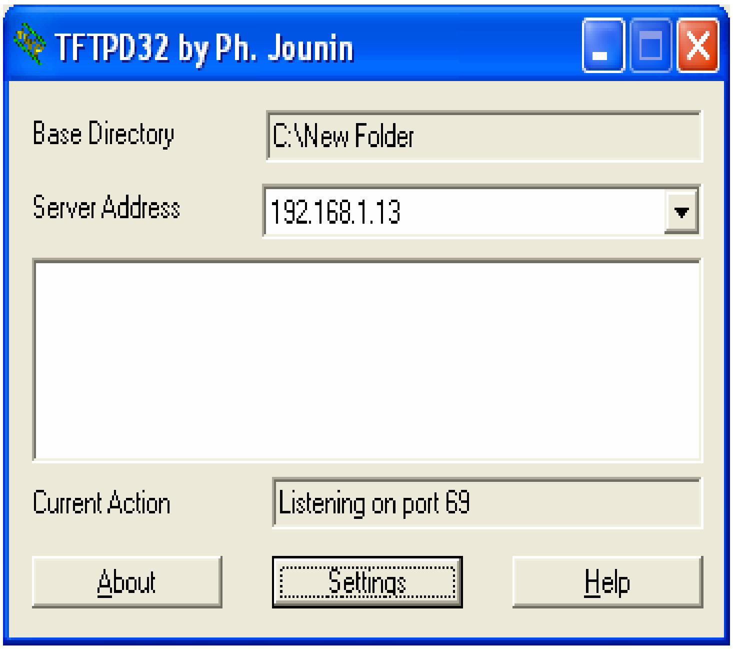
Step 3: Click **Update** to update the firmware.



```
Writing block: 8/12 done.
Writing block: 9/12 done.
Writing block: 10/12 done.
Writing block: 11/12 done.
Writing block: 12/12 done.
Checking Written Data... ok
ChkLength is 391683
Checksum ok.
Please Reboot to run new code.
```

Method 2:

Step 1: Run a TFTP server program such as TFTPD32. (TFTPD32 is a shareware and you may download it or other TFTP server programs from Internet.)

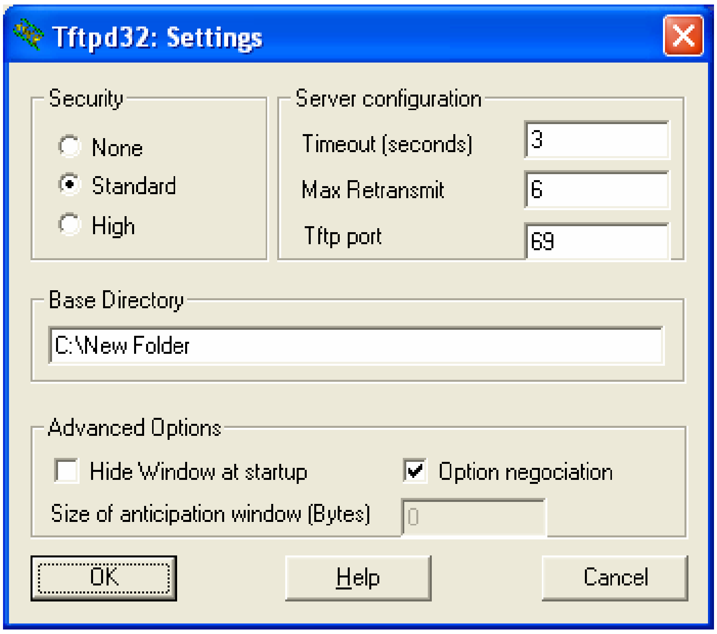


Base Directory: C:\New Folder

Server Address: 192.168.1.13

Current Action: Listening on port 69

Step2: Make a base directory in this server



Tftpd32: Settings

Security

○ None

● Standard

○ High

Server configuration

Timeout (seconds)	3
Max Retransmit	6
Tftp port	69

Base Directory

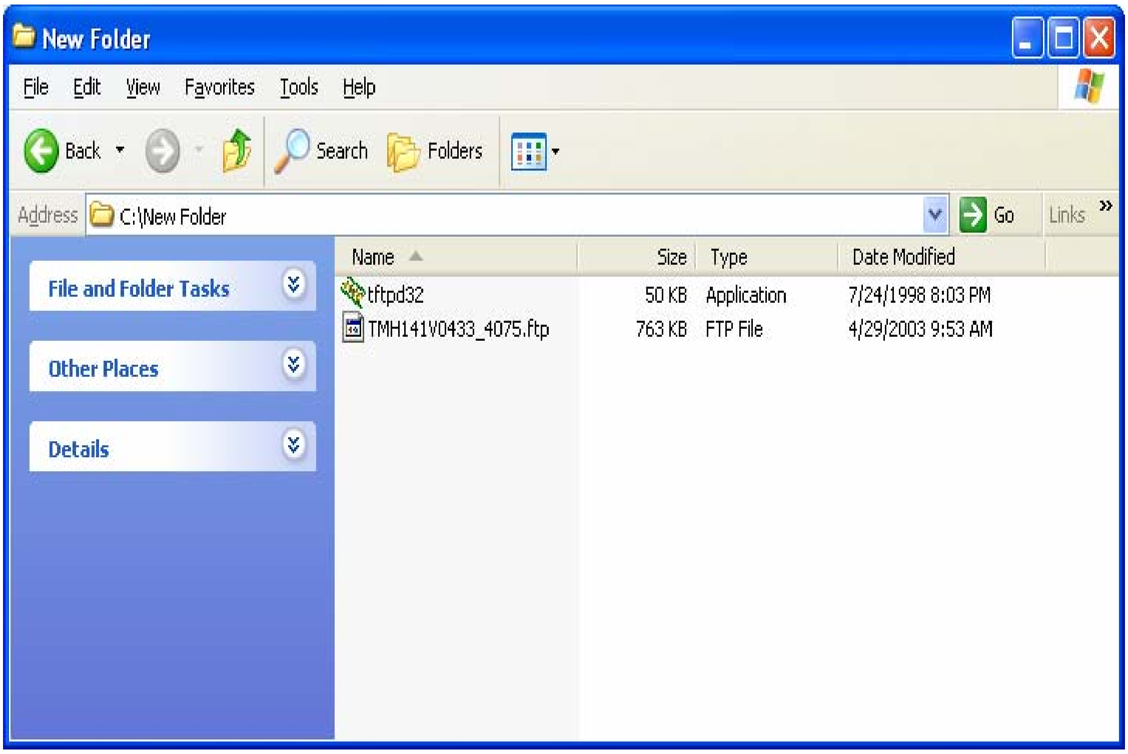
C:\New Folder

Advanced Options

□ Hide Window at startup ☑ Option negociation

Size of anticipation window (Bytes) 0

Step 3: Save the image file of firmware to the directory of TFTPD32

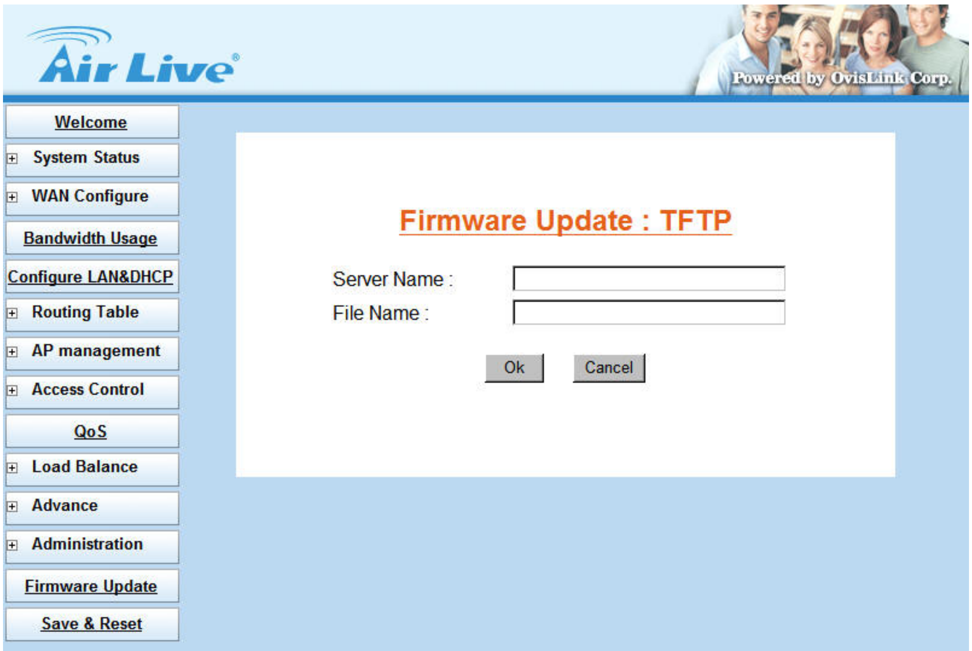


New Folder

Address C:\New Folder

Name	Size	Type	Date Modified
tftpd32	50 KB	Application	7/24/1998 8:03 PM
TMH141V0433_4075.ftp	763 KB	FTP File	4/29/2003 9:53 AM

Step 4: Enter the **Server Name** and **File Name** in the new folder fields of **Firmware Update** window and then click **Ok**.



Firmware Update : TFTP

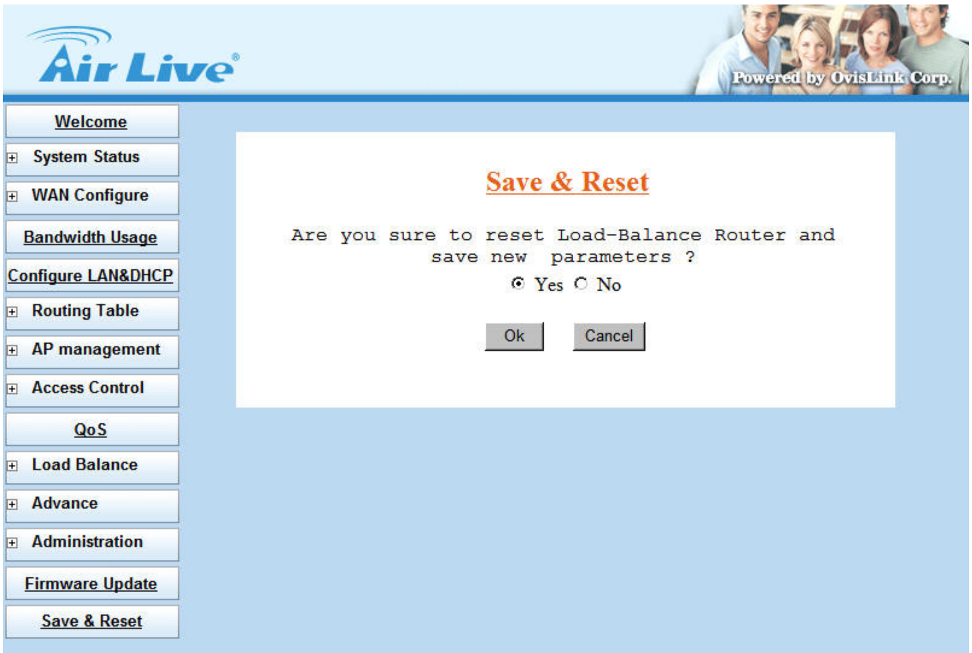
Server Name :

File Name :

Step 5: You will see the updating processing. After finishing update procedure, you must **reboot** IGR-2500 to run new code.

3.14 Save & Reset

In order to save the configuration changes that have been made to the IGR-2500, you must save them to the IGR-2500's Flash memory. If you do not save the changes, the configuration settings will be lost in the event of a power loss or system reboot to the IGR-2500. (Figure 3-63)



Save & Reset

Are you sure to reset Load-Balance Router and save new parameters ?

● Yes ○ No

Figure 3-63 Load Factory Default

Appendix A In-Bound Load Balance Function

Authorities DNS is just a fancy term for the official IP address keeper/provider of particular Domain (or Internet) name, such as www.example.com is analogous to a telephone book where a person's name is associated with his telephone number. Wikipedia, the free encyclopedia has a good general discussion of DNS: http://en.wikipedia.org/wiki/Domain_Name_System.

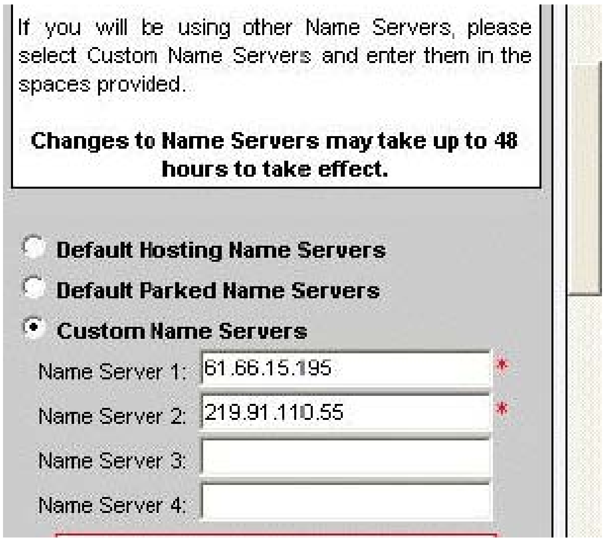
This IN-BOUND ROUTER DNS server contains the names and Internet addresses of servers that you wish to host. In order for all DNS requests of your domain names to be ultimately routed to your IN-BOUND ROUTER, it has to be setup at the registrar of your Internet name. In general, logon to your registrar site, and manage your domain name. For example, www.example.com is located at a WEB hosting company, and the original Domain server was registered in listed order:

NS0.DNSMADEEASY.COM NS1.DNSMADEEASY.COM NS2.DNSMADEEASY.COM
NS3.DNSMADEEASY.COM NS4.DNSMADEEASY.COM

We need to change www.example.com to be hosted by IN-BOUND ROUTER; so we follow the registrar's instructions and delete: NS2, NS3, and NS4, and assign Domain server:

Name	IP address
NS0.EXAMPLE.COM	WAN1
NS1.EXAMPLE.COM	WAN2

The name is arbitrary; the most important are about the IP addresses. It is absolutely necessary for WAN1 to be a static address, and for redundant, fault-tolerant accesses, WAN2 should also be a static address. It would take approximately 24 – 48 hours for this change to take effect throughout the Internet. Below is the actual display of godaddy for Name Servers:



If you will be using other Name Servers, please select Custom Name Servers and enter them in the spaces provided.

Changes to Name Servers may take up to 48 hours to take effect.

○ **Default Hosting Name Servers**

○ **Default Parked Name Servers**

● **Custom Name Servers**

Name Server 1: 61.66.15.195 *

Name Server 2: 219.91.110.55 *

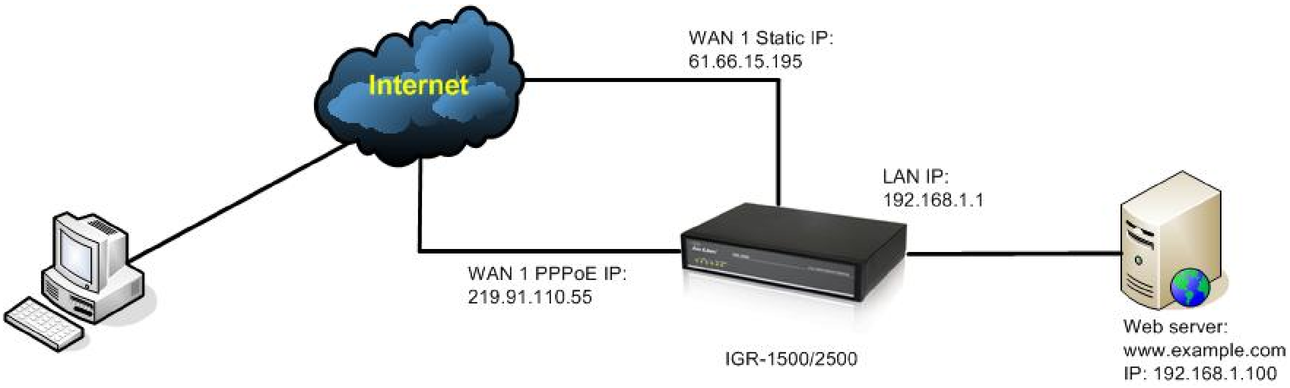
Name Server 3:

Name Server 4:

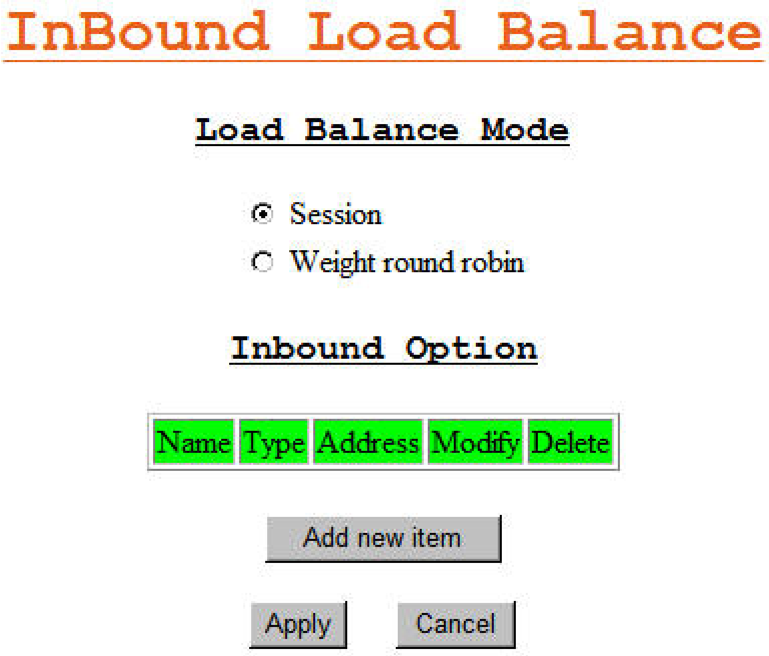
All registrars have the same basic name server facility. For www.example.com, we use godaddy.com, and the process is: Login Manage domain Set Name Servers. We enter WAN1 and WAN2 for Custom Name Servers.

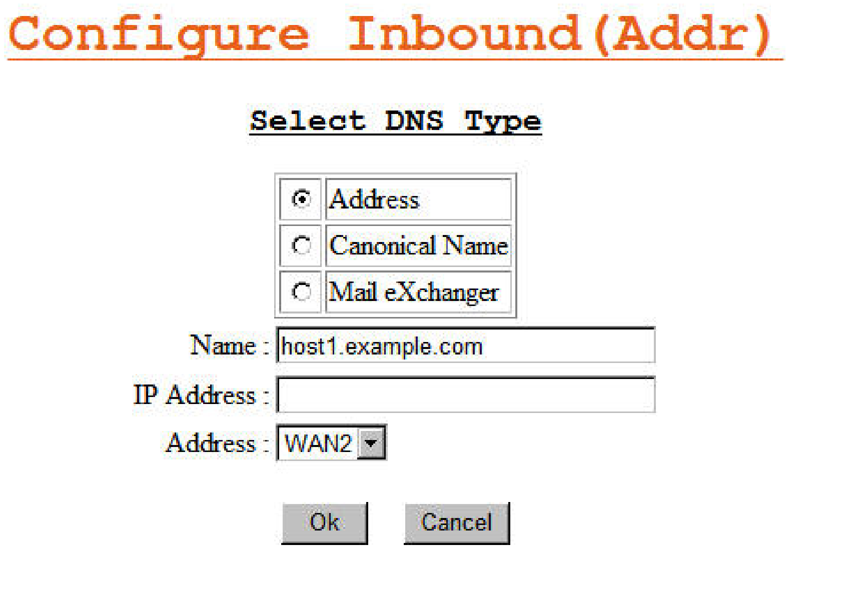
A.1 Simple Load Balance (2 WAN lines; Session 1:1)

Let us assume that the upload speed of WAN1 and WAN2 are the same; so we will use inbound load-balancing setting: Session with a load-balancing ratio of 1:1.



In the IN-BOUND ROUTER configuration **Load Balance → Inbound**:

 InBound Load Balance Load Balance Mode ● Session ○ Weight round robin Inbound Option Name Type Address Modify Delete Add new item Apply Cancel	**Step 1:** Click on **Add new item**



Configure Inbound(Addr)

Select DNS Type

● Address
○ Canonical Name
○ Mail eXchanger

Name : host1.example.com

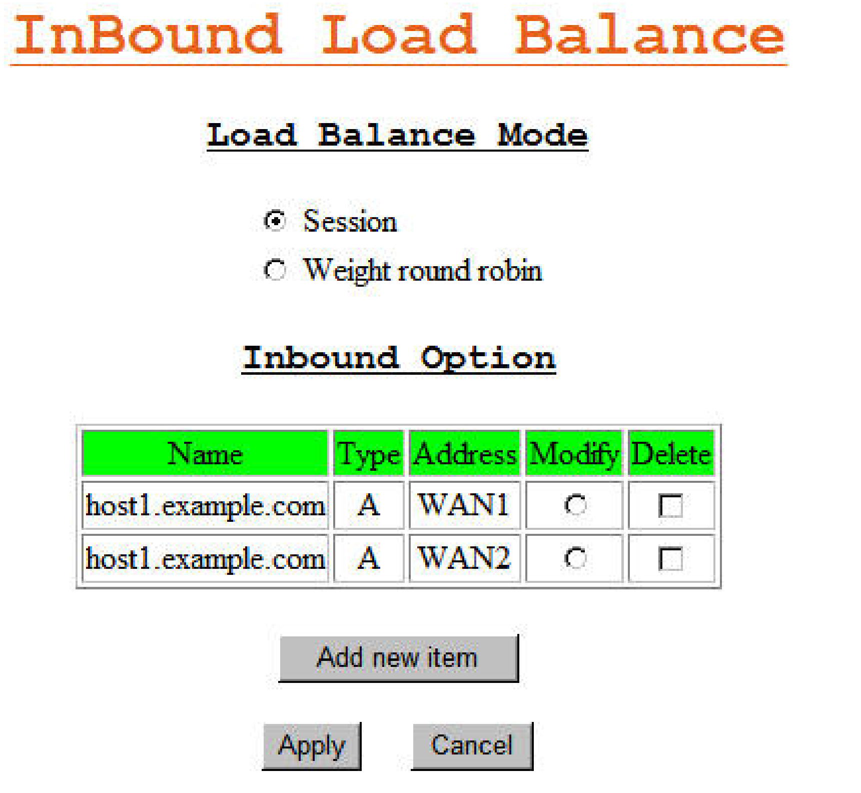
IP Address :

Address : WAN2

Step 2:

Enter host1.example.com two times, once for WAN1 and once for WAN2 with **Address** Type. This display show the 1st time for WAN1, after clicking **Ok**. Repeat the previous configuration with the same name for WAN2 at this time.

You don’t need to explicitly enter any IP address.



InBound Load Balance

Load Balance Mode

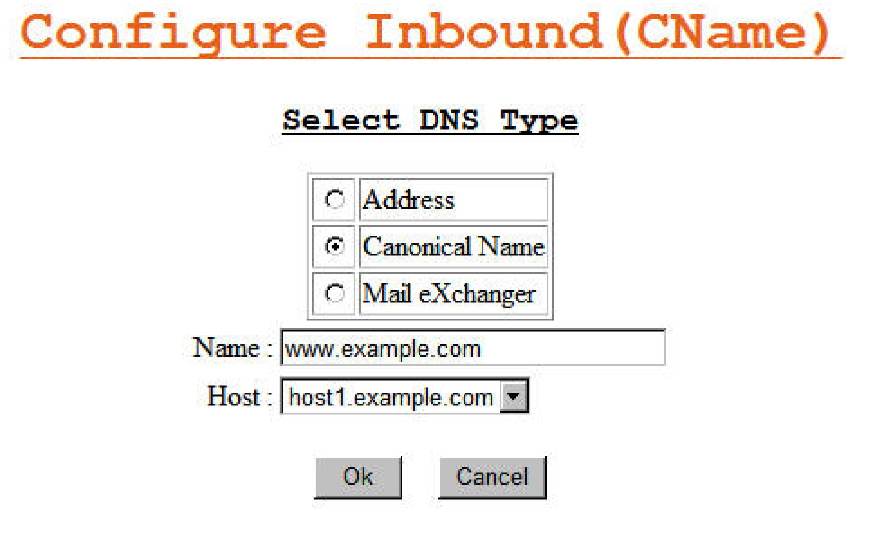
● Session
○ Weight round robin

Inbound Option

Name	Type	Address	Modify	Delete
host1.example.com	A	WAN1	○	□
host1.example.com	A	WAN2	○	□

Step 3:

Now, we have 2 entries in the DNS table. Click on **Add new item** again.



Configure Inbound(CName)

Select DNS Type

○ Address
● Canonical Name
○ Mail eXchanger

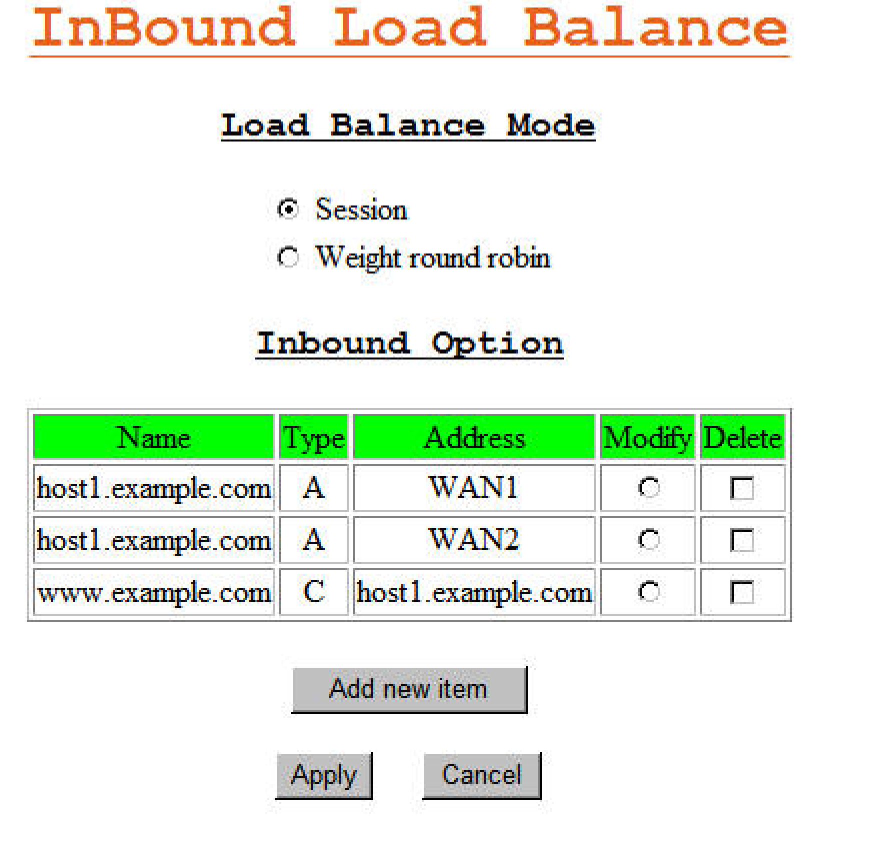
Name : www.example.com
Host : host1.example.com

Step 4:

This time we are adding the DNS record with the real name for web server.

Select DNS Type with **Canonical Name**.

Name: www.example.com
Host: host1.example.com



InBound Load Balance

Load Balance Mode

● Session
○ Weight round robin

Inbound Option

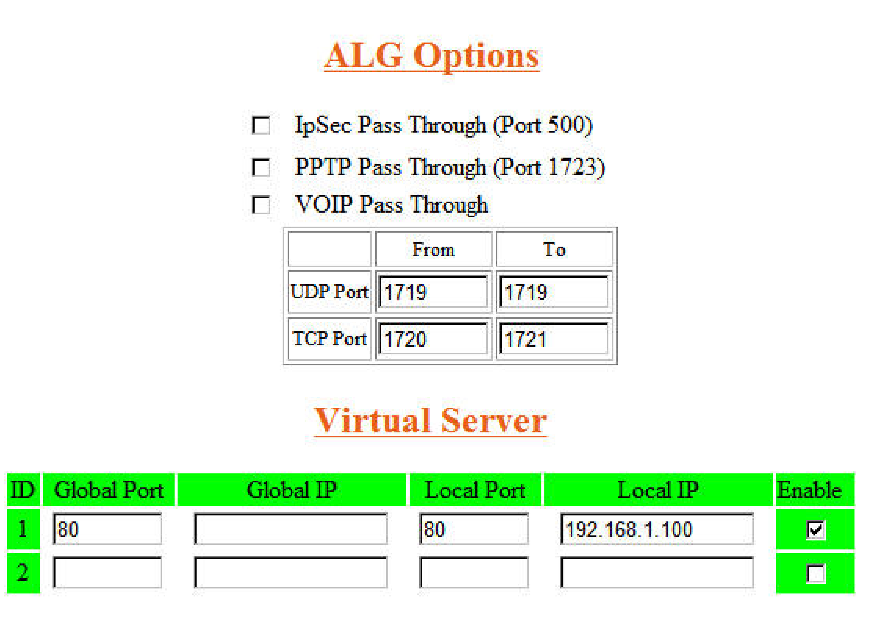
Name	Type	Address	Modify	Delete
host1.example.com	A	WAN1	○	□
host1.example.com	A	WAN2	○	□
www.example.com	C	host1.example.com	○	□

Step 5:

The simplest case for the configuration of IN-BOUND ROUTER DNS server is done.

Now the Inbound Load-balancing DNS Server is configured to redirect the Internet requests of www.example.com to the IP address of either WAN1 or WAN2. But we'll still need to configure the virtual server.

In the IN-BOUND ROUTER configuration: **Advance → Virtual Server**



ALG Options

☐ IpSec Pass Through (Port 500)

☐ PPTP Pass Through (Port 1723)

☐ VOIP Pass Through

	From	To
UDP Port	1719	1719
TCP Port	1720	1721

Virtual Server

ID	Global Port	Global IP	Local Port	Local IP	Enable
1	80		80	192.168.1.100	☑
2					☐

Step 1:

The port for www.example.com is 80 and the IP address is: 192.168.1.100.

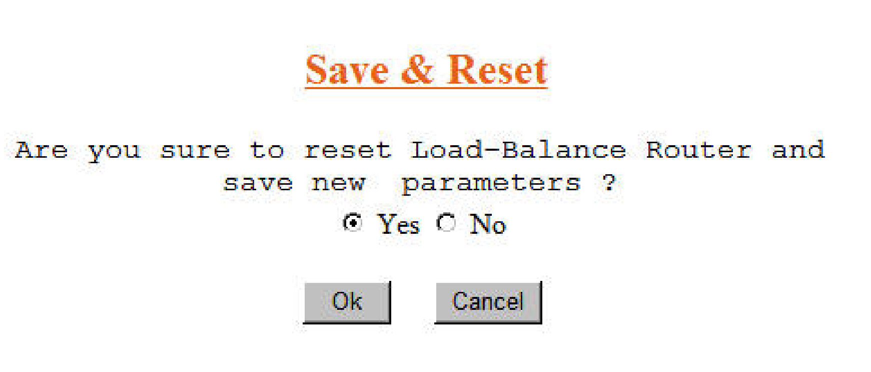
Enter:

Global Port: 80

Local Port: 80

Local IP: 192.168.1.100

Select **Enable**, and then click **APPLY**.



Save & Reset

Are you sure to reset Load-Balance Router and save new parameters ?

● Yes ○ No

Step 2:

In order for the Inbound Load Balancing to take effect, we will need to do a system reboot.

Select **Yes** and click on **Ok.**

After the reset sequence is finished, the configured for Inbound Load Balancing is completed.

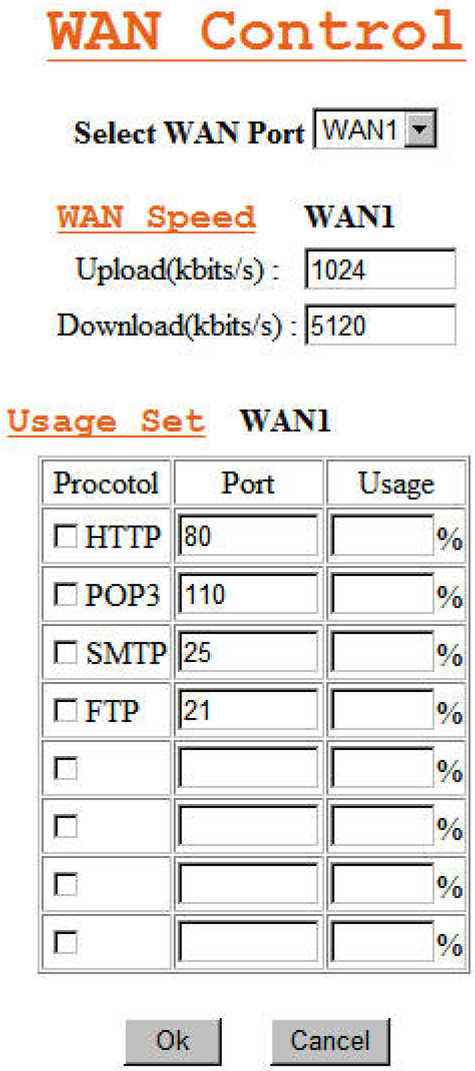
A.2 Advanced Load Balancing

We will describe Inbound Load Balancing using “Weighted round robin” algorithm for three Internet servers:

1. Web server, www.example.com, using WAN1 – WAN2, with ratio of 1:2
2. FTP server, ftp.example.com, using WAN1 –WAN4, with ration of 1:2:3:4
3. Mail server, mail.example.com, using WAN3 & WAN4, with ratio of 3:4

The ratio of 1:2 means that every return of IP address from WAN1, there will be two returned IP addresses from WAN2 for the DNS request.

For the Load Balancing “Weighted round robin” algorithm, you should specify the data rate of each individual WAN ports.



WAN Control

Select WAN Port WAN1

WAN Speed WAN1

Upload(kbits/s) : 1024

Download(kbits/s) : 5120

Usage Set WAN1

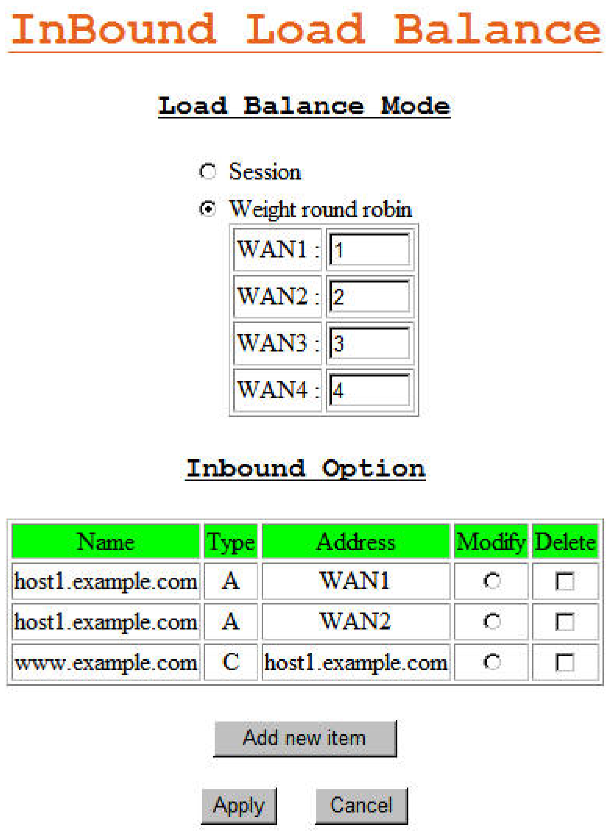
Procotol	Port	Usage
□ HTTP	80	%
□ POP3	110	%
□ SMTP	25	%
□ FTP	21	%
□		%
□		%
□		%
□		%

■ **Define the WAN speed**

■

In **Bandwidth Usage** page, select the WAN port and enter the specific **Download** and **Upload** bandwidth. The bandwidth must be the correct value provided by ISP, or the load balance function might not work properly.

Do the same configuration for the other WAN ports.



InBound Load Balance

Load Balance Mode

○ Session

● Weight round robin

WAN1 :	1
WAN2 :	2
WAN3 :	3
WAN4 :	4

Inbound Option

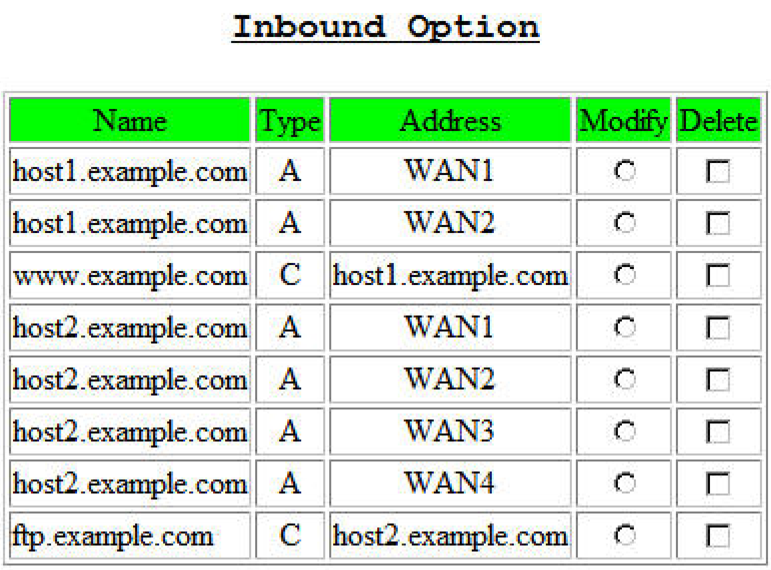
Name	Type	Address	Modify	Delete
host1.example.com	A	WAN1	○	□
host1.example.com	A	WAN2	○	□
www.example.com	C	host1.example.com	○	□

■ **Define www.example.com in Inbound Option**

In **Load Balance → Inbound**, select **Weight round robin** for the inbound load balance mode.

Now you can enter the ratio for each WAN port into their respective fields.

Add the appropriate entries into the Inbound Option table. The entries are similar to the entries for www.example.com in previous section A.1. We will use host2 for ftp.example.com, and here are the results so far.



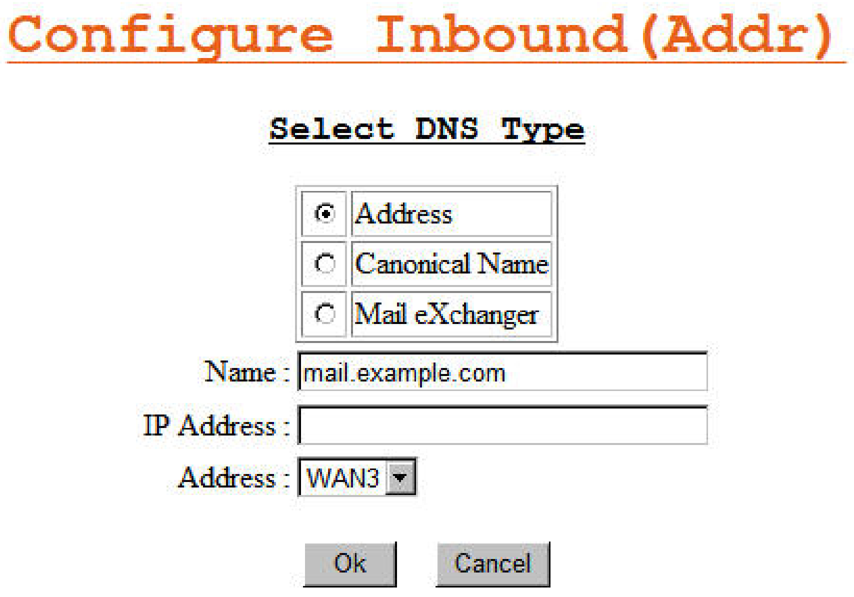
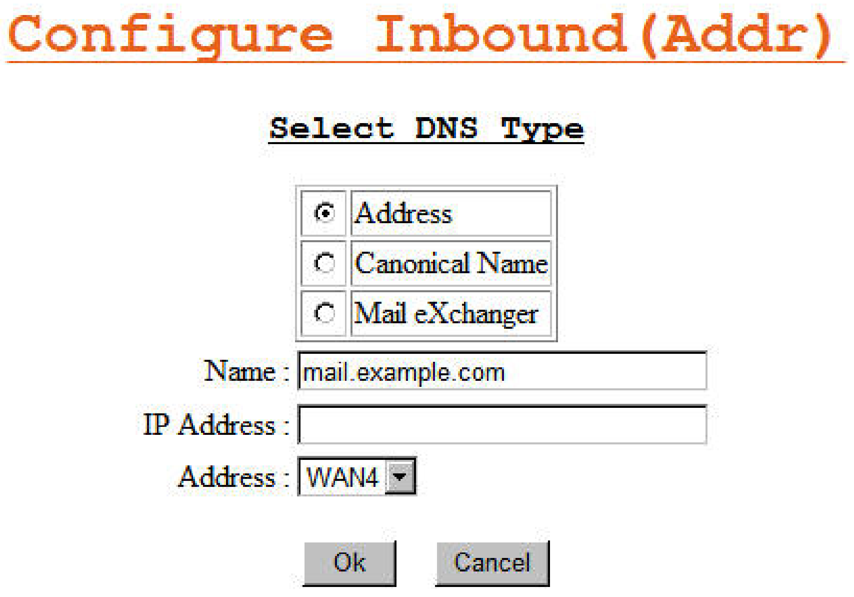
Inbound Option

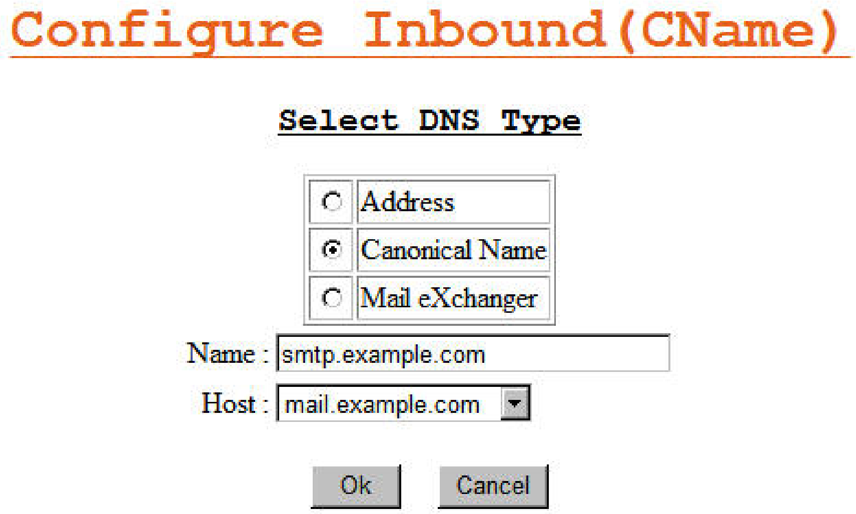
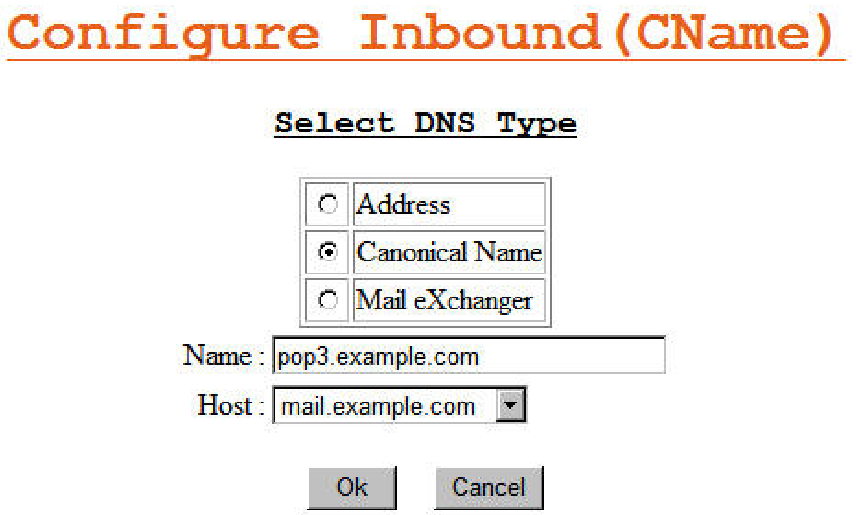
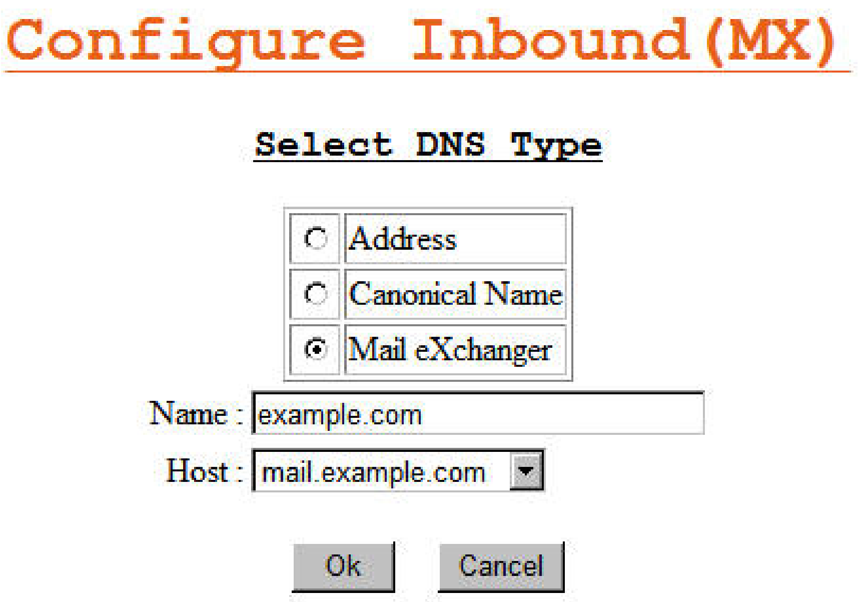
Name	Type	Address	Modify	Delete
host1.example.com	A	WAN1	○	□
host1.example.com	A	WAN2	○	□
www.example.com	C	host1.example.com	○	□
host2.example.com	A	WAN1	○	□
host2.example.com	A	WAN2	○	□
host2.example.com	A	WAN3	○	□
host2.example.com	A	WAN4	○	□
ftp.example.com	C	host2.example.com	○	□

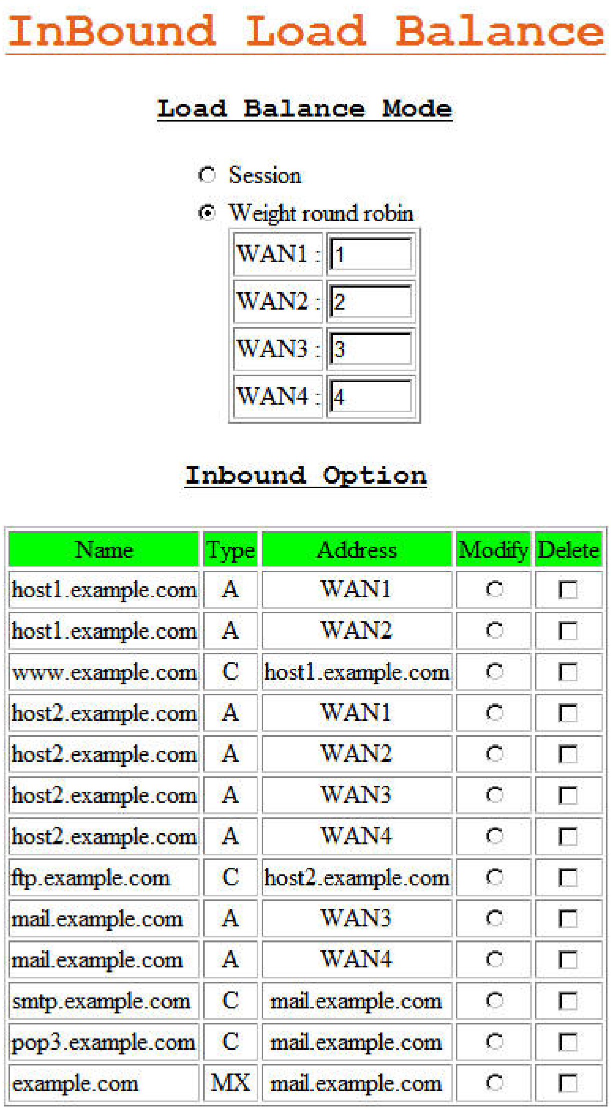
■ **Define ftp.example.com in Inbound Option**

In **Load Balance → Inbound** page, this figure is the display for entering: www.example.com and ftp.example.com.

The mail server requires some additional steps.

 Configure Inbound(Addr) Select DNS Type ● Address ○ Canonical Name ○ Mail eXchanger Name : mail.example.com IP Address : Address : WAN3 	■ **Define mail.example.com in Inbound Option** **Step 1:** In **Load Balance → Inbound** page, click **Add new item**, select **DNS Type** as **Address**, and configure host name for the Mail server address entry: Enter: Name: mail.example.com rather than Name: host3.example.com Port: WAN3
 Configure Inbound(Addr) Select DNS Type ● Address ○ Canonical Name ○ Mail eXchanger Name : mail.example.com IP Address : Address : WAN4 	**Step 2:** **Load Balance → Inbound → Add new item → Configure Inbound (Addr):** Enter the same domain mail.example.com to WAN4

 Configure Inbound(CName) Select DNS Type ○ Address ● Canonical Name ○ Mail eXchanger Name : smtp.example.com Host : mail.example.com ▾ Ok Cancel	**Step 3:** **Load Balance → Inbound → Add new item → Configure Inbound (CName):** Select **Canonical Name** and enter the name as smtp.example.com, select Host with mail.example.com
 Configure Inbound(CName) Select DNS Type ○ Address ● Canonical Name ○ Mail eXchanger Name : pop3.example.com Host : mail.example.com ▾ Ok Cancel	**Step 4:** **Load Balance → Inbound → Add new item → Configure Inbound (CName):** Similarly, do the previous step again for pop3.example.com.
 Configure Inbound(MX) Select DNS Type ○ Address ○ Canonical Name ● Mail eXchanger Name : example.com Host : mail.example.com ▾ Ok Cancel	**Step 5:** **Load Balance → Inbound → Add new item → Configure Inbound (MX):** Select Mail eXchange as DNS type and enter: Name: example.com Host: mail.example.com



InBound Load Balance

Load Balance Mode

○ Session

● Weight round robin

WAN1 :	1
WAN2 :	2
WAN3 :	3
WAN4 :	4

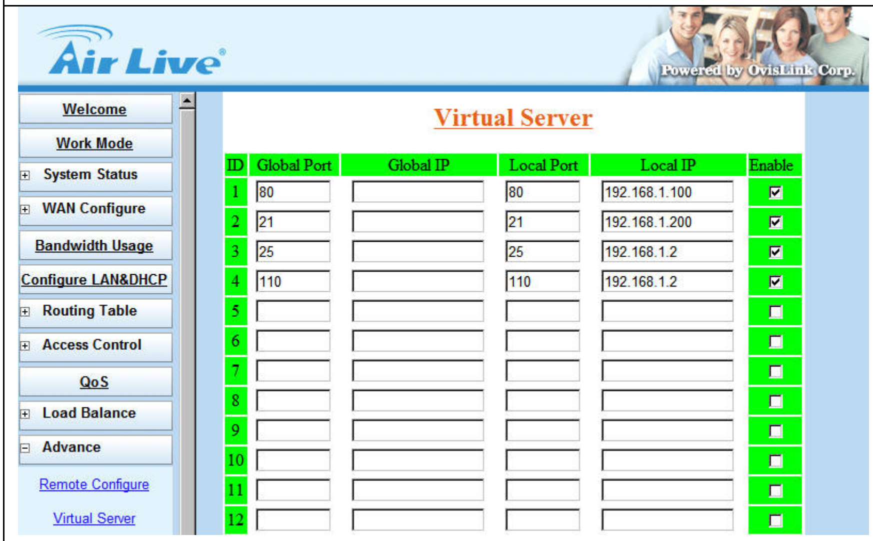
Inbound Option

Name	Type	Address	Modify	Delete
host1.example.com	A	WAN1	○	□
host1.example.com	A	WAN2	○	□
www.example.com	C	host1.example.com	○	□
host2.example.com	A	WAN1	○	□
host2.example.com	A	WAN2	○	□
host2.example.com	A	WAN3	○	□
host2.example.com	A	WAN4	○	□
ftp.example.com	C	host2.example.com	○	□
mail.example.com	A	WAN3	○	□
mail.example.com	A	WAN4	○	□
smtp.example.com	C	mail.example.com	○	□
pop3.example.com	C	mail.example.com	○	□
example.com	MX	mail.example.com	○	□

Step 6:

Load Balance → Inbound:

The Mail Server is configured by the last 5 entries of the DNS Name table.



Virtual Server

ID	Global Port	Global IP	Local Port	Local IP	Enable
1	80		80	192.168.1.100	☑
2	21		21	192.168.1.200	☑
3	25		25	192.168.1.2	☑
4	110		110	192.168.1.2	☑
5					□
6					□
7					□
8					□
9					□
10					□
11					□
12					□

Step 7:

Advance → Virtual Server:

Now we finish the IN-BOUND ROUTER DNS server setting, and we still have to link the WAN IP addresses with the Internal & local LAN servers.

This is done by the **Virtual Server**. Just specify the **Global Port**, **Local Port**, **Local IP Address**, and select **Enable**.

The ratio was specified: WAN1, WAN2, WAN3, WAN4 = 1:2:3:4

- www.example.com uses WAN1 and WAN2 with a ratio of 1:2. The IP addresses return to the queries for the Web Server accesses are: WAN1, WAN2, WAN2, WAN1, WAN2, WAN2…, etc.

- ftp.example.com uses WAN1 – WAN4 with a ratio of 1:2:3:4. The IP addresses return to the queries for the Web Server accesses are: WAN1, WAN2, WAN2, WAN3, WAN3, WAN3, WAN4, WAN4, WAN4, WAN4, and the sequence will repeat.

- Mail.example.com uses WAN3 and WAN4 with a ratio of 3:4. The IP addresses return to the queries for the Web Server accesses are: WAN3, WAN3, WAN3, WAN4, WAN4, WAN4, WAN4, and the sequence will repeat.

For multiple Internet servers, if you have Multiple Public Static IPs, you may use the Multiple DMZ to map public static IP address to each server. Or, if you are using Apache or Microsoft Windows Server, then you can use the Virtual Hosting and Virtual Servers function respectively.