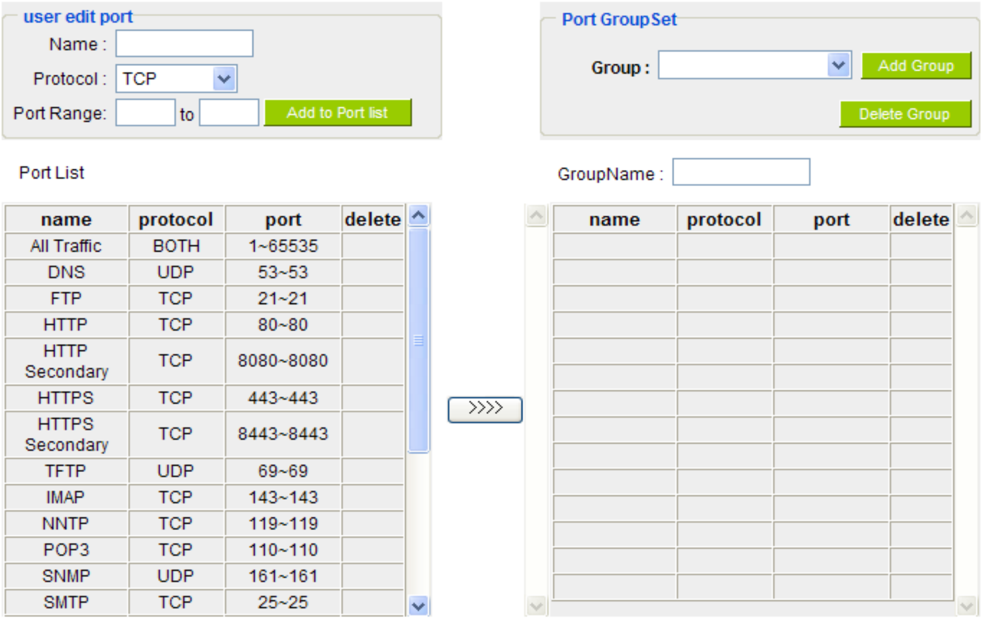
your future life

Port Group Management

User Manual

Port Group Management

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



user edit port

Name :

Protocol : TCP

Port Range: to

Port List

name	protocol	port	delete
All Traffic	BOTH	1~65535	
DNS	UDP	53~53	
FTP	TCP	21~21	
HTTP	TCP	80~80	
HTTP Secondary	TCP	8080~8080	
HTTPS	TCP	443~443	
HTTPS Secondary	TCP	8443~8443	
TFTP	UDP	69~69	
IMAP	TCP	143~143	
NNTP	TCP	119~119	
POP3	TCP	110~110	
SNMP	UDP	161~161	
SMTP	TCP	25~25	

Port GroupSet

Group :

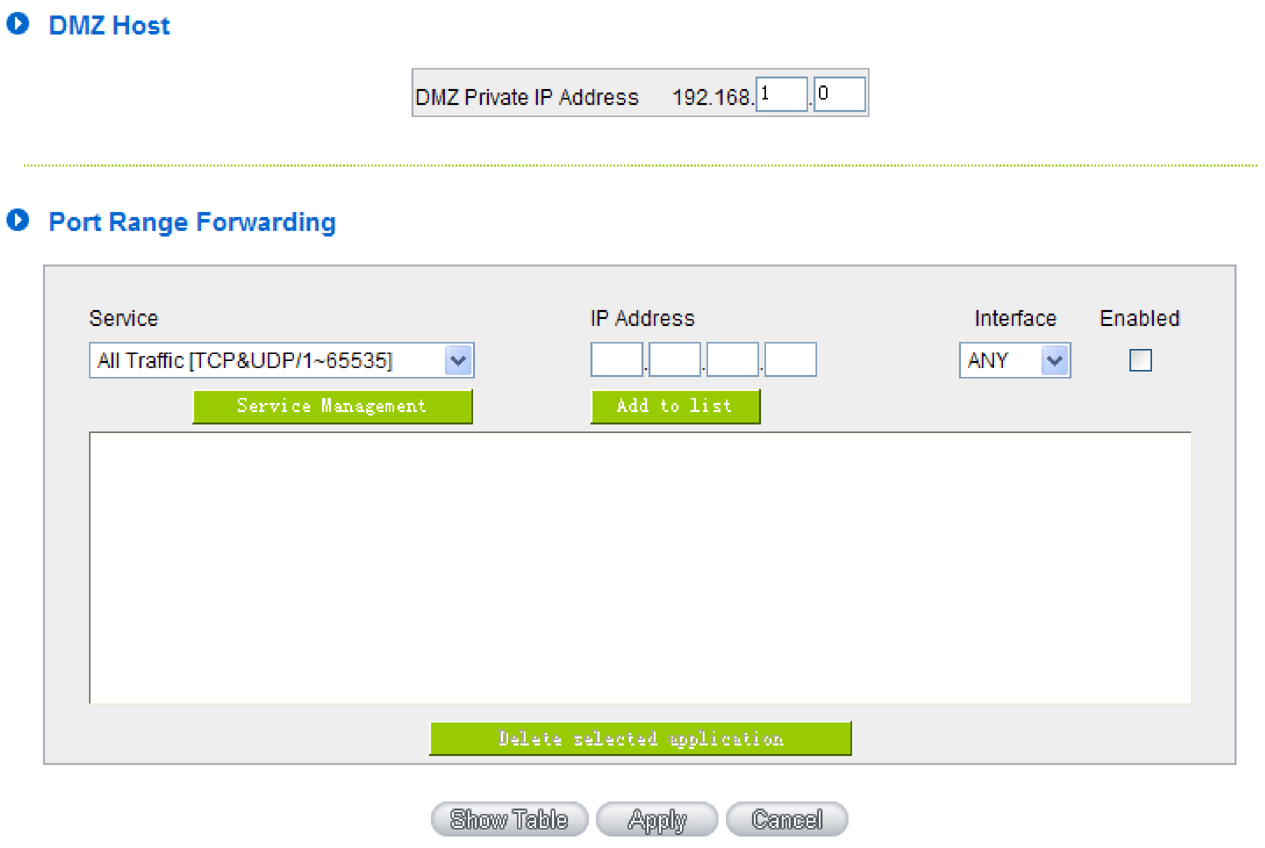
GroupName :

name	protocol	port	delete

User edit port	Input the name, protocol, and port range for the specific service port.
Name	Name the Port in order to identify its property. For example, Virus 135.
Protocol	Choose the port protocol form the pull down list like TCP, UDP or TCP and UDP.
Port Range	Input the port range. For example, 135 to 135.
Add to Port List	After setting name, protocol and port range, push this button to add the information into the Port list below. This port can be from some port groups.
Group Name	When you add new groups, please note if the group name is in the column. For example, Virus.
Delete Group	Choose the group that you would like to delete from the pull- down list, and push the “Delete Group” button. System will ask you again if you would like to delete the group. After pushing the confirmation button, the group will be deleted.
›››› **button**	You can choose several ports from Port list on the left side, and push this button to have them added into the group the right side.
Delete 🗑	Delete self- defined port or port range.
Apply	Click **“Apply”** to save the network configuration modification
Cancel	Click **“Cancel"** to leave without making any changes.

X. Advanced Function

10.1 DMZ Host/ Port Range Forwarding



DMZ Host

DMZ Private IP Address 192.168.1.0

Port Range Forwarding

Service	IP Address	Interface	Enabled
All Traffic [TCP&UDP/1~65535]	. . .	ANY	□

11.1.1 DMZ Host

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

If the “DMZ Host” function is selected, to cancel this function, users must input "0” in the following “DMZ Private IP”. This function will then be closed.

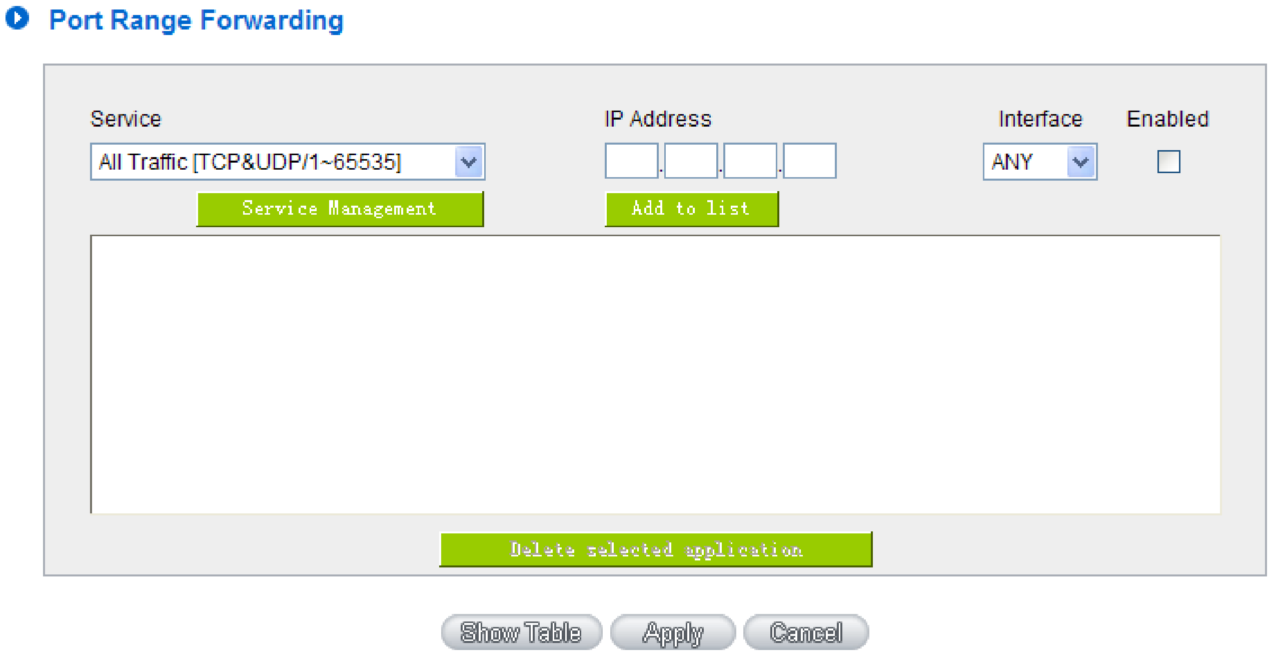
After the changes are completed, click “Apply” to save the network configuration modification, or click “Cancel" to leave without making any changes.

11.1.2 Port Range Forwarding

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

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

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



Port Range Forwarding

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

IP Address: . . .

Interface: ANY

Enabled: □

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

Internal IP Address: Input the virtual host IP address.

Interface: Select the WAN port.

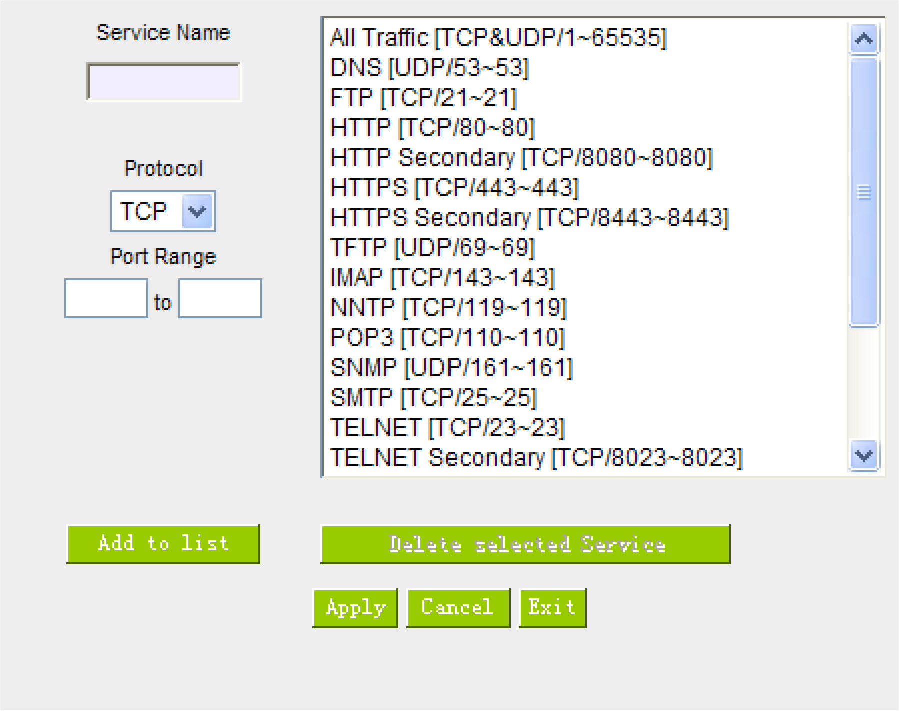
Enabled: Activate this function.

Service Port Management: Add or remove service ports from the list of service ports.

Add to list: Add to the active service content.

Service Port Management

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



Protocol: TCP

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

Service Name: Input the name of the service port users want to activate on the list, such as E-donkey, etc.

Protocol: To select whether a service port is TCP or UDP.

Port Range: To activate this function, input the range of the service port locations users want to activate.

Add to list: Add the service to the service list.

Delete selected item: To remove the selected services.

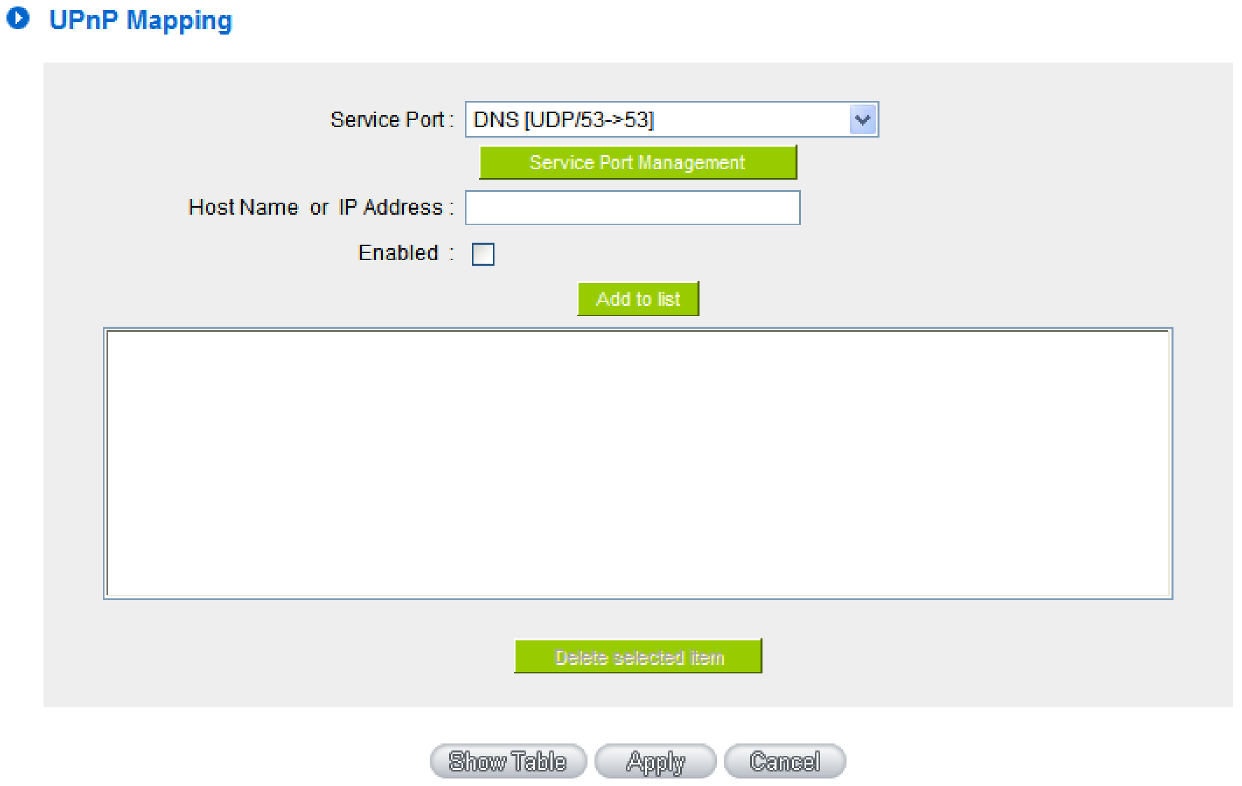
Apply: Click the “Apply” button to save the modification.

Cancel: Click the “Cancel” button to cancel the modification. This only works before “Apply” is clicked.

Close: Quit this configuration window.

10.2 UPnP

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



UPnP Mapping

Service Port : DNS [UDP/53->53]

Host Name or IP Address :

Enabled : □

Service Port: Select the UPnP service number default list here; for example, WWW is 80~80, FTP is 21~21. Please refer to the default service number list.

Host Name or IP Address: Input the Intranet virtual IP address or name that maps with UPnP such as 192.168.1.100.

Enabled: Activate this function.

Service Port Management: Add or remove service ports from the management list.

Add to List: Add to active service content.

Delete Selected Item: Remove selected services.

Show Table: This is a list which displays the current active UPnP functions.

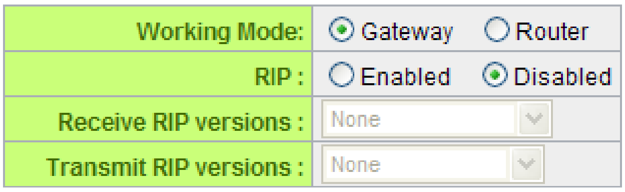
Apply: Click “Apply” to save the network configuration modification.

Cancel: Click “Cancel" to leave without making any change.

10.3 Routing

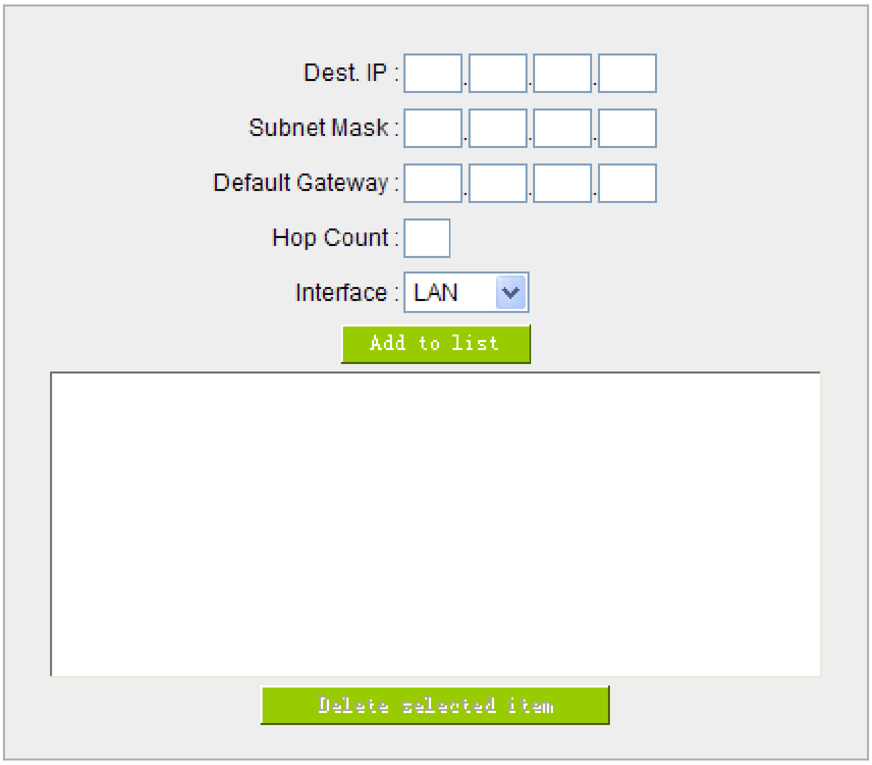
In this chapter we introduce the Dynamic Routing Information Protocol and Static Routing Information Protocol.

Dynamic Routing



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

Static Routing



Dest. IP : □.□.□.□

Subnet Mask : □.□.□.□

Default Gateway : □.□.□.□

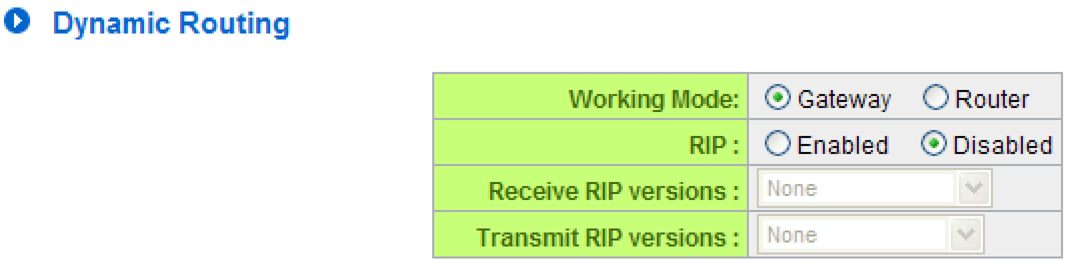
Hop Count : □

Interface : LAN

10.3.1 Dynamic Routing

The abbreviation of Routing Information Protocol is RIP. There are two kinds of RIP in the IP environment – RIP I and RIP II. Since there is usually only one router in a network, ordinarily just Static Routing will be used. RIP is used when there is more than one router in a network, and if an administrator doesn't want to assign a path list one by one to all of the routers, RIP can help refresh the paths.

RIP is a very simple routing protocol, in which Distance Vector is used. Distance Vector determines transmission distance in accordance with the number of routers, rather than based on actual session speed. Therefore, sometimes it will select a path through the least number of routers, rather than through the fastest routers.



Dynamic Routing

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

Working Mode: Select the working mode of the device: NAT mode or Router mode.

RIP: Click “Enabled” to open the RIP function.

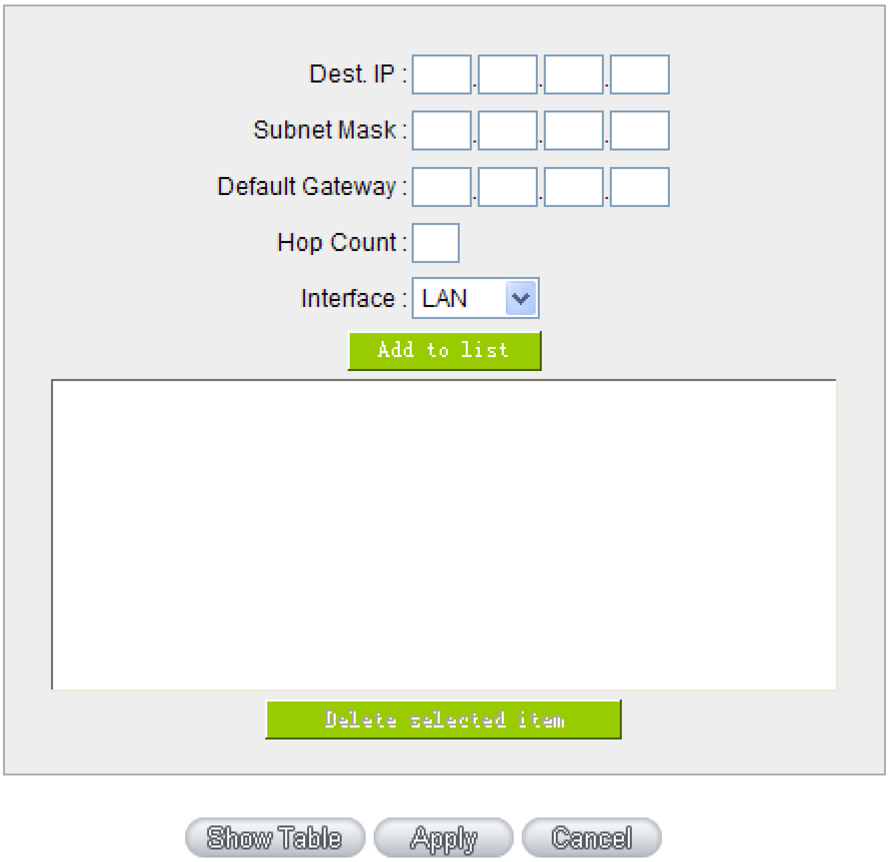
Receive RIP versions: Use Up/Down button to select one of “**None**， **RIPv1**， **RIPv2**， **Both RIPv1 and v2**” as the “**TX**” function for transmitting dynamic RIP.

Transmit RIP versions: Use Up/Down button to select one of “**None**，**RIPv1**，**RIPv2-Broadcast**，**RIPv2-Multicast**” as the “**RX**” function for receiving dynamic RIP.

10.3.2 Static Routing

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

Static Routing



Dest. IP : [ ] . [ ] . [ ] . [ ]

Subnet Mask : [ ] . [ ] . [ ] . [ ]

Default Gateway : [ ] . [ ] . [ ] . [ ]

Hop Count : [ ]

Interface : LAN

Dest. IP: Input the remote network IP locations and subnet that is to be

Subnet Mask: routed. For example, the IP/subnet is 192.168.2.0/255.255.255.0.

Gateway: The default gateway location of the network node which is to be routed.

Hop Count: This is the router layer count for the IP. If there are two routers under the device, users should input “2” for the router layer; the default is “1”. (Max. is 15.)

Interface: This is to select “WAN port” or “LAN port” for network connection location.

Add to List: Add the routing rule into the list.

Delete Selected Item: Remove the selected routing rule from the list.

Show Table: Show current routing table.

Apply: Click **“Apply”** to save the network configuration modification

Cancel: Click **“Cancel"** to leave without making any changes.

10.4 One to One NAT

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

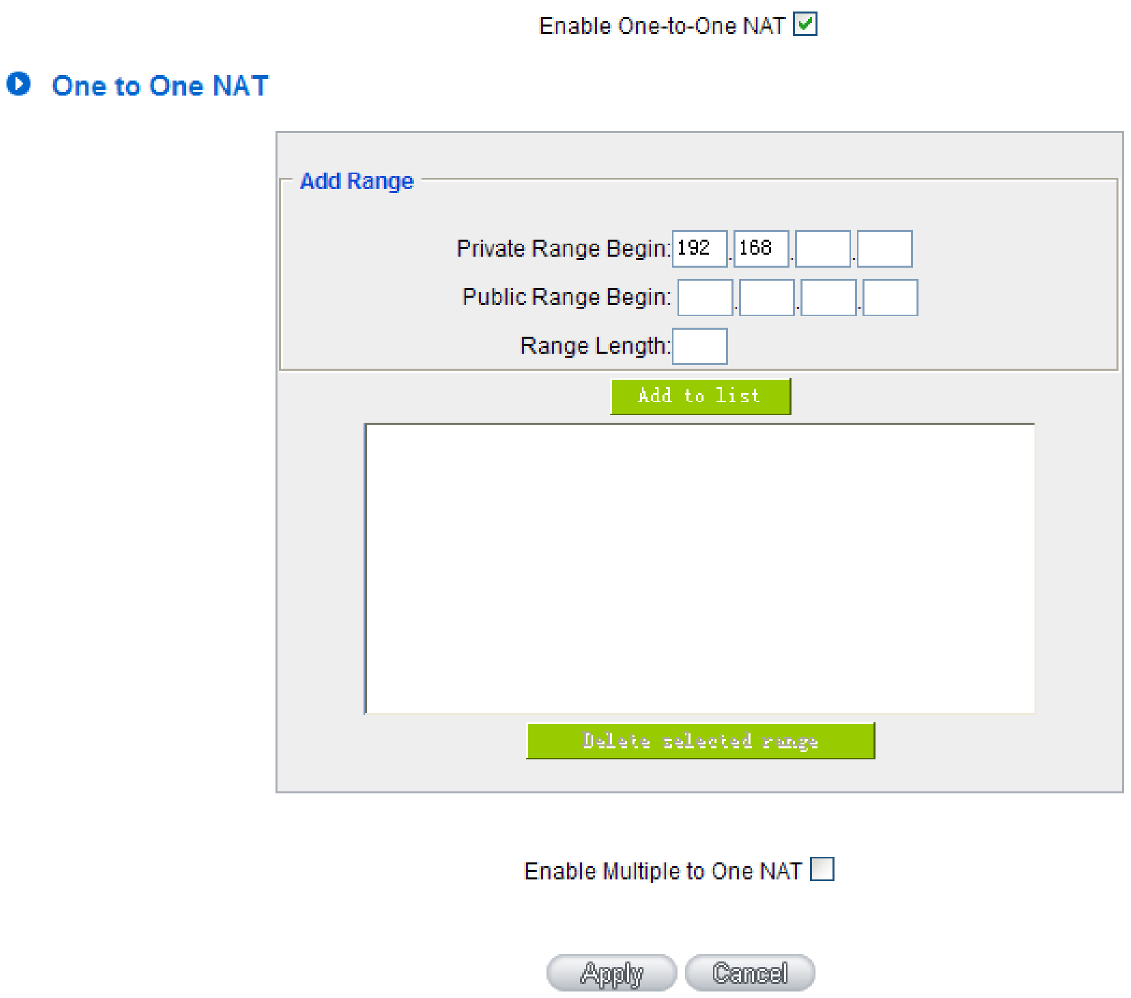
For example, if there are more than 2 web servers requiring public IP addresses, administrators can map several public IP addresses directly to internal private IP addresses.

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

210.11.1.2→	192.168.1.3
210.11.1.3→	192.168.1.4
210.11.1.4→	192.168.1.5
210.11.1.5→	192.168.1.6

Attention！

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



Enable One-to-One NAT ☑

One to One NAT

Add Range

Private Range Begin: 192 . 168 . .

Public Range Begin: . . .

Range Length:

Enable Multiple to One NAT □

Enabled One to One NAT: To activate or close the One-to-One NAT function. (Check to activate the function).

Private IP Range Begin: Input the Private IP address for the Intranet One-to-One NAT function.

Public IP Range Begin: Input the Public IP address for the Internet One-to-One NAT function.

Range Length: The numbers of final IP addresses of actual Internet IP addresses. (Please do not include IP addresses in use by WANs.)

Add to List: Add this configuration to the One-to-One NAT list.

Delete Selected Item: Remove a selected One-to-One NAT list.

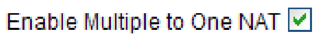
Apply: Click **“Apply”** to save the network configuration modification.

Cancel: Click **“Cancel"** to leave without making any changes.

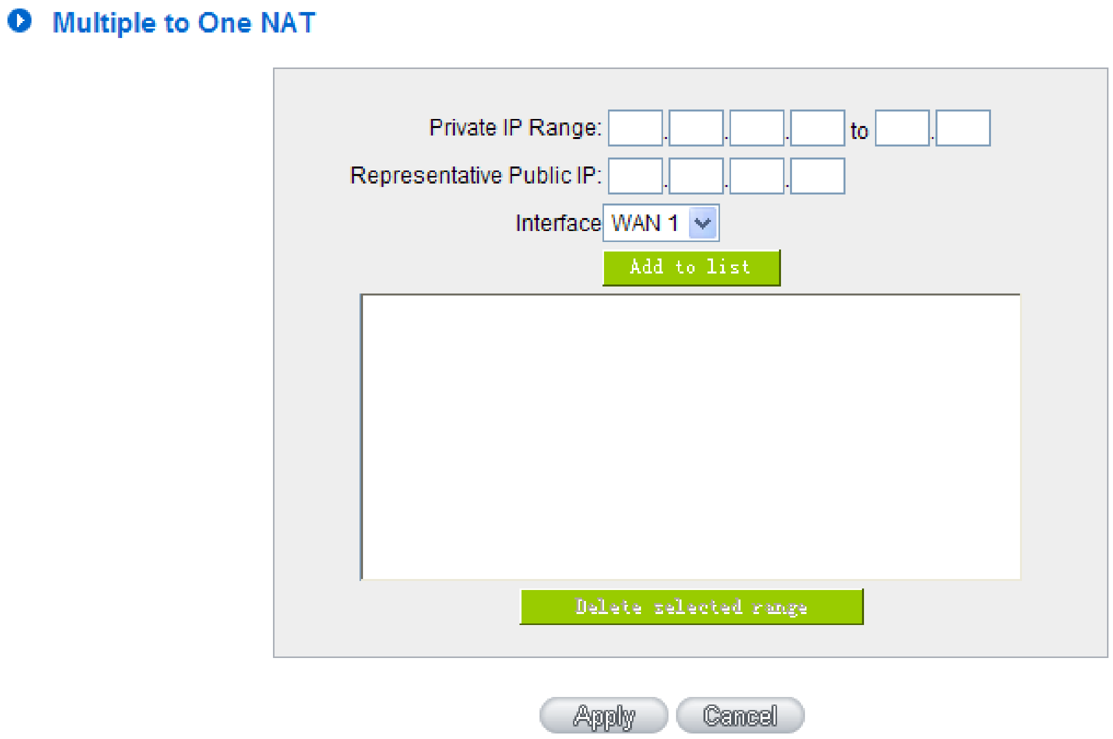
Attention！

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

Multiple to One NAT



Enable Multiple to One NAT ☑



Multiple to One NAT

Private IP Range: [ ].[ ].[ ].[ ] to [ ].[ ]

Representative Public IP: [ ].[ ].[ ].[ ]

Interface WAN 1

Enable Multiple to One NAT Click to enable multiple to one NAT function.

Private IP Range Input intranet IPs for NAT mapping.

Respective Public IP Input the respective public IP addresses. This should go along with the following interface selection. If the IP address is not within the interface ranges, the setting will not work.

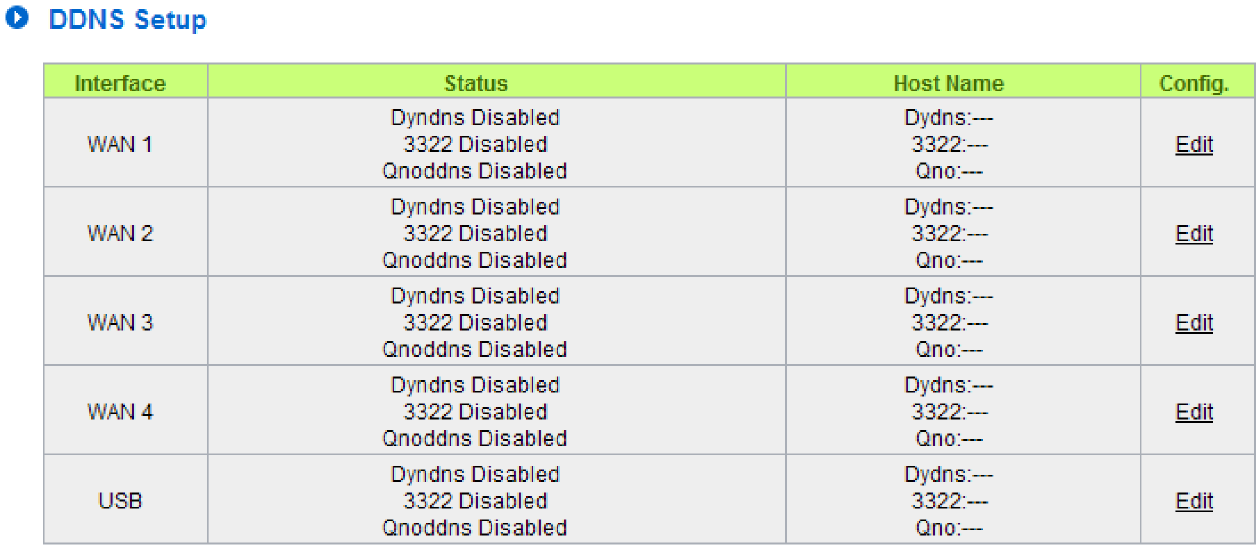
Interface Select the mapping interface. If the WAN IP above is not within the interface range, the setting will not work.

Add to List	Add this configuration to the One-to-One NAT list.
Delete selected range	Remove a selected One-to-One NAT list.
Apply	Click **“Apply”** to save the network configuration modification.
Cancel	Click **“Cancel"** to leave without making any changes.

10.5 DDNS- Dynamic Domain Name Service

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

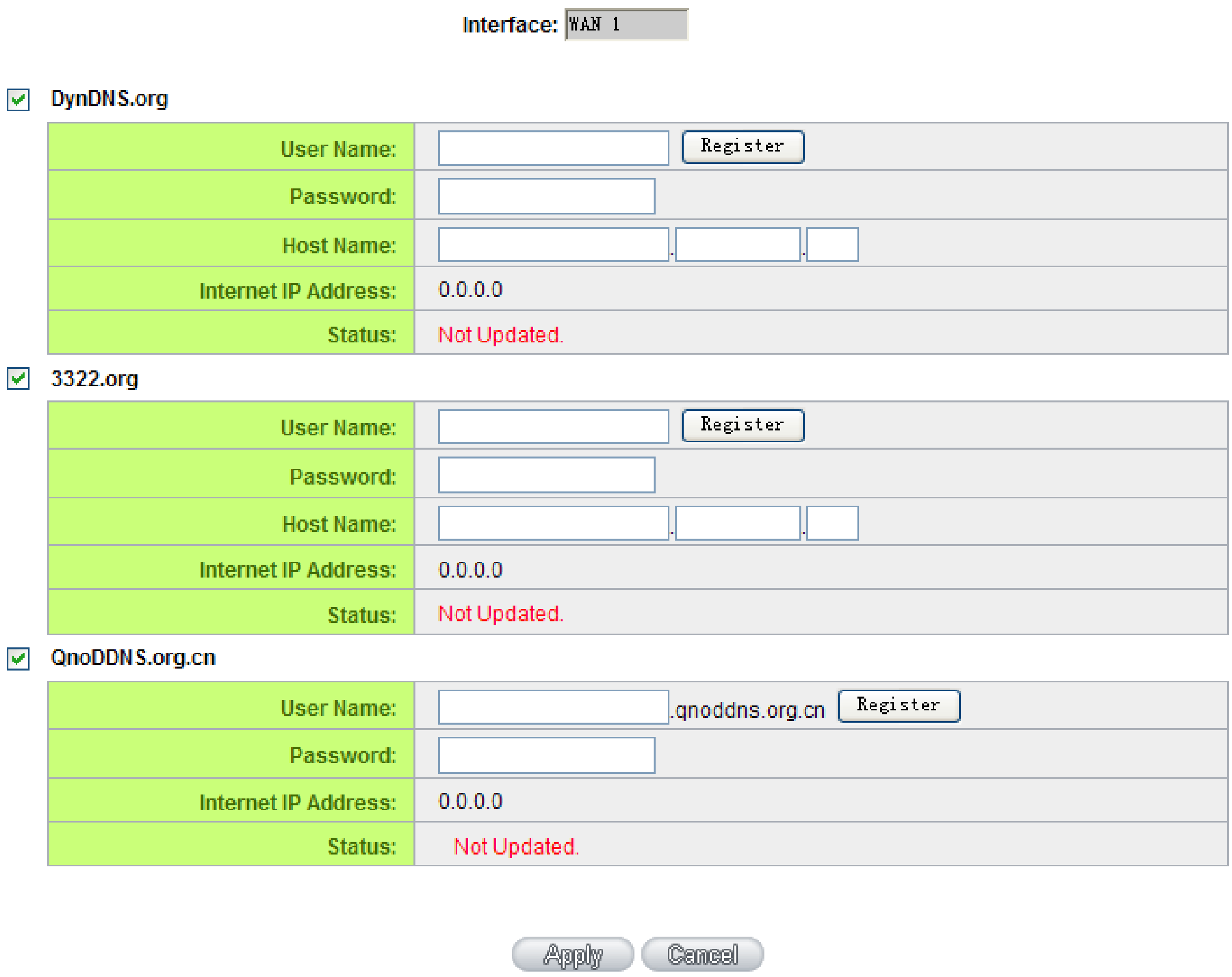
Also, in order to solve the issue that DDNS server is not stable, the device can update the dynamic IP address with different services at the same time.



DDNS Setup

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

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



Interface: WAN 1

☑ DynDNS.org

User Name:	Register
Password:	
Host Name:	. .
Internet IP Address:	0.0.0.0
Status:	Not Updated.

☑ 3322.org

User Name:	Register
Password:	
Host Name:	. .
Internet IP Address:	0.0.0.0
Status:	Not Updated.

☑ QnoDDNS.org.cn

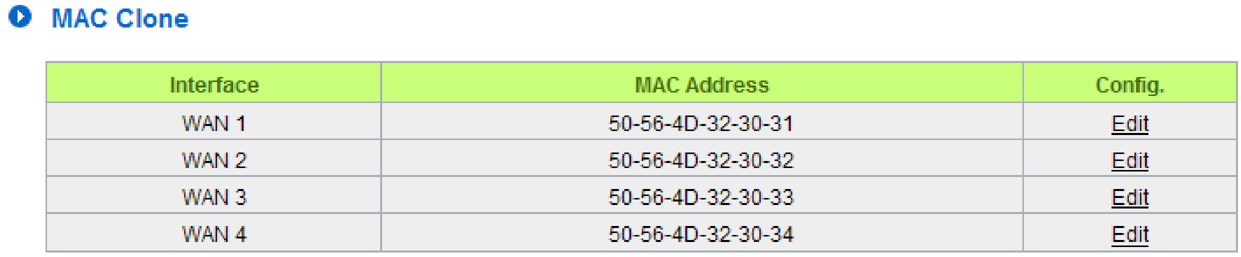
User Name:	.qnoddns.org.cn Register
Password:	
Internet IP Address:	0.0.0.0
Status:	Not Updated.

Interface	This is an indication of the WAN port the user has selected.
DDNS	Check either of the boxes before DynDNS.org, 3322.org, DtDNS.com and QnoDDNS.org.cn to select one of the four DDNS website address transfer functions.
Username	The name which is set up for DDNS. Input a complete website address such as abc.qnoddns.org.cn as a user name for QnoDDNS.
Password	The password which is set up for DDNS.
Host Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.
Internet IP Address	Input the actual dynamic IP address issued by the ISP.
Status	An indication of the status of the current IP function refreshed by DDNS.
Apply	After the changes are completed, click **“Apply”** to save the network

	configuration modification.
Cancel	Click **“Cancel"** to leave without making any changes.

10.6 MAC Clone

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

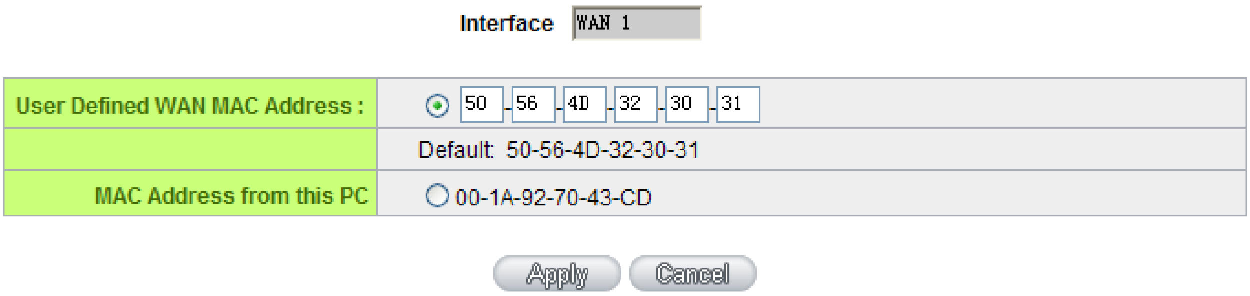


MAC Clone

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

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

Default MAC address is the WAN MAC address.



Interface: WAN 1

User Defined WAN MAC Address :	● 50 - 56 - 4D - 32 - 30 - 31
	Default: 50-56-4D-32-30-31
MAC Address from this PC	○ 00-1A-92-70-43-CD

10.7 Inbound Load Balance

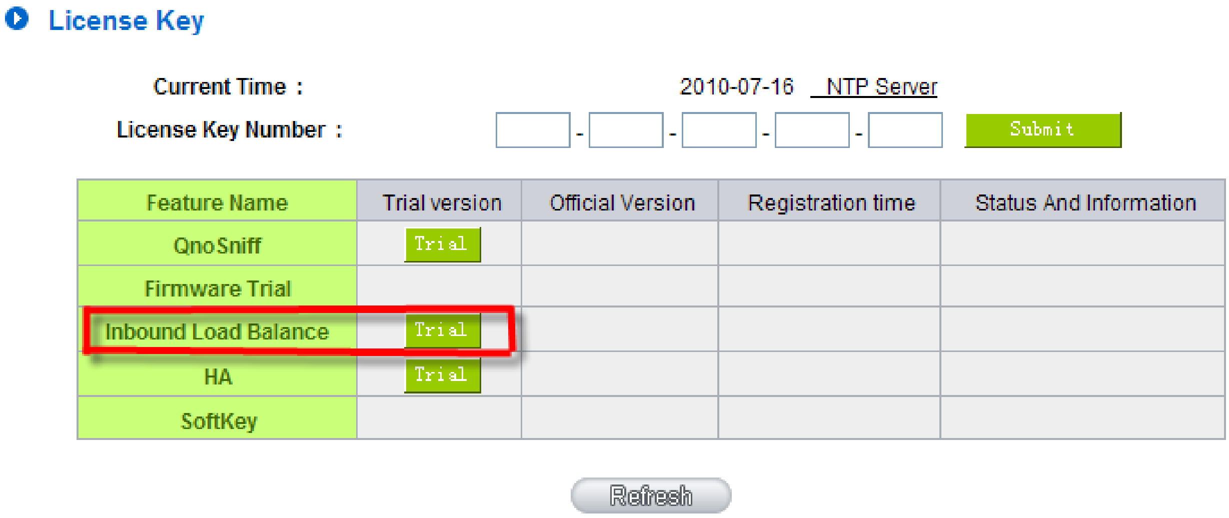
Qno Firewall/Router not only supports efficient Outbound Load Balance, but Inbound Load Balance. It distributes inbound traffic equally to every WAN port to make best use of bandwidth. It also can prevent traffic from unequally distribution and congested. Users can use only one device to satisfy the demand of Inbound/Outbound Load Balance simultaneously.

Following introduces how to enable and setup Inbound Load Balance step by step.

Attention!

In For some models of Qno routers, user can try the function for a period but with time limit. If the function can match your network demand, you can apply for the official version License Key in Qno Official Website (www.qno.com.tw). After applying, auditing, paying and inputting License Key successfully, users can use the official version without time limit.

1. System Tool => License Key => Try to enable “Inbound Load Balance.”



License Key

Current Time : 2010-07-16 NTP Server

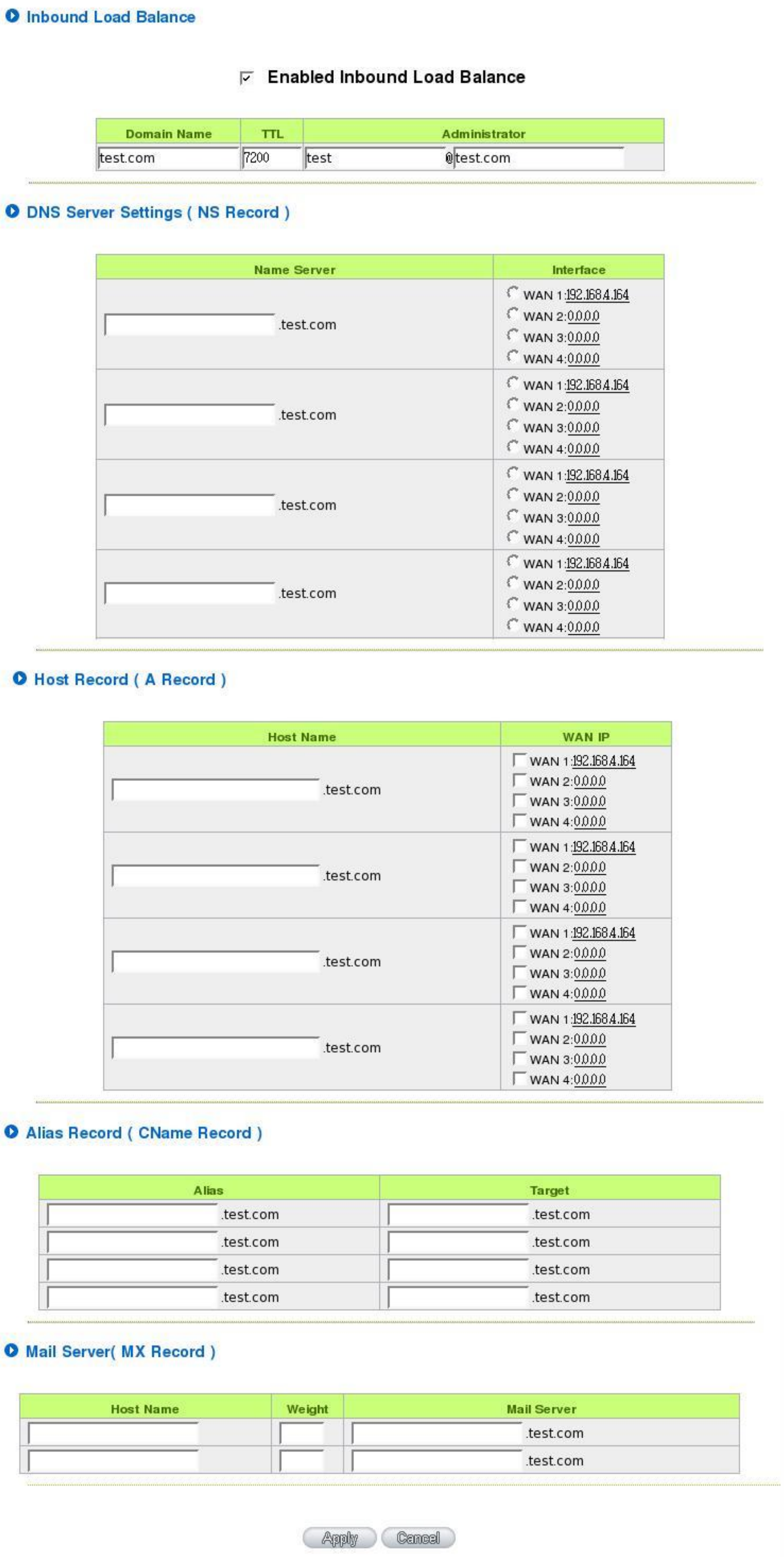
License Key Number : [ ]-[ ]-[ ]-[ ]-[ ] Submit

Feature Name	Trial version	Official Version	Registration time	Status And Information
QnoSniff	Trial			
Firmware Trial				
Inbound Load Balance	Trial			
HA	Trial			
SoftKey				

After enabling Trial version, “Status and Information” column will display the remaining trial time. If trial expires, the function can not work out at all unless users enter an official License Key.

2. Go to “Inbound Load Balance” in “Advanced Function” and click “Edit” to configure.

3. Enable “Inbound Load Balance.”



Inbound Load Balance

☑ Enabled Inbound Load Balance

Domain Name	TTL	Administrator
test.com	7200	test @test.com

DNS Server Settings (NS Record)

Name Server	Interface
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0

Host Record (A Record)

Host Name	WAN IP
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0

Alias Record (CName Record)

Alias	Target
.test.com	.test.com
.test.com	.test.com
.test.com	.test.com
.test.com	.test.com

Mail Server(MX Record)

Host Name	Weight	Mail Server
		.test.com
		.test.com

4. Configure Domain Name and Host IP.

Assign DNS service provider and Host IP address. Take the setting on TWNIC as an example, the network structure and IP are as following:

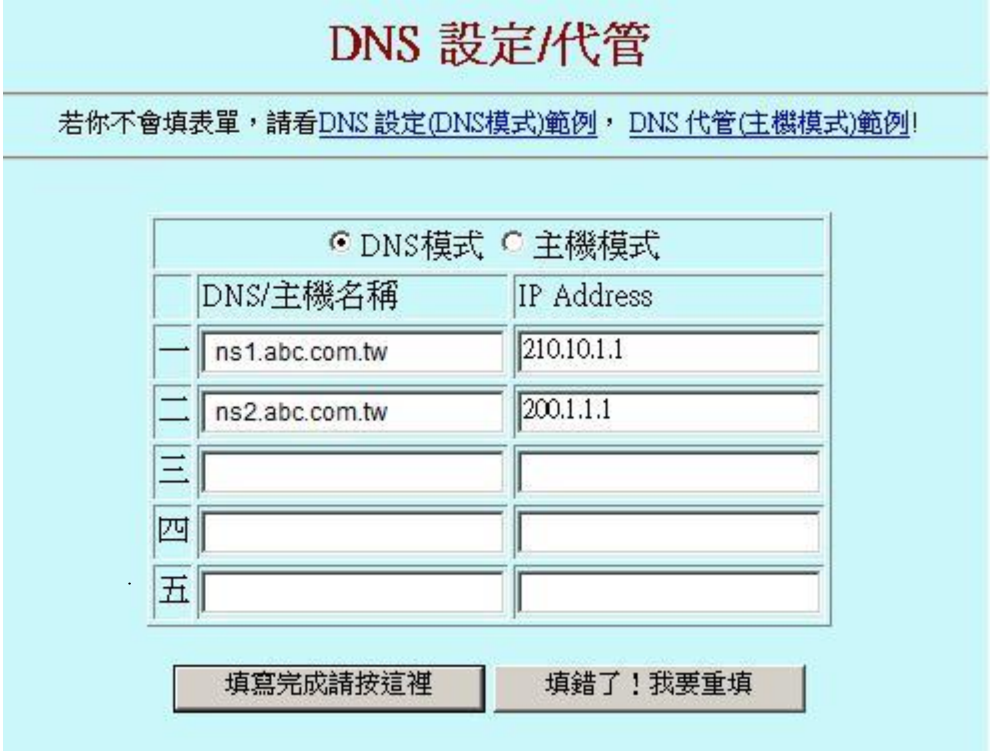
WAN1:ADSL ISP A 210.10.1.1

WAN2:ADSL ISP B 200.1.1.1

Domain Name:abc.com.tw

Name Server(NS):ns1.abc.com.tw /ns2.abc.com.tw

Go to website of your DNS service provider to modify your own DNS Host/IP, as the following figure:



DNS 設定/代管

若你不會填表單，請看DNS 設定(DNS模式)範例， DNS 代管(主機模式)範例!

● DNS模式 ○ 主機模式

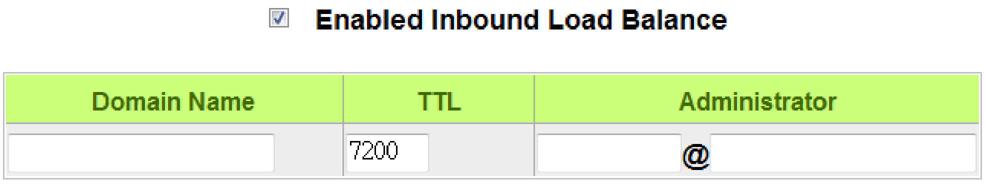
	DNS/主機名稱	IP Address
一	ns1.abc.com.tw	210.10.1.1
二	ns2.abc.com.tw	200.1.1.1
三		
四		
五		

Choose DNS mode, and then fill in the Host name and corresponding IP address of WAN1 and WAN2. Press “Finish” button, the setting will be effective in 24 hours.

Attention!

Please follow your ISP to modify Host/IP assignment if your upper level isn’t TWNIC! If your DNS agent is other ISP, please refer to the Web configuration provided by your ISP!?

5. Configure Firewall/Router Domain Name



☑ Enabled Inbound Load Balance

Domain Name	TTL	Administrator
	7200	@

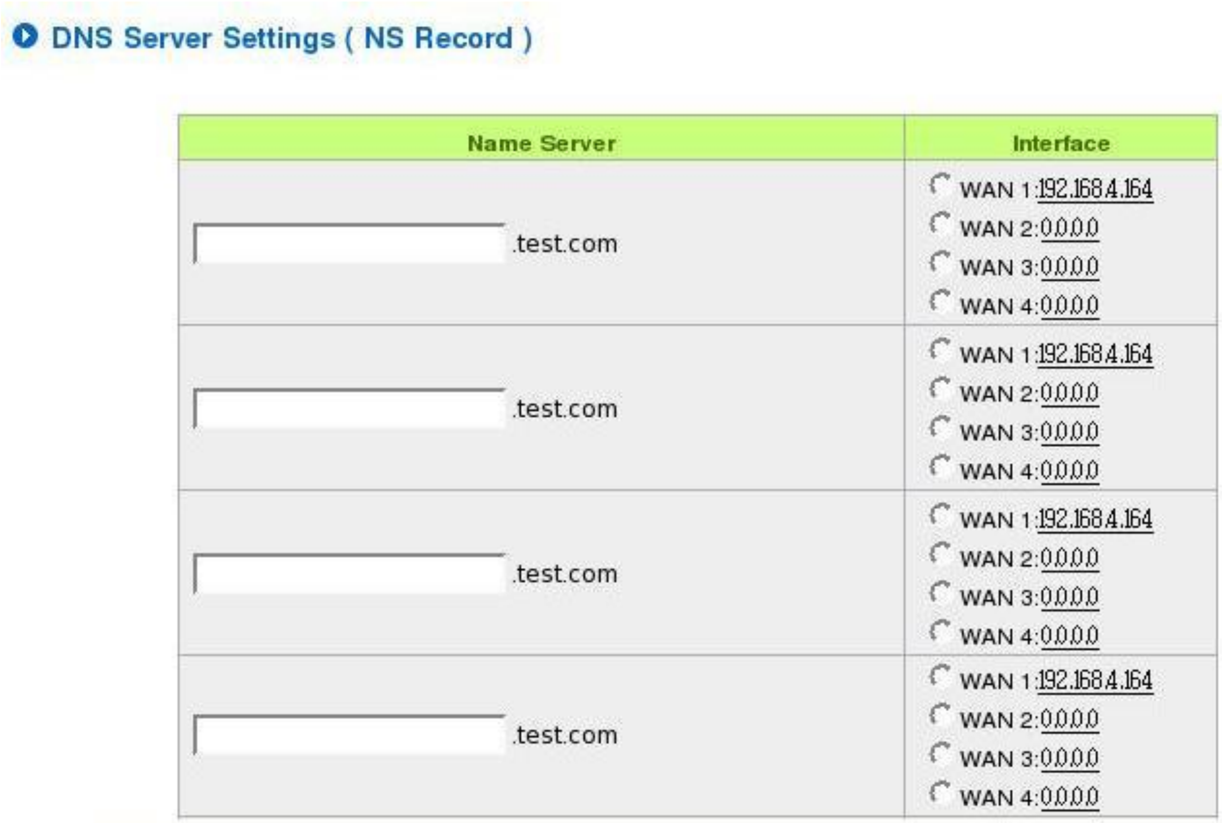
Domain Name: Input the Domain Name which is applied before. The domain name will be shown in following configuration automatically without entering again.

Time To Live: Time To Live (the abbreviation is TTL) is time interval of DNS inquiring (second, 0~65535). Too long interval will affect refresh time. Shorter time will increase system's loading, but the effect of Inbound Load Balance will be more correct. You can adjust according your reality application.

Administrator: Enter administrator's E-mail address, e.g. test@abc.com.tw.

6. DNS Server Settings: Add or Modify NS Record. (NS Record)

NS Record is the record of DNS server to assign which DNS server translates the domain name.



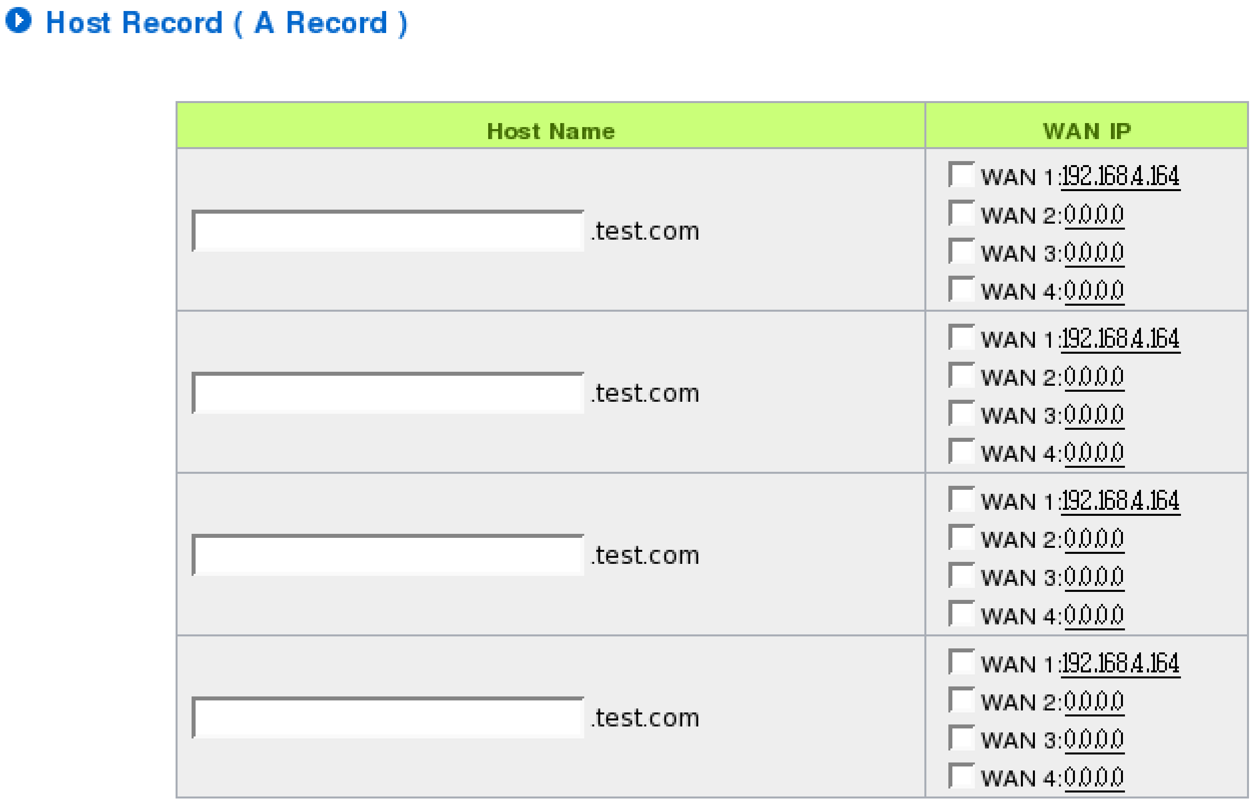
DNS Server Settings (NS Record)

Name Server	Interface
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0
.test.com	○ WAN 1:192.168.4.164 ○ WAN 2:0.0.0.0 ○ WAN 3:0.0.0.0 ○ WAN 4:0.0.0.0

DNS Server Input registered NS Record, ex. ns1, ns2.

Interface: Assign WAN IP address as corresponding IP of NS Record. The system will show all acquired enabled WAN IP addresses automatically so that users can check directly. But users have to check if the IP addresses are the same as the corresponding settings on TWNIC DNS service provider. (Ex. ns1.abc.com.tw ⇔ WAN1: 210.10.1.1, ns2.abc.com.tw⇔WAN2: 200.1.1.1)

7. Host Record: Add or modify host record. (A Record)



Host Record (A Record)

Host Name	WAN IP
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0
.test.com	□ WAN 1:192.168.4.164 □ WAN 2:0.0.0.0 □ WAN 3:0.0.0.0 □ WAN 4:0.0.0.0

Host Name: Input the host name which provides services. E.g. mail server or FTP.

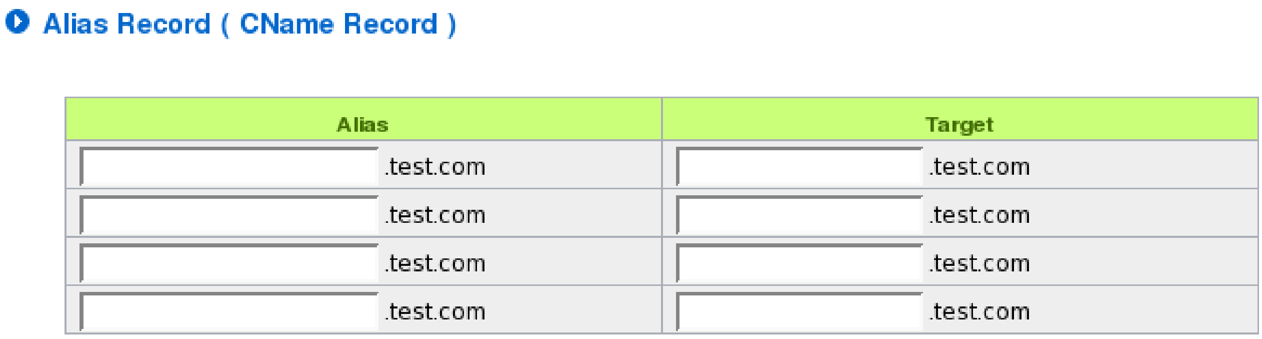
WAN IP: Check corresponding A Record IP (WAN Port IP). If more than one IPs is checked, Inbound traffic will be distributed on this WANs.

8. Alias Record : Add or modify alias record (CNAME Record)

This kind of record allows you to assign several names to one computer host, which may provide several services on it.

For instance, there is a computer whose name is “host.mydomain.com” (A record). It provides WWW and Mail services concurrently. Administrator can configure as two CNAME: WWW and Mail. They are “www.mydomain.com” and “mail.mydomain.com”. They are both orientated to “host.mydomain.com.”

You can also assign several domain names to the same IP address. One of the domains will be A record corresponding server IP, and the others will be alias of A record domain. If you change your server IP, you don’t have to modify every domain one by one. Just changing A record domain, and the other domains will be assigned to new IP address automatically.



Alias Record (CName Record)

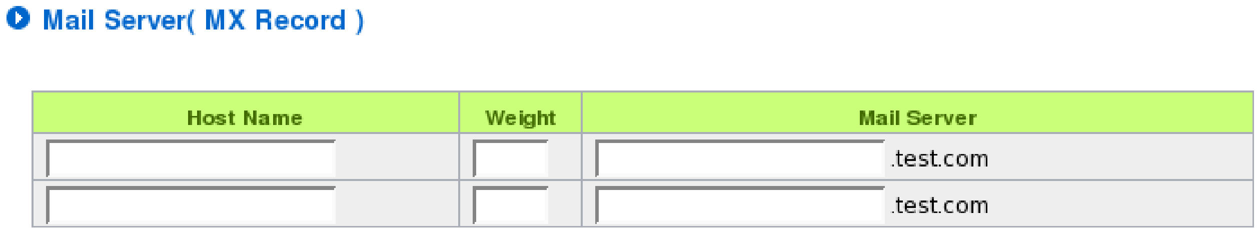
Alias	Target
.test.com	.test.com
.test.com	.test.com
.test.com	.test.com
.test.com	.test.com

Alias: Input Alias Record corresponding to A Record.

Target: Input the existed A Record domain name.

9. Mail Server: Add or modify mail server record.

MX Record is directed to a mail server. It orientates to a mail server according to the domain name of an E-mail address. For example, someone on internet sends a mail to user@myhomain.com. The mail server will search MX Record of mydomain.com through DNS. If the MX Record exists, sender PC will send mails to the mail server assigned by MX Record.



Mail Server(MX Record)

Host Name	Weight	Mail Server
		.test.com
		.test.com

Host Name: Display the host name without domain name of mail host.

Weight: Indicate the order of several mail hosts, the smaller has more priority.

Mail Server:	Input the server name which is saved in A Record or external mail server.

Click **"Apply"** button to save the configuration. Besides, users have to configure DNS service port as following description.

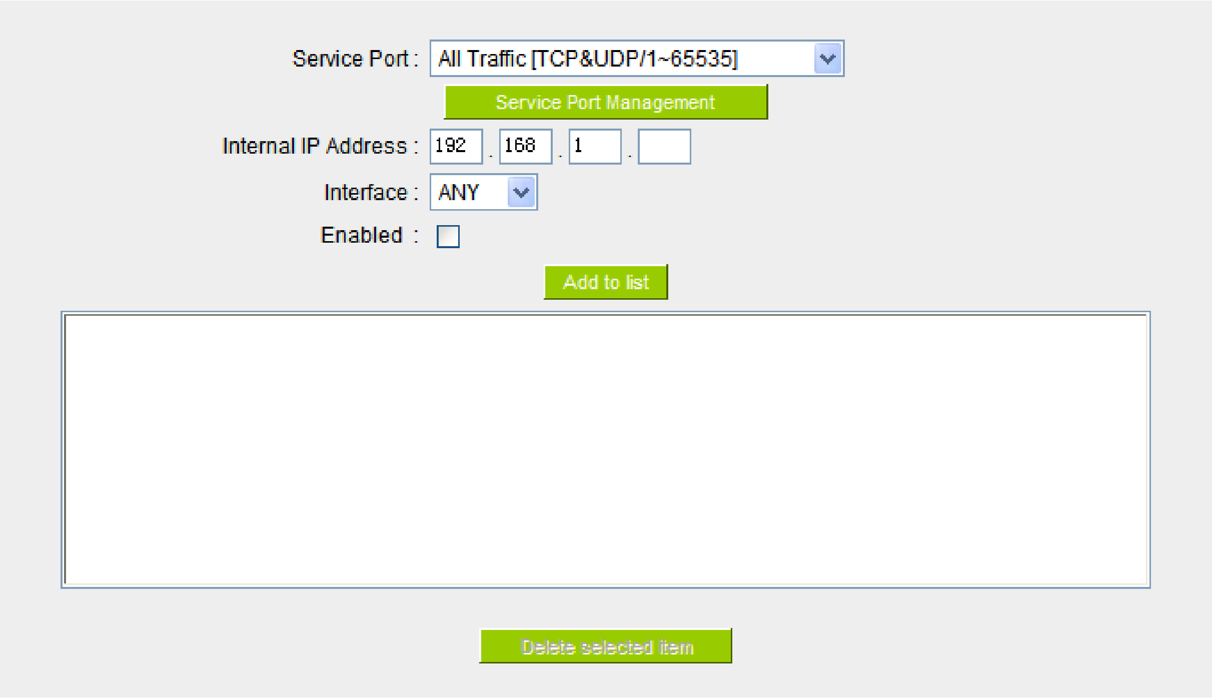
10. Enable DNS Query (DNS service port) in Access Rule of Firewall setting.

Add a new access rule in Firewall setting to enable DNS service port of the WAN on which Inbound Load Balance need to be enabled.

Action:	Check "Allow".
Service Port:	From the drop-down menu, select "DNS [UDP/53~53]."
Log:	Check "Enable" if DNS Query data should be recorded.
Interface:	Check the WAN port on which Inbound Load Balance is enabled.
Source IP:	Select "Any".
Dest. IP:	Select WAN port and input correspondingly IP of the domain name. Take the previous example, input 210.10.1.1.
Scheduling:	Select "Always".

11. Enable internal IP and service port corresponding to A Record in Port Range Forwarding of Advanced Function.

Port Range Forwarding



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

Internal IP Address : 192 . 168 . 1 .

Interface : ANY

Enabled : □

Service Port: Activate the service port of A Record server, e.g. SMTP [TCP/25~25] for Mail.

Internal IP: Input the internal IP of A Record, e.g. 192.168.8.100 of Mail server.

Interface: Select the WAN port of A Record and corresponding IP.

Enable: Activate the configuration.

Add to List: Add to the active service content.

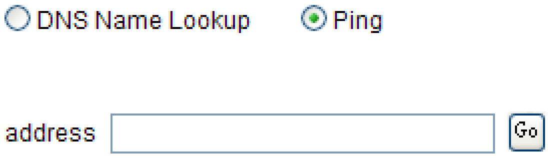
XI. System Tool

This chapter introduces the management tool for controlling the device and testing network connection.

For security consideration, we strongly suggest to change the password. Password and Time setting is in Chapter 5.2.

11.1 Diagnostic

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

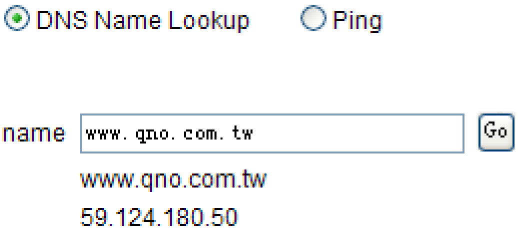


○ DNS Name Lookup ● Ping

Ping host or IP address

DNS Name lookup

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



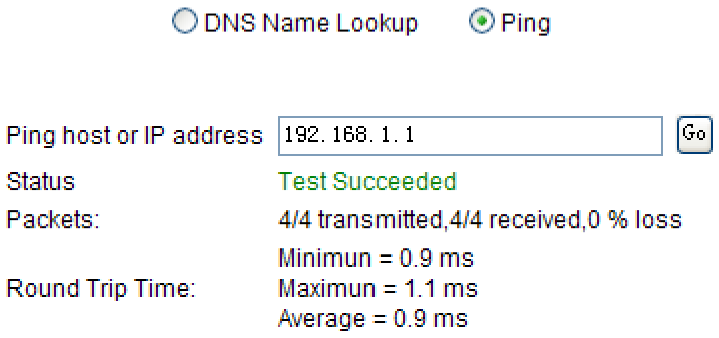
● DNS Name Lookup ○ Ping

Look up the name: www.qno.com.tw

Name: www.qno.com.tw

Address: 59.124.180.50

Ping



○ DNS Name Lookup ● Ping

Ping host or IP address	192. 168. 1. 1 [Go]
Status	Test Succeeded
Packets:	4/4 transmitted,4/4 received,0 % loss

Round Trip Time:	Minimun = 0.9 ms
	Maximun = 1.1 ms
	Average = 0.9 ms

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

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

.

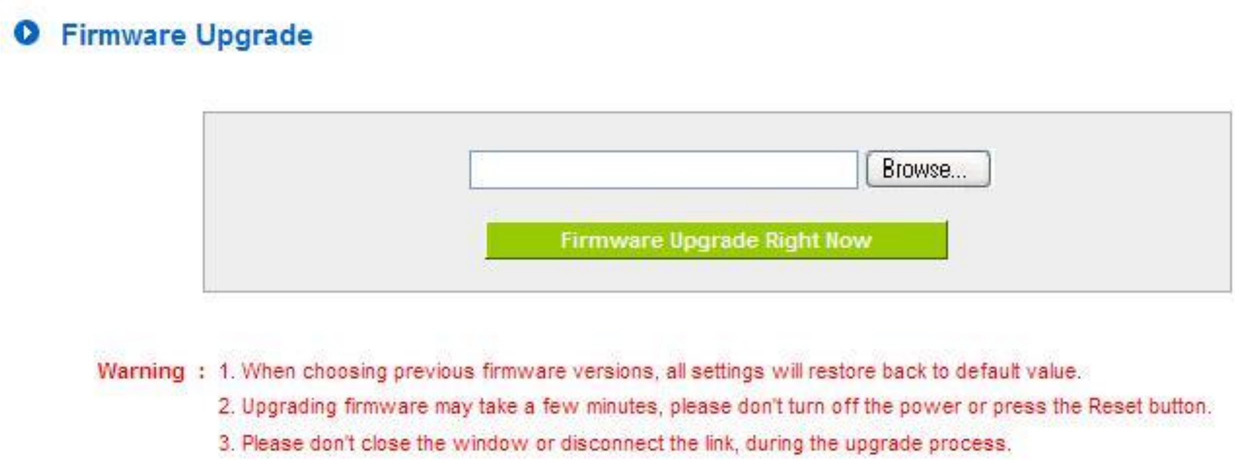
11.2 Firmware Upgrade

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

Note！

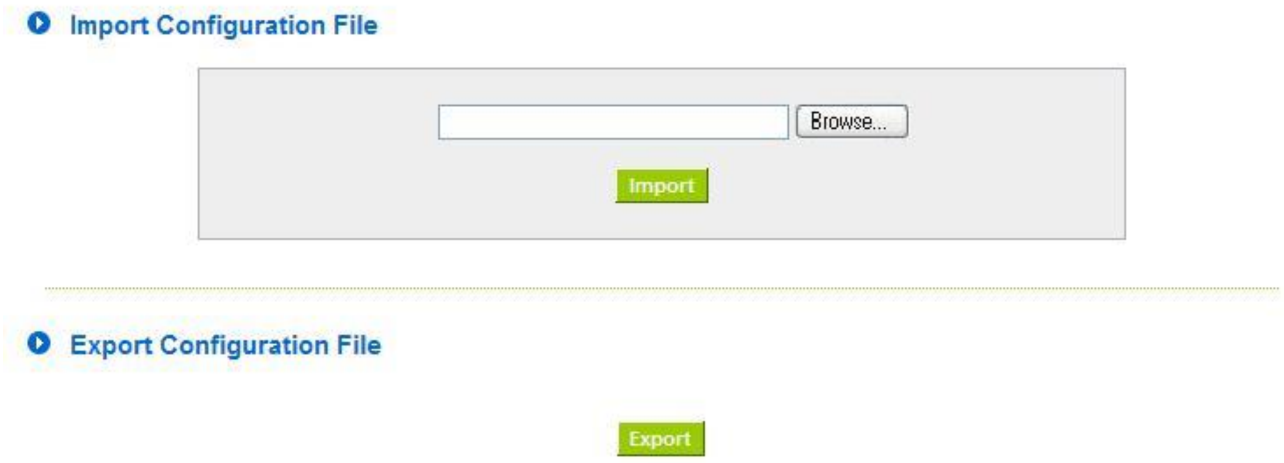
Please read the warning before firmware upgrade.

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



Warning ： 1. When choosing previous firmware versions, all settings will restore back to default value.
2. Upgrading firmware may take a few minutes, please don't turn off the power or press the Reset button.
3. Please don't close the window or disconnect the link, during the upgrade process.

11.3 Setting Backup



Import Configuration File:

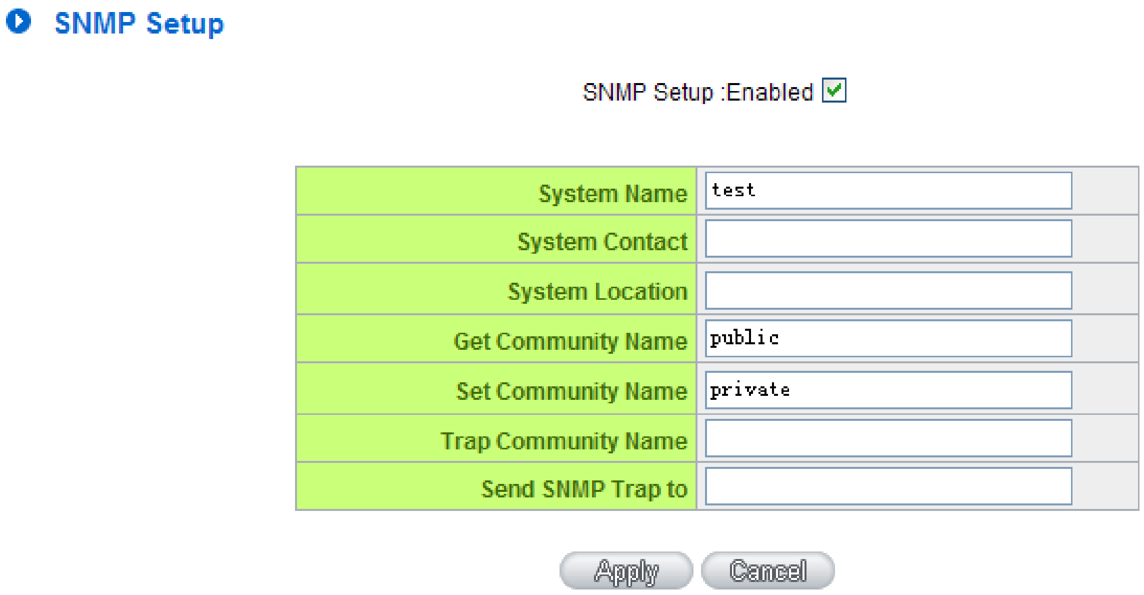
This feature allows users to integrate all backup content of parameter settings into the device. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to import the file.

Export Configuration File:

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

11.4 SNMP

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



SNMP Setup

SNMP Setup :Enabled ☑

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

Enabled: Activate SNMP feature. The default is activated.

System Name: Set the name of the device such as Qno.

System Contact: Set the name of the person who manages the device (i.e. John).

System Location: Define the location of the device (i.e. Taipei).

Get Community Name: Set the name of the group or community that can view the device SNMP data. The default setting is "Public".

Set Community Name: Set the name of the group or community that can receive the device SNMP data. The default setting is "Private".

Trap Community Name: Set user parameters (password required by the Trap-receiving host computer) to receive Trap message.

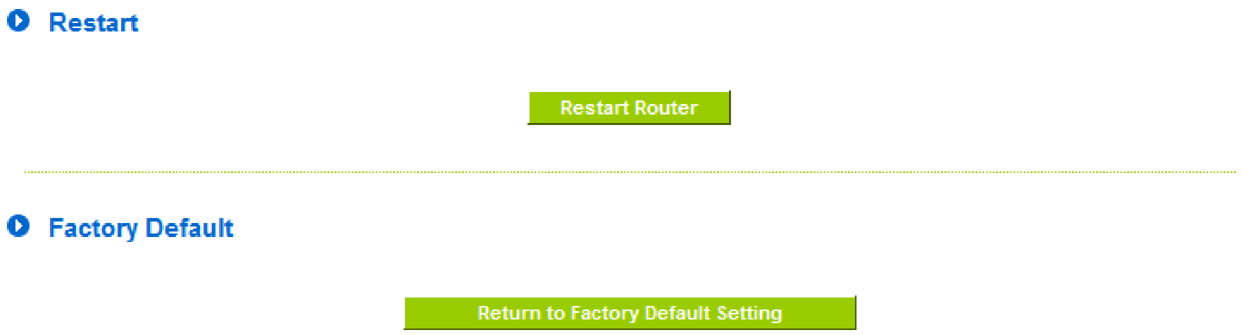
Send SNMP Trap to: Set one IP address or Domain Name for the Trap-receiving host computer.

Apply: Press **“Apply”** to save the settings.

Cancel: Press **“Cancel”** to keep the settings unchanged.

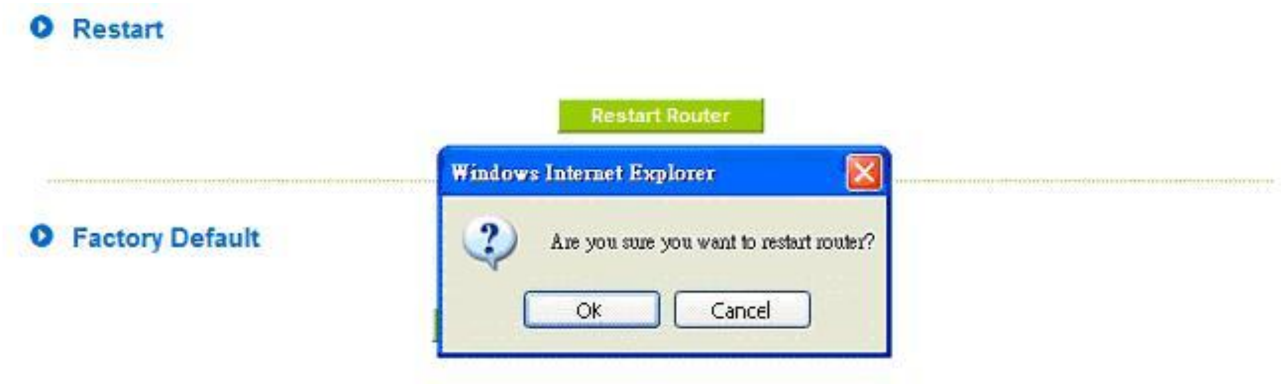
11.5 System Recover

Users can restart the device with System Recover button.



Restart

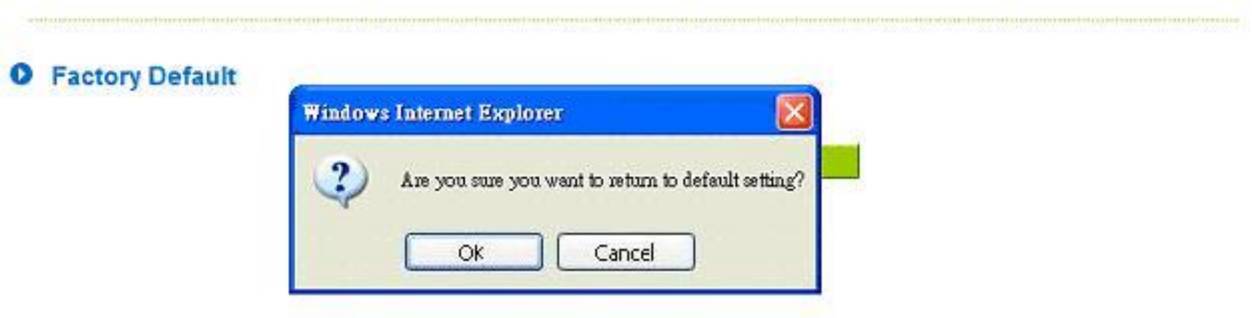
As the figure below, if clicking “Restart Router” button, the dialog block will pop out, confirming if users would like to restart the device.



Are you sure you want to restart router?

Return to Factory Default Setting

If clicking “Return to Factory Default Setting, the dialog block will pop out, if the device will return to factory default.



Factory Default

Windows Internet Explorer

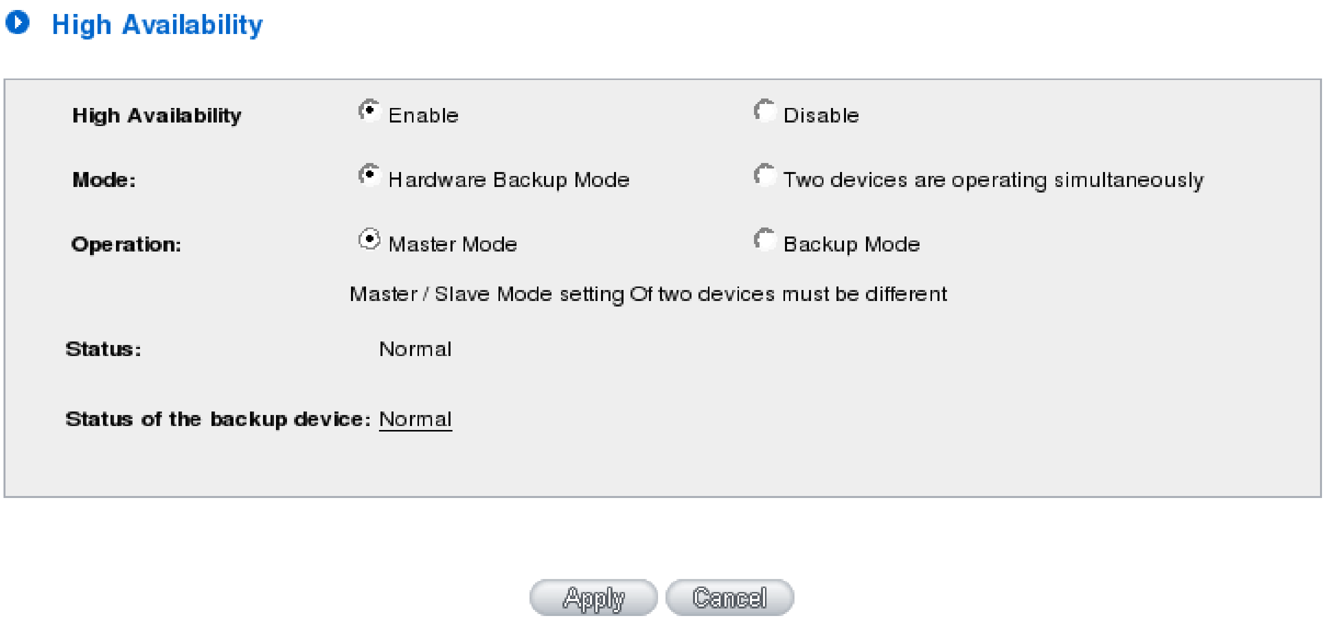
Are you sure you want to return to default setting?

It’s recommended to save the current configuration before upgrading firmware. After firmware upgraded, import the configuration file after returning to factory default to ensure system stable. (Please refer to 12.3)

11.6 High Availability

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

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



High Availability

High Availability: ● Enable ○ Disable

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

Operation: ● Master Mode ○ Backup Mode

Master / Slave Mode setting Of two devices must be different

Status: Normal

Status of the backup device: Normal

High Availability Enable: Activate HA function.

Disable: Disable HA function.

Mode (1) Hardware Backup Mode

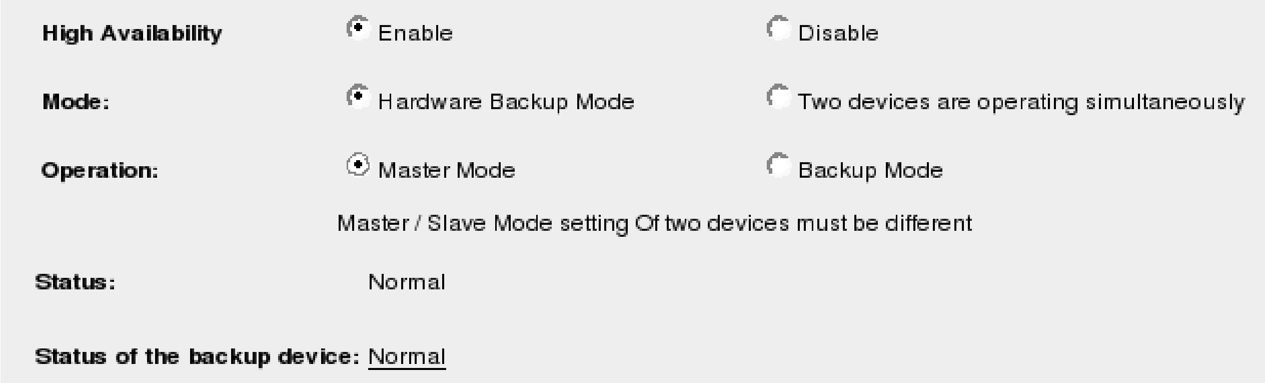
It is the general backup mode. The master device takes responsibility of network transmitting and the other one is set as idle. When the master device fails transmitting, it will send out the message to the idle device for taking over network transmitting immediately.

(2) Two devices are operating simultaneously

Two devices operate outbound linking simultaneously, but they are still separated as Master device and Backup device. In normal situation, Master device is major DHCP IP issuer, and Backup device will disable DHCP issuing automatically. When Master device fails transmitting, the Backup device will take over all outbound links and enable DHCP server to provide IP addresses.

Following is the description of the two different modes.

Hardware Backup



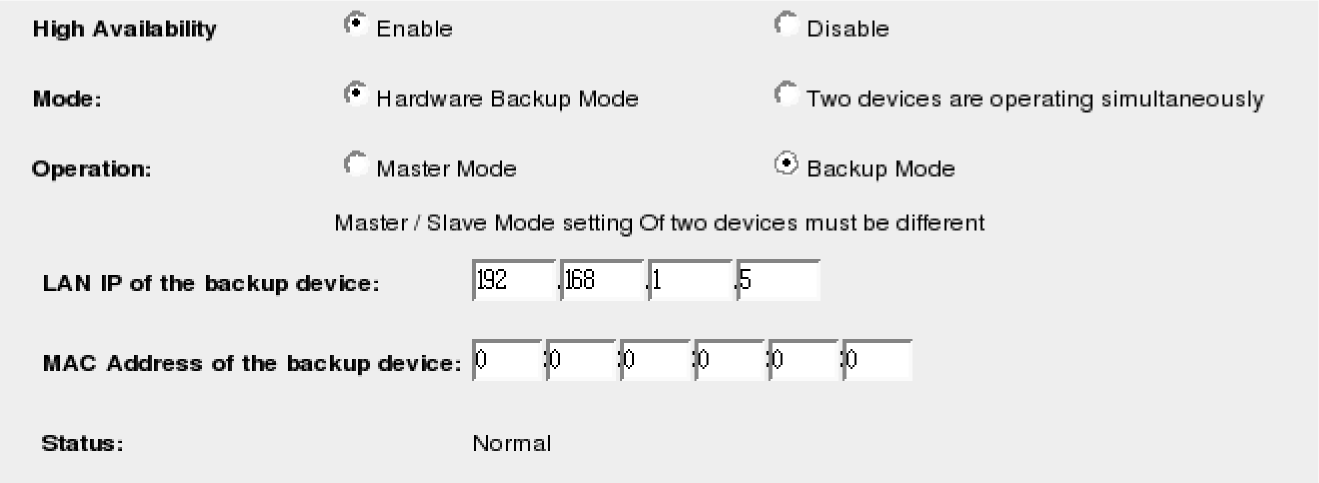
High Availability	● Enable	○ Disable
Mode:	● Hardware Backup Mode	○ Two devices are operating simultaneously
Operation:	● Master Mode	○ Backup Mode
	Master / Slave Mode setting Of two devices must be different	
Status:	Normal	
Status of the backup device:	Normal	

※ Operation-Master Mode Indicates the master device will operate for all outbound links. When the master device fails transmitting, the backup device will take over.

Status “Status- Normal” indicates the device operates well.

Status of the backup device Indicates status of backup device. If the status is normal, administrators can login the device remotely to manage. (Remote Management should be enabled).

“Status- Abnormal” indicates the backup device can not be detected or does exist, and need to inspect the backup device actual status.



High Availability	● Enable	○ Disable
Mode:	● Hardware Backup Mode	○ Two devices are operating simultaneously
Operation:	○ Master Mode	● Backup Mode
	Master / Slave Mode setting Of two devices must be different	
LAN IP of the backup device:	192 . 168 . 1 . 5	
MAC Address of the backup device:	0 : 0 : 0 : 0 : 0 : 0	
Status:	Normal	

Operation-Backup Mode Indicates the backup device will take over when the master fails transmitting. WAN and LAN IP setting in backup device should be the same as those of master device. The backup device should not be in charge of network transmitting and DHCP server.

※ If the original LAN IP addresses are issued by Master device, DHCP server setting of Backup device should be the same as Master device. The Backup device can keep DHCP functioning and there will be no LAN disconnection.

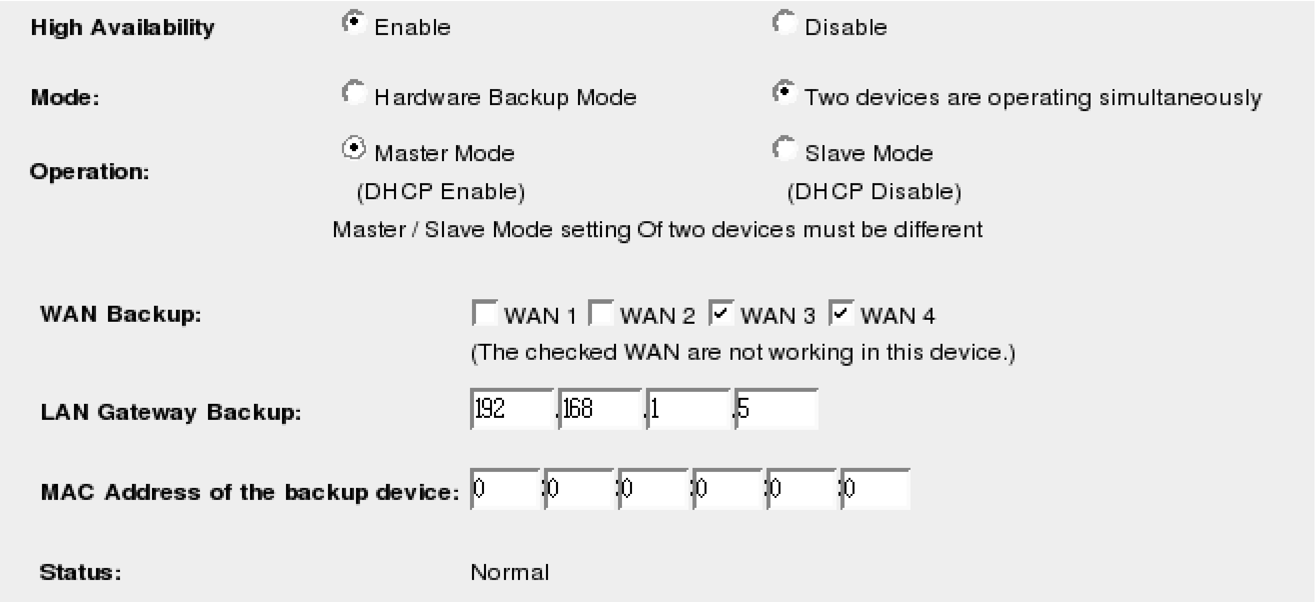
LAN IP of the backup device Input LAN IP of Master mode, which is backed up.

MAC Address of the backup device: Input Master device MAC address, which is backed up.

Status "Status- Normal" indicates the status is idle. Master device operates normally.

"Status- Backup" indicates the device takes over all the network transmitting. The status will return to "Normal" when Master device boots normally and send a message to the backup device. Then, the status will return to Normal, which the backup device remains idle.

Two devices are operating simultaneously:



High Availability	● Enable	○ Disable
Mode:	○ Hardware Backup Mode	● Two devices are operating simultaneously
Operation:	● Master Mode (DHCP Enable)	○ Slave Mode (DHCP Disable)
	Master / Slave Mode setting Of two devices must be different	
WAN Backup:	□ WAN 1 □ WAN 2 ☑ WAN 3 ☑ WAN 4 (The checked WAN are not working in this device.)	
LAN Gateway Backup:	192 .168 .1 .5	
MAC Address of the backup device:	0 :0 :0 :0 :0 :0	
Status:	Normal	

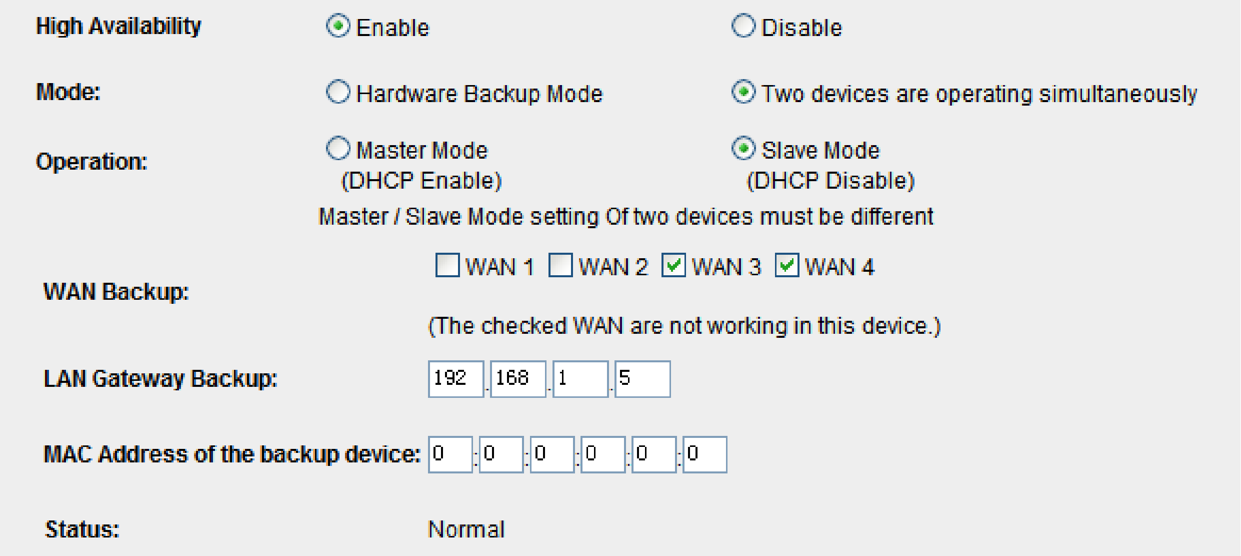
Operation-Master Mode Besides operating network with another device, Master device is also the DHCP server to issue LAN IP addresses. Although Slave device also supports outbound linking, its DHCP server is disabled.

WAN Backup (The Checked WANs are not working in this device.) The checked WANs will works in the other device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in the other device, WAN3 and WAN4 should be checked.

LAN Gateway Backup Input LAN IP of Slave device. The IP should be different from LAN IP of Master device.

MAC Address of the backup device Input LAN MAC of Slave device. It should be different from LAN MAC of Master device.

Status "Status-Normal" means both two devices operate normally.
"Status-Backup" indicates Slave mode has problems, and the device enables backup to take over WAN



High Availability	● Enable	○ Disable
Mode:	○ Hardware Backup Mode	● Two devices are operating simultaneously
Operation:	○ Master Mode (DHCP Enable)	● Slave Mode (DHCP Disable)
	Master / Slave Mode setting Of two devices must be different	
WAN Backup:	□ WAN 1 □ WAN 2 ☑ WAN 3 ☑ WAN 4 (The checked WAN are not working in this device.)	
LAN Gateway Backup:	192 . 168 . 1 . 5	
MAC Address of the backup device:	0 : 0 : 0 : 0 : 0 : 0	
Status:	Normal	

Operation-Slave Mode

Although working with master device, Backup device's DHCP server is disabled. LAN users need to transmit traffic through the WAN on Slave device. You should add LAN IP of Slave device into Master device DHCP server default gateway, which is DHCP server IP address.

For example, if the DHCP server's IP of Master device is 192.168.1.1, and the subnet mask is 255.255.255.0, Salve device should be in the same subnet, ex. 192.168.1.2.

WAN Backup (The Checked WANs are not working in this device.)

The checked WANs will works in another device. For an example, if WAN1 and WAN2 work in this device, and WAN3 and WAN4 work in another, WAN3 and WAN4 should be checked.

LAN Gateway Backup

Input the LAN IP of Master device. It should be different from Slave device's IP. (Must be in the same subnet.)

MAC Address of the backup device

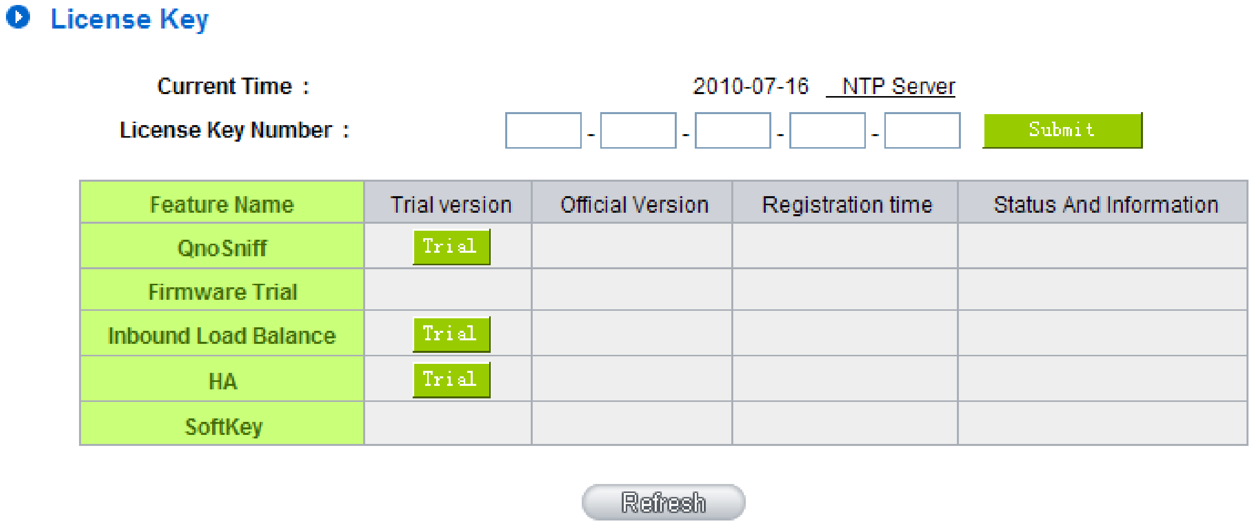
Input the LAN MAC of Master device. It should be different from Salve device's LAN MAC.

Status

"Status-Normal" indicates both devices work normally; "Status-Backup" indicates the Backup device is enabled for backing up Master device to take over WAN connection and DHCP issuing function.

11.7 License Key

Users have to purchase License Key to “enable” some functions in Qno Firwalls/Routers series or upgrade to “Official Version”(not trial version), such as QnoSniff or Inbound Load Balance, etc.



License Key

Current Time : 2010-07-16 NTP Server

License Key Number : □ - □ - □ - □ - □ Submit

Feature Name	Trial version	Official Version	Registration time	Status And Information
Qno Sniff	Trial			
Firmware Trial				
Inbound Load Balance	Trial			
HA	Trial			
SoftKey				

Refresh

Current Time: Before inputing License Key, the device will check whether current time is correct and whether License Key is still in valid period. In order to prevent from dysfuction problems, we strongly recommend you to check and update the time correctly before attempting a feature and entering License Key.

License Key Number: Input License Key you purchase. Generally the key is composed by several alphanumeric characters. Enter the key and click “Submit”, and the system will check whether the License Key is valid. If the key is valid, users will be allowed to use the feature. The “Official Version” column of that feature will be checked.

Feature Name: List value-added features. If there is no “Trial Version” button in the “Trial Version” column, it means the feature has no trail version, or it just supports the amount of VPN tunnels, such as QnoSoftKey.

Trial Version / Official Version: Display “Trial” button in the “Trial Version” column at default if the functions have trial versions. Users can try the functions for certain period of time by pressing the button.

After entering and registering License Key successfully,“Official Version”column will be checked. The feature will be in official version and not be limited by trial expiration date.

Registration Time: Display successfully inputted and registered time.

Status Information: Indicate remaining trial date or supported amount of QnoSoftkey VPN Tunnels.

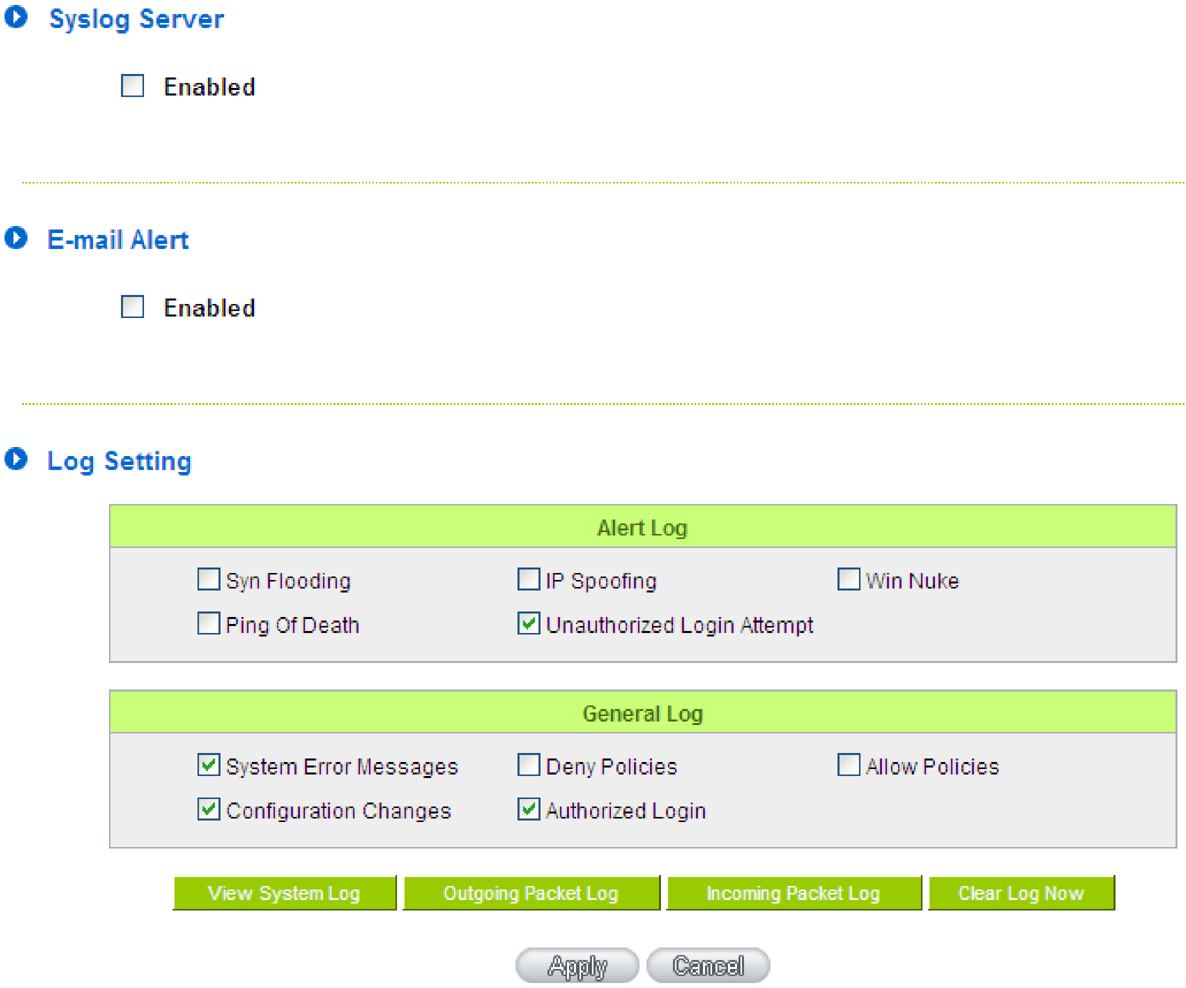
Refresh: Refresh current system status and time.

XII. Log

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

12.1 System Log

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



Syslog Server

□ Enabled

E-mail Alert

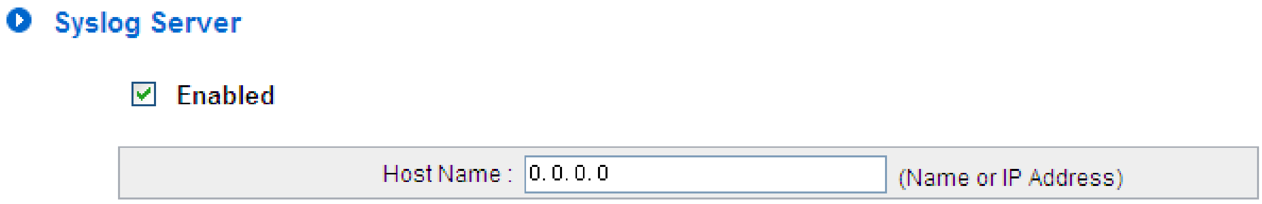
□ Enabled

Log Setting

Alert Log		
□ Syn Flooding	□ IP Spoofing	□ Win Nuke
□ Ping Of Death	☑ Unauthorized Login Attempt	

General Log		
☑ System Error Messages	□ Deny Policies	□ Allow Policies
☑ Configuration Changes	☑ Authorized Login	

System Log



Syslog Server

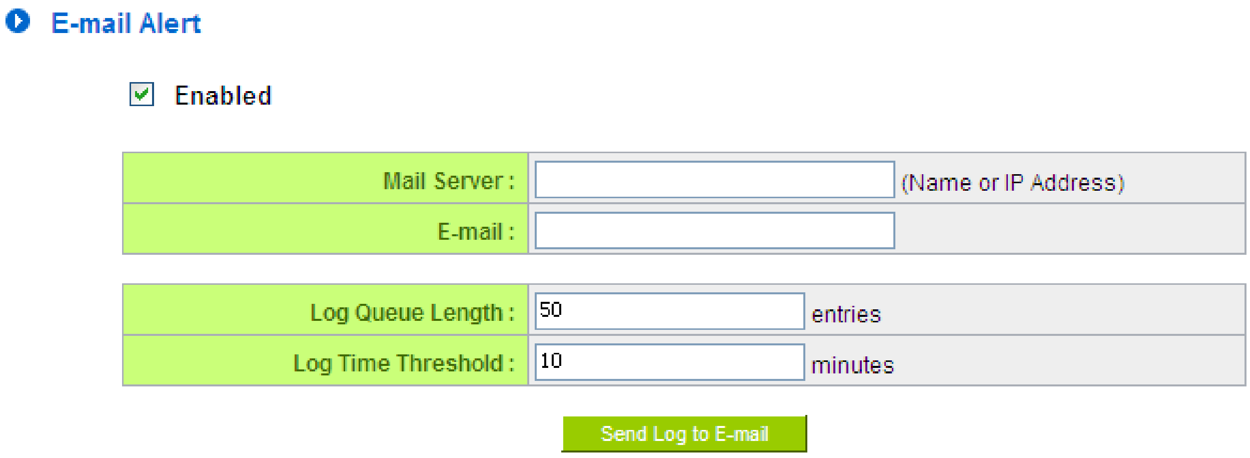
☑ Enabled

Host Name : 0.0.0.0 (Name or IP Address)

Enabled: If this option is selected, the System Log feature will be enabled.

Host Name: The device provides external system log servers with log collection feature. System log is an industrial standard communications protocol. It is designed to dynamically capture related system message from the network. The system log provides the source and the destination IP addresses during the connection, service number, and type. To apply this feature, enter the system log server name or the IP address into the empty "system log server" field.

E-mail Alert(Future Feature)



E-mail Alert

☑ Enabled

Mail Server :		(Name or IP Address)
E-mail :		

Log Queue Length :	50	entries
Log Time Threshold :	10	minutes

Enabled: If this option is selected, E-mail Warning will be enabled.

Mail Server: If users wish to send out all the logs, please enter the E-mail server name or the IP address; for instance, mail.abc.com .

E- mail: This is set as system log recipient email address such as abc@mail.abc.com.

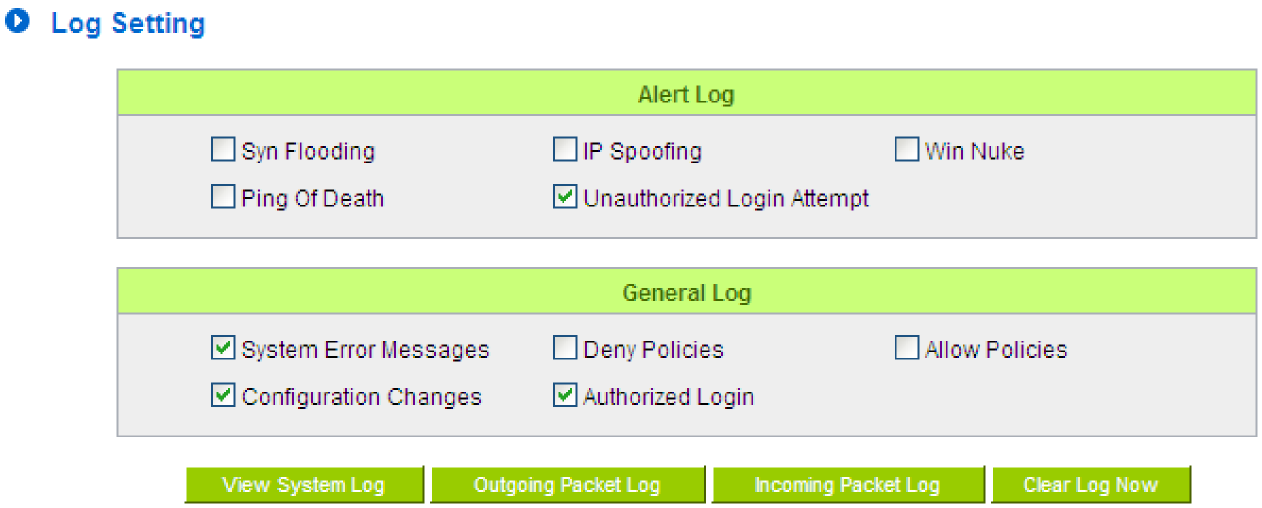
Log Queue Length: Set the number of Log entries, and the default entry number is 50. When this defined number is reached, it will automatically send out the log mail.

Log Time Threshold: Set the interval of sending the log, and the default is set to 10 minutes. Reaching this defined number, it will automatically send out the Mail log.

The device will detect which parameter (either entries or intervals) reaches the threshold first and send the log message of that parameter to the user.

Send Log to E- mail: Users may send out the log right away by pressing this button.

Log Setting



Log Setting

Alert Log		
□ Syn Flooding	□ IP Spoofing	□ Win Nuke
□ Ping Of Death	☑ Unauthorized Login Attempt	

General Log		
☑ System Error Messages	□ Deny Policies	□ Allow Policies
☑ Configuration Changes	☑ Authorized Login	

Alert Log

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

Syn Flooding: Bulky syn packet transmission in a short time causes the overload of the system storage of record in connection information.

IP Spoofing: Through the packet sniffing, hackers intercept data transmitted on the network. After they access the information, the IP address from the sender is changed so that they can access the resource in the source system.

Win Nuke: Servers are attacked or trapped by the Trojan program.

Ping of Death: The system fails because the sent data exceeds the maximum packet that can be handled by the IP protocol.

Unauthorized Login: If intruders into the device are identified, the message will be sent to the system log.

General Log

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

System Error Message: Provides the system log with all kinds of error messages. For example, wrong settings, occurrence of abnormal functions, system reactivation, disconnection of PPPoE and so on.

Deny Policies: If remote users fail to enter the system because of the access rules; for instance, message will be recorded in the system log.

Allow Policies: If remote users enter the system because of compliance with access rules; for instance, message will be recorded in the system log.

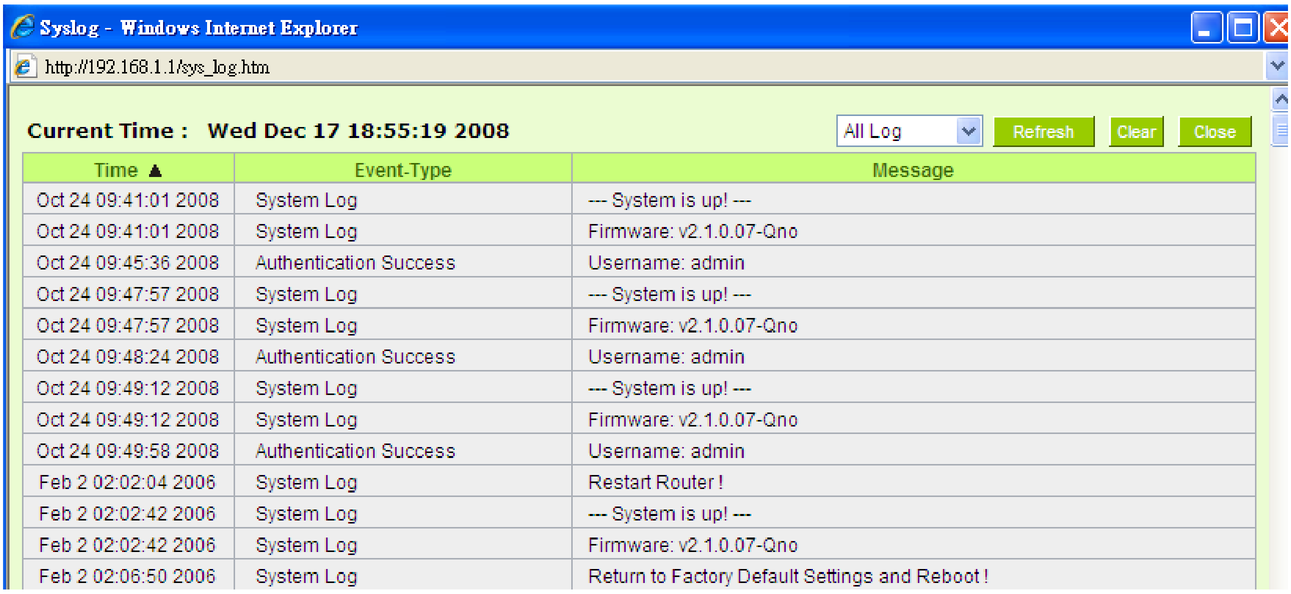
Configuration Change: When the system settings are changed, this message will be sent back to the system log.

Authorized Login: Successful entry into the system includes login from the remote end or from the LAN into this device. These messages will be recorded in the system log.

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

View System Log:

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



Syslog - Windows Internet Explorer
http://192.168.1.1/sys_log.htm

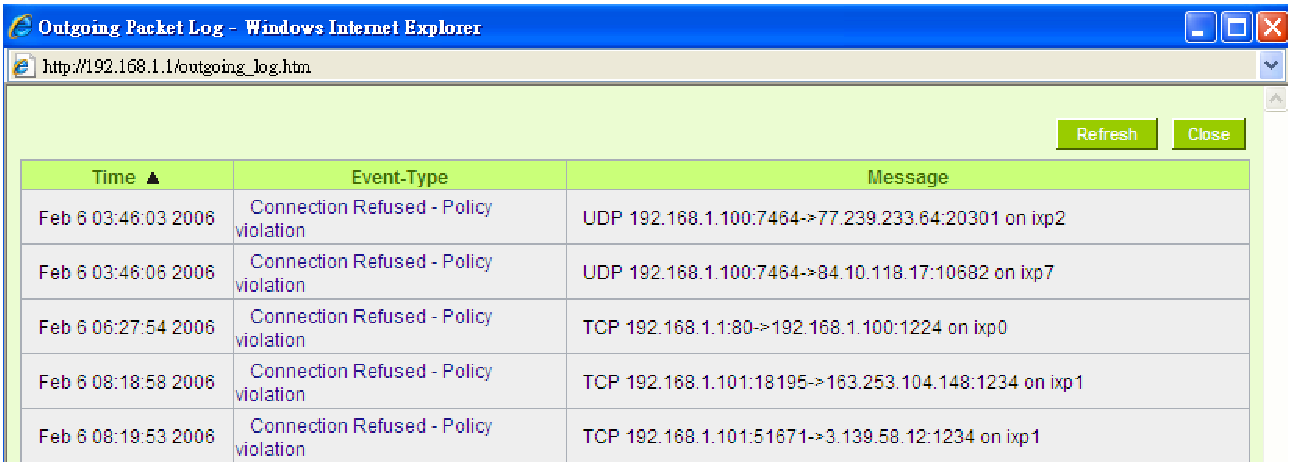
Current Time : Wed Dec 17 18:55:19 2008

All Log
Refresh
Clear
Close

Time ▲	Event-Type	Message
Oct 24 09:41:01 2008	System Log	--- System is up! ---
Oct 24 09:41:01 2008	System Log	Firmware: v2.1.0.07-Qno
Oct 24 09:45:36 2008	Authentication Success	Username: admin
Oct 24 09:47:57 2008	System Log	--- System is up! ---
Oct 24 09:47:57 2008	System Log	Firmware: v2.1.0.07-Qno
Oct 24 09:48:24 2008	Authentication Success	Username: admin
Oct 24 09:49:12 2008	System Log	--- System is up! ---
Oct 24 09:49:12 2008	System Log	Firmware: v2.1.0.07-Qno
Oct 24 09:49:58 2008	Authentication Success	Username: admin
Feb 2 02:02:04 2006	System Log	Restart Router !
Feb 2 02:02:42 2006	System Log	--- System is up! ---
Feb 2 02:02:42 2006	System Log	Firmware: v2.1.0.07-Qno
Feb 2 02:06:50 2006	System Log	Return to Factory Default Settings and Reboot !

Outgoing Packet Log:

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

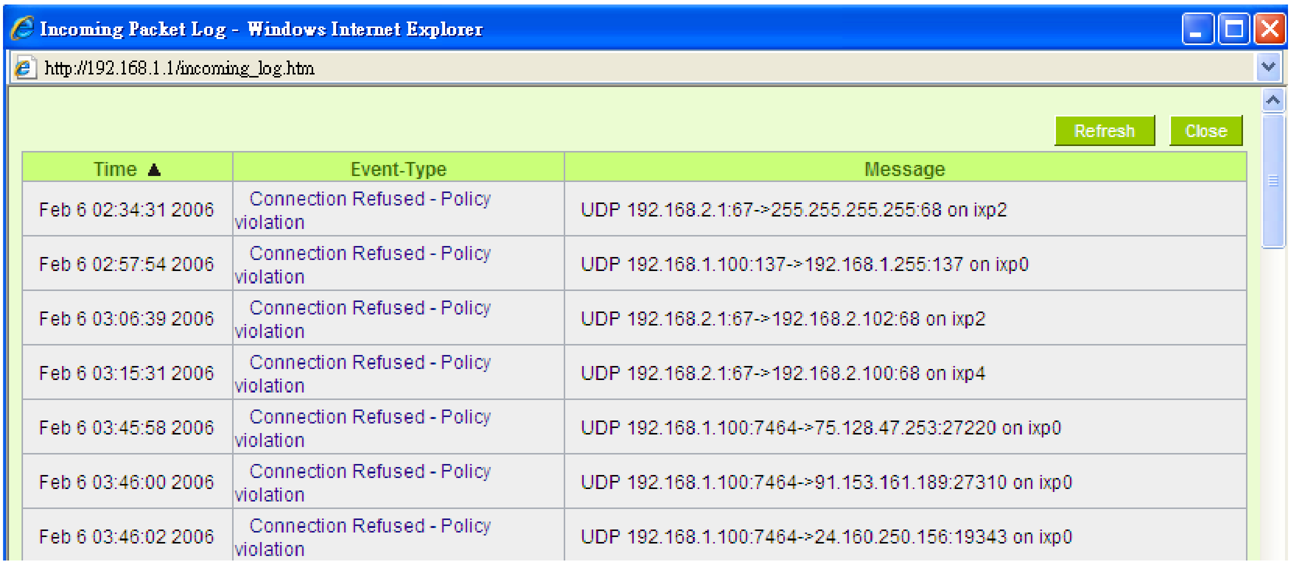


Outgoing Packet Log - Windows Internet Explorer
http://192.168.1.1/outgoing_log.htm
Refresh
Close

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

Incoming Packet Log:

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


Incoming Packet Log - Windows Internet Explorer
http://192.168.1.1/incoming_log.htm
Refresh
Close

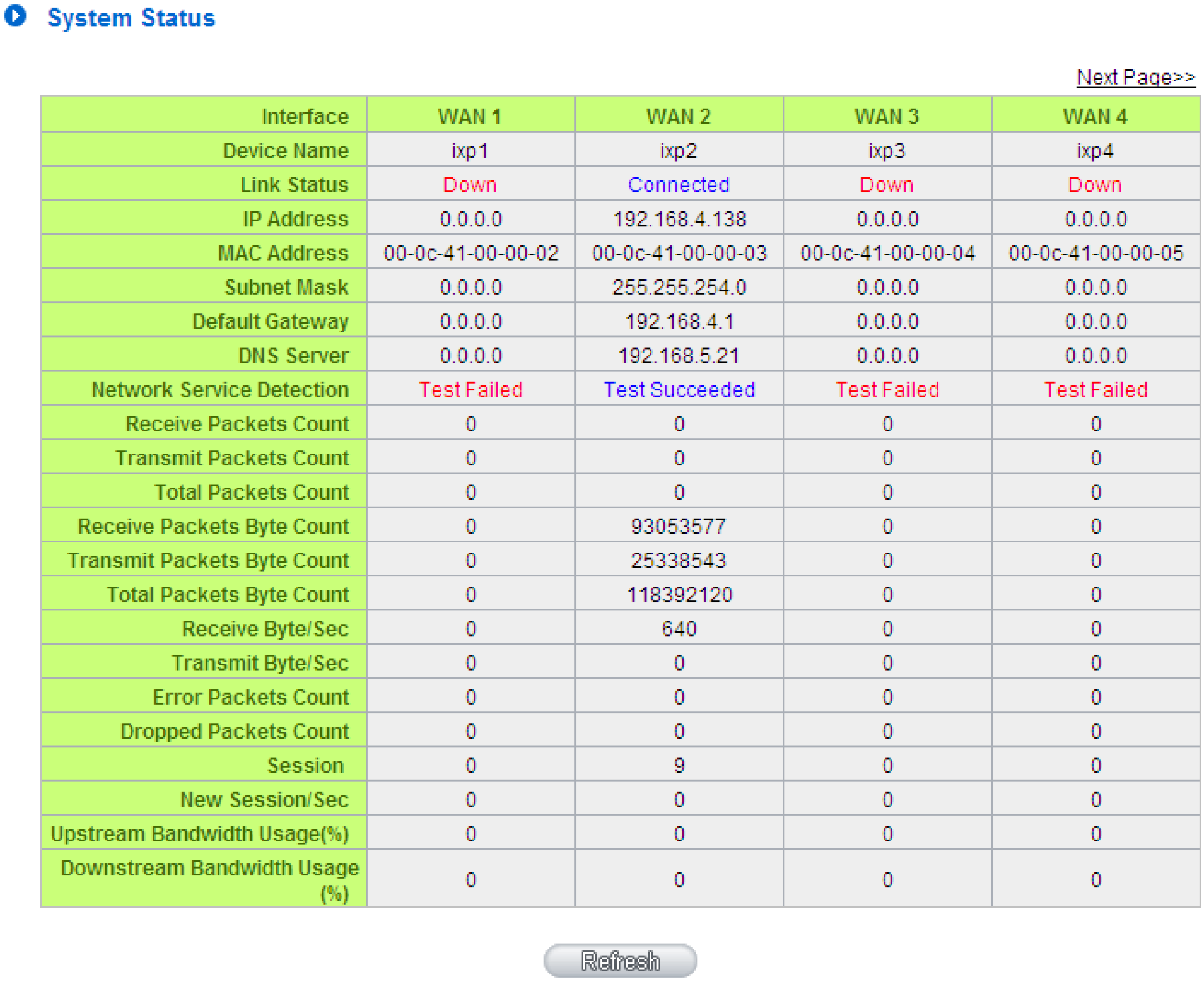
Time ▲	Event-Type	Message
Feb 6 02:34:31 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->255.255.255.255:68 on ixp2
Feb 6 02:57:54 2006	Connection Refused - Policy violation	UDP 192.168.1.100:137->192.168.1.255:137 on ixp0
Feb 6 03:06:39 2006	Connection Refused - Policy violation	UDP 192.168.2.1:67->192.168.2.102:68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

Clear Log Now:

This feature clears all the current information on the log.

12.2 System Statistic

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



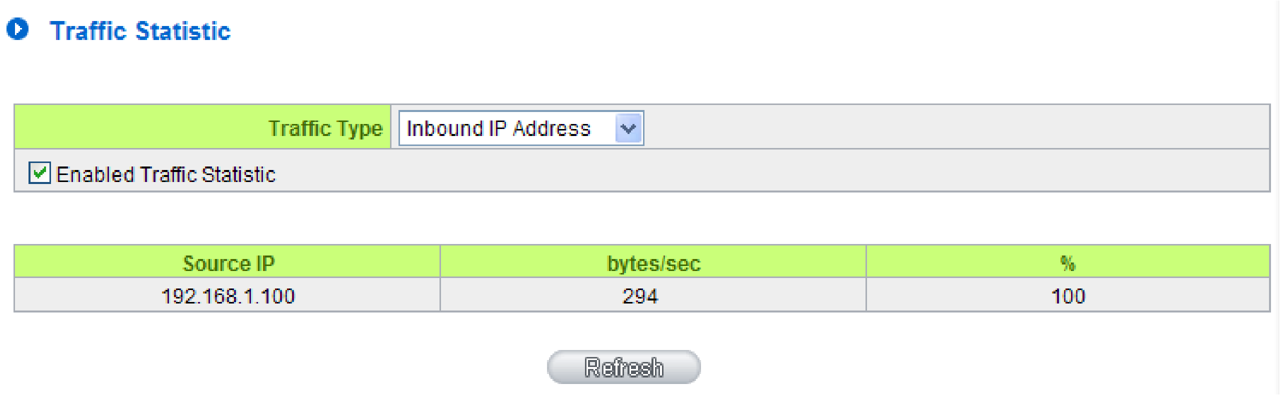
System Status

Next Page>>

Interface	WAN 1	WAN 2	WAN 3	WAN 4
Device Name	ixp1	ixp2	ixp3	ixp4
Link Status	Down	Connected	Down	Down
IP Address	0.0.0.0	192.168.4.138	0.0.0.0	0.0.0.0
MAC Address	00-0c-41-00-00-02	00-0c-41-00-00-03	00-0c-41-00-00-04	00-0c-41-00-00-05
Subnet Mask	0.0.0.0	255.255.254.0	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	192.168.4.1	0.0.0.0	0.0.0.0
DNS Server	0.0.0.0	192.168.5.21	0.0.0.0	0.0.0.0
Network Service Detection	Test Failed	Test Succeeded	Test Failed	Test Failed
Receive Packets Count	0	0	0	0
Transmit Packets Count	0	0	0	0
Total Packets Count	0	0	0	0
Receive Packets Byte Count	0	93053577	0	0
Transmit Packets Byte Count	0	25338543	0	0
Total Packets Byte Count	0	118392120	0	0
Receive Byte/Sec	0	640	0	0
Transmit Byte/Sec	0	0	0	0
Error Packets Count	0	0	0	0
Dropped Packets Count	0	0	0	0
Session	0	9	0	0
New Session/Sec	0	0	0	0
Upstream Bandwidth Usage(%)	0	0	0	0
Downstream Bandwidth Usage (%)	0	0	0	0

12.3 Traffic Statistic

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



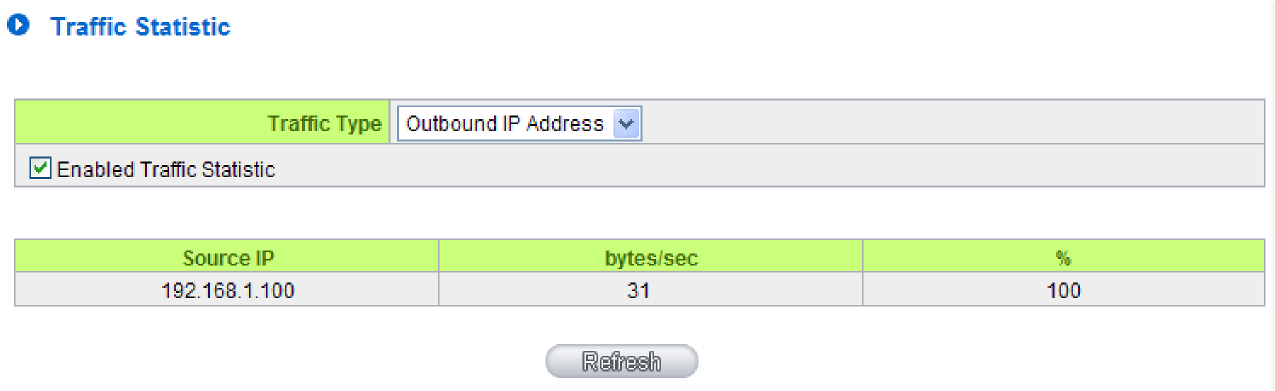
Traffic Statistic

Traffic Type	Inbound IP Address
☑ Enabled Traffic Statistic	

Source IP	bytes/sec	%
192.168.1.100	294	100

By Inbound IP Address:

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



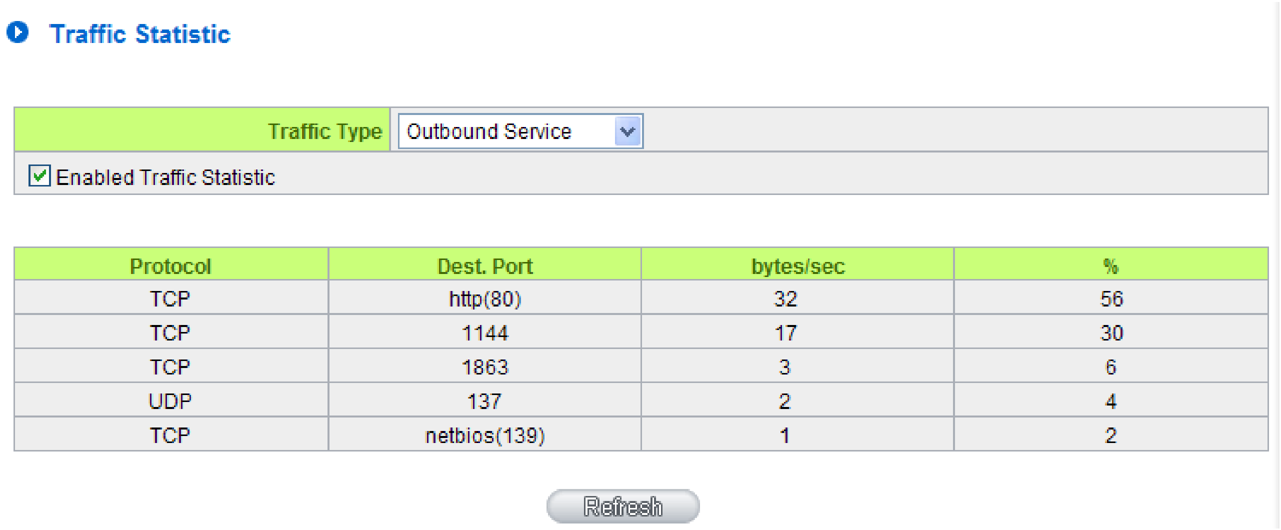
Traffic Statistic

Traffic Type	Outbound IP Address
☑ Enabled Traffic Statistic	

Source IP	bytes/sec	%
192.168.1.100	31	100

By outbound IP Address:

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



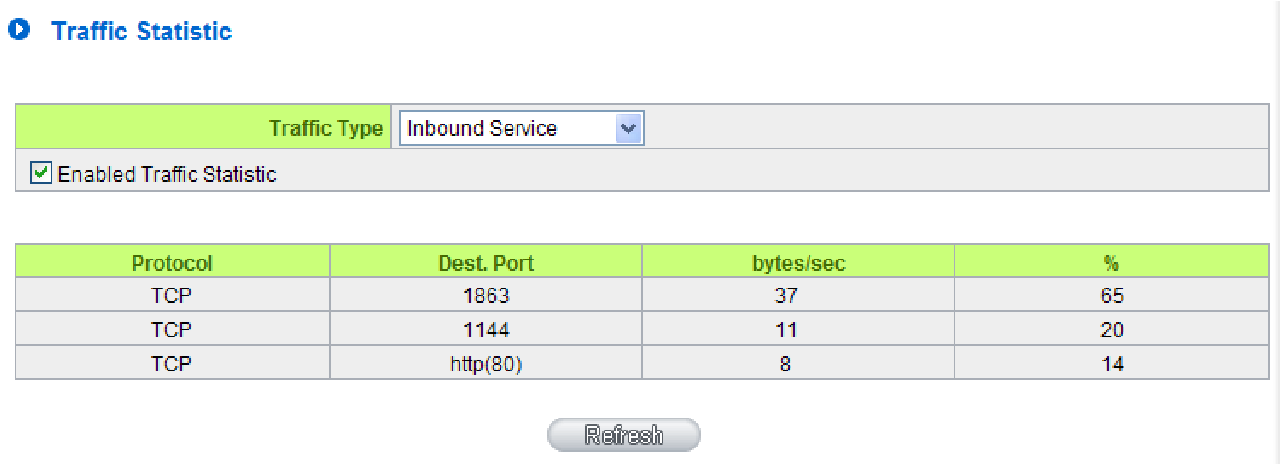
Traffic Statistic

Traffic Type	Outbound Service
☑ Enabled Traffic Statistic	

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

By Outbound Port:

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



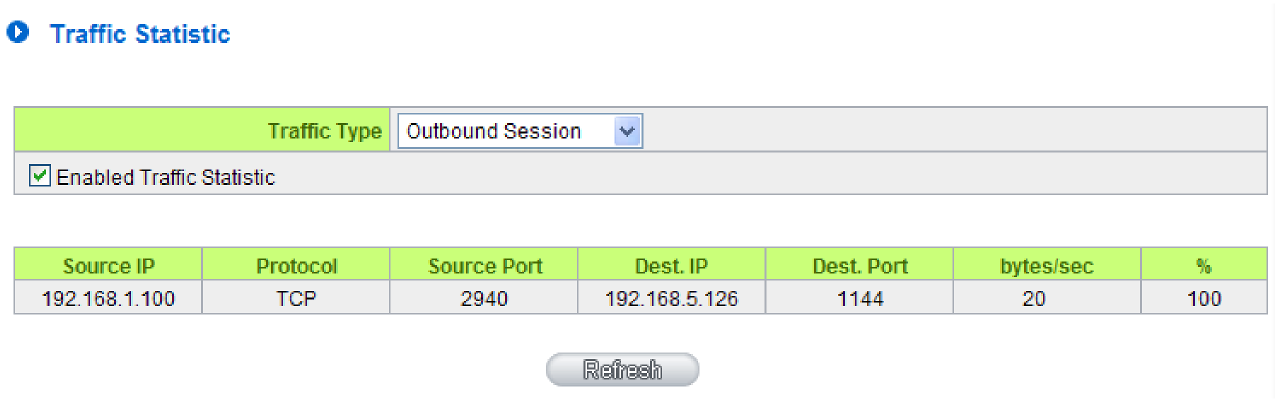
Traffic Statistic

Traffic Type	Inbound Service
☑ Enabled Traffic Statistic	

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

By Inbound Port:

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



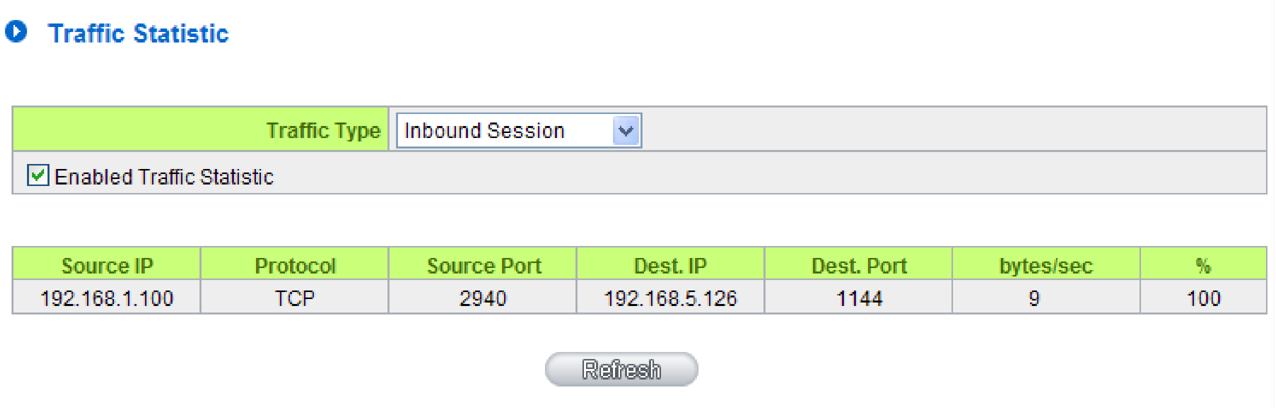
Traffic Statistic

Traffic Type	Outbound Session
☑ Enabled Traffic Statistic	

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2940	192.168.5.126	1144	20	100

By Outbound Session:

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



Traffic Statistic

Traffic Type	Inbound Session
☑ Enabled Traffic Statistic	

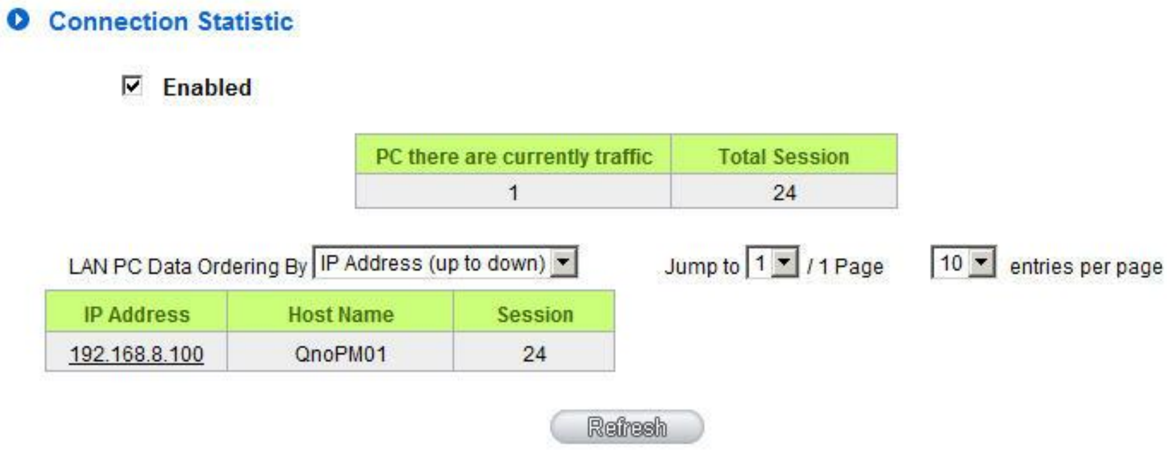
Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2940	192.168.5.126	1144	9	100

By Inbound Session:

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

12.4 Connection Statistic **(Future Feature)**

Connection Statistic function is used to record the numbers of network connections, including outbound sessions, and intranet users (PC). It also displays the user connection sessions.



Connection Statistic

☑ Enabled

PC there are currently traffic	Total Session
1	24

LAN PC Data Ordering By: IP Address (up to down)   Jump to 1 / 1 Page   10 entries per page

IP Address	Host Name	Session
192.168.8.100	QnoPM01	24

Enable: When enabling Connection Statistic function, parts of system efficiency will be influenced. Therefore, the system will remind you the influence when you enable this function.

PC there are currently traffic: Display current PC amounts having outbound connections. If the PC does not boot up or is not connected to internet, it will not be counted in the statistic.

LAN PC Data Ordering By: Select this function to sort the data by [IP Address up to down], [IP Address down to up], [Session down to up], and [Session up to down].

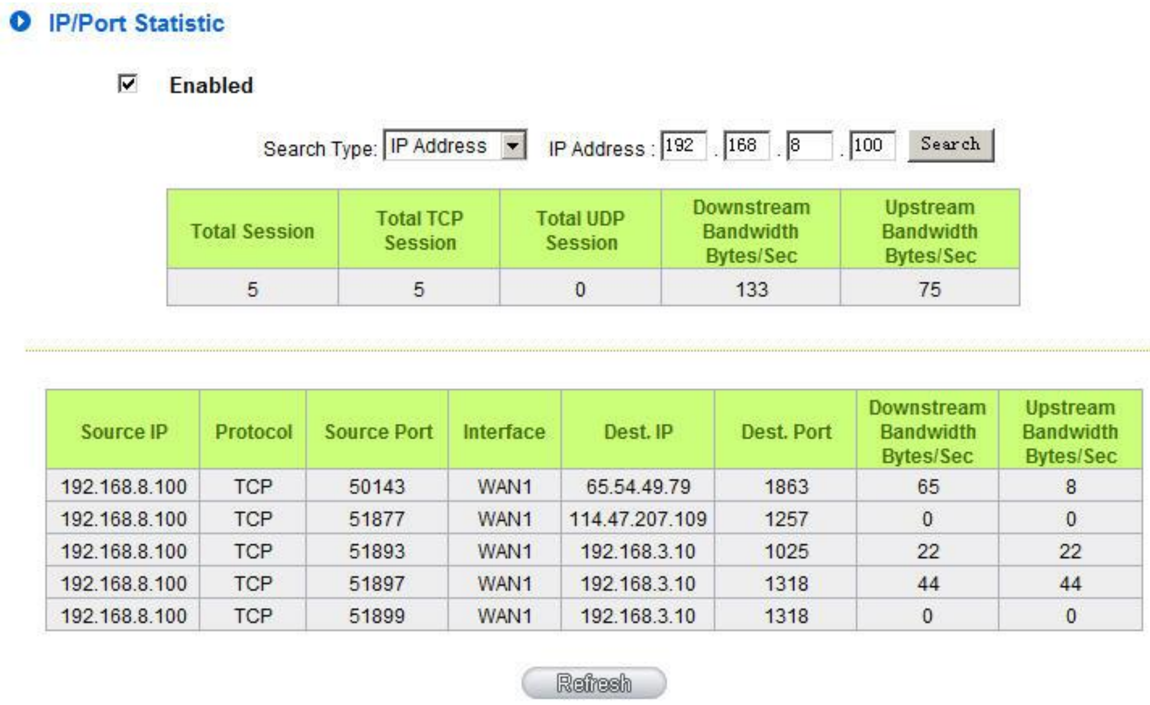
Jump to___/___Page；

Entries per page___

Select this function to display the data by how many entries of data per page will be displayed. Also you can select the page you would like to see from the drop down menu.

Data List field

IP Address: Display PC's IP address which has outbound traffic. Also you can click the IP hyperlink to display the current connection statistic and details.(As the following graph):



IP/Port Statistic

☑ Enabled

Search Type: IP Address ▼ IP Address : 192 . 168 . 8 . 100 Search

Total Session	Total TCP Session	Total UDP Session	Downstream Bandwidth Bytes/Sec	Upstream Bandwidth Bytes/Sec
5	5	0	133	75

Source IP	Protocol	Source Port	Interface	Dest. IP	Dest. Port	Downstream Bandwidth Bytes/Sec	Upstream Bandwidth Bytes/Sec
192.168.8.100	TCP	50143	WAN1	65.54.49.79	1863	65	8
192.168.8.100	TCP	51877	WAN1	114.47.207.109	1257	0	0
192.168.8.100	TCP	51893	WAN1	192.168.3.10	1025	22	22
192.168.8.100	TCP	51897	WAN1	192.168.3.10	1318	44	44
192.168.8.100	TCP	51899	WAN1	192.168.3.10	1318	0	0

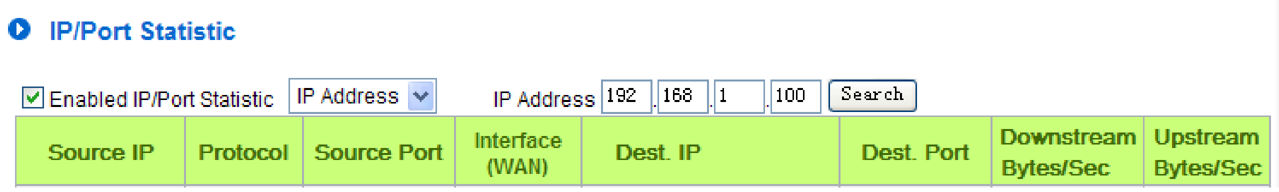
Host Name: Display PC names that having outbound traffic. It will show blank when the system cannot analyze.

Session: Display PC connection sessions that having outbound traffic.

Refresh: Click the Refresh button that the latest data and list will be updated.

12.5 IP/ Port Statistic

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



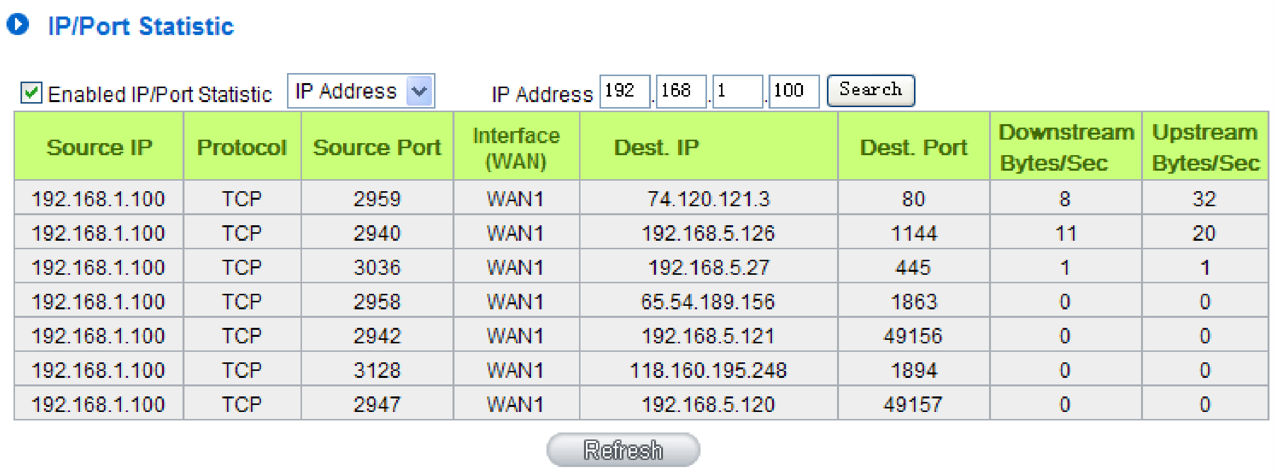
IP/Port Statistic

☑ Enabled IP/Port Statistic IP Address IP Address 192 . 168 . 1 . 100 Search

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

Specific IP Status：

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



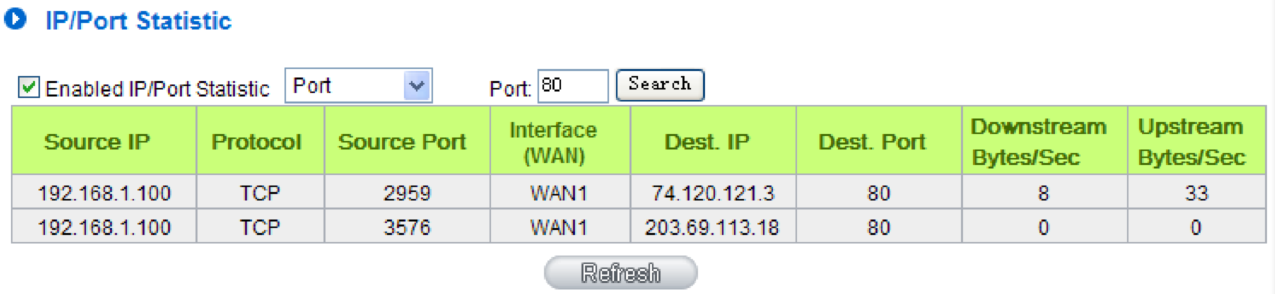
IP/Port Statistic

☑ Enabled IP/Port Statistic IP Address IP Address 192 . 168 . 1 . 100 Search

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

Specific Port Status：

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



IP/Port Statistic

☑ Enabled IP/Port Statistic Port Port: 80

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

12.6 QRTG (Qno Router Traffic Grapher)

QRTG utilizes dynamic GUI and simple statistic to display system status of Qno Firewall/ Router presently, including CPU Utilization(%), Memory Utilization(%), Session and WAN Traffic.

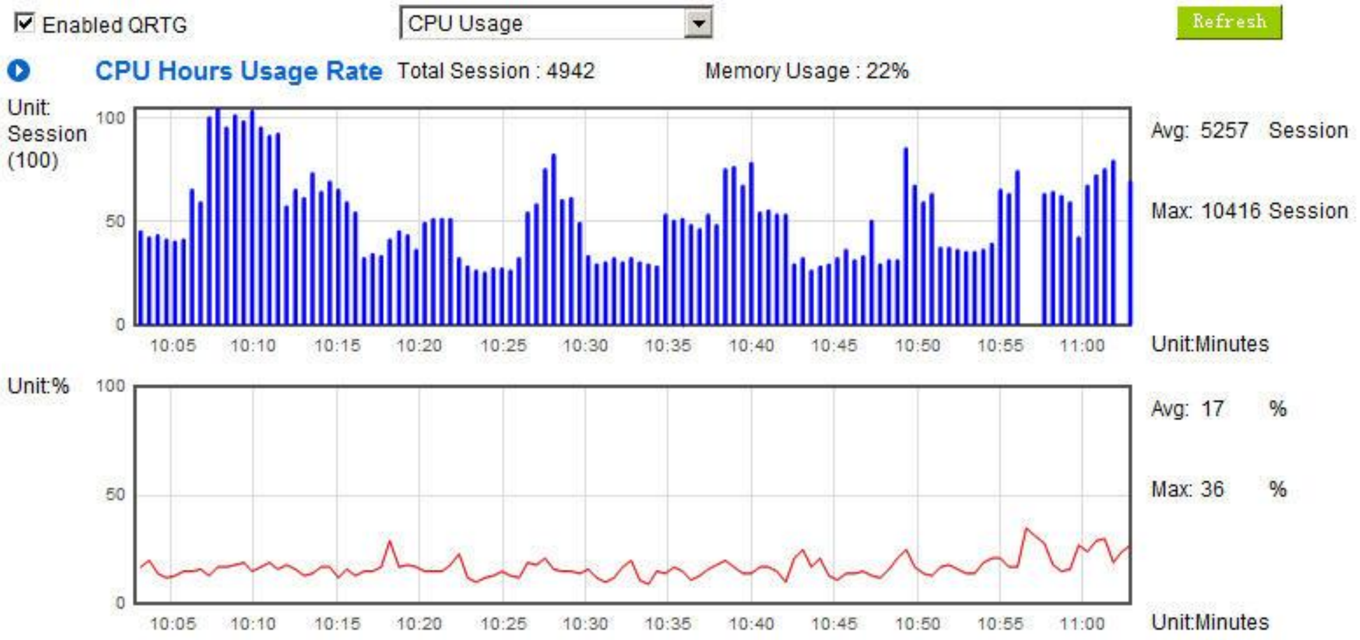
Enable QRTG: The funcation is disabled by default. When you are going to enable the QRTG function, system will pop-up a warning massage to remind you this function will be enabled, which may influence router efficiency. You can use drop down menu to select current status that including statistic and graphics of the following items when this function is enabled. System will refresh the statistic and graphics to latest data timing when you click "Refresh" button.

I. CPU Usage (As in the the following figure)

(1) CPU Hours Usage Rate graphic / average/ maximum

(2) CPU Days Usage Rate graphic / average/ maximum

(3) CPU, Week Usage Rate graphic / average/ maximum



☑ Enabled QRTG

CPU Usage

Refresh

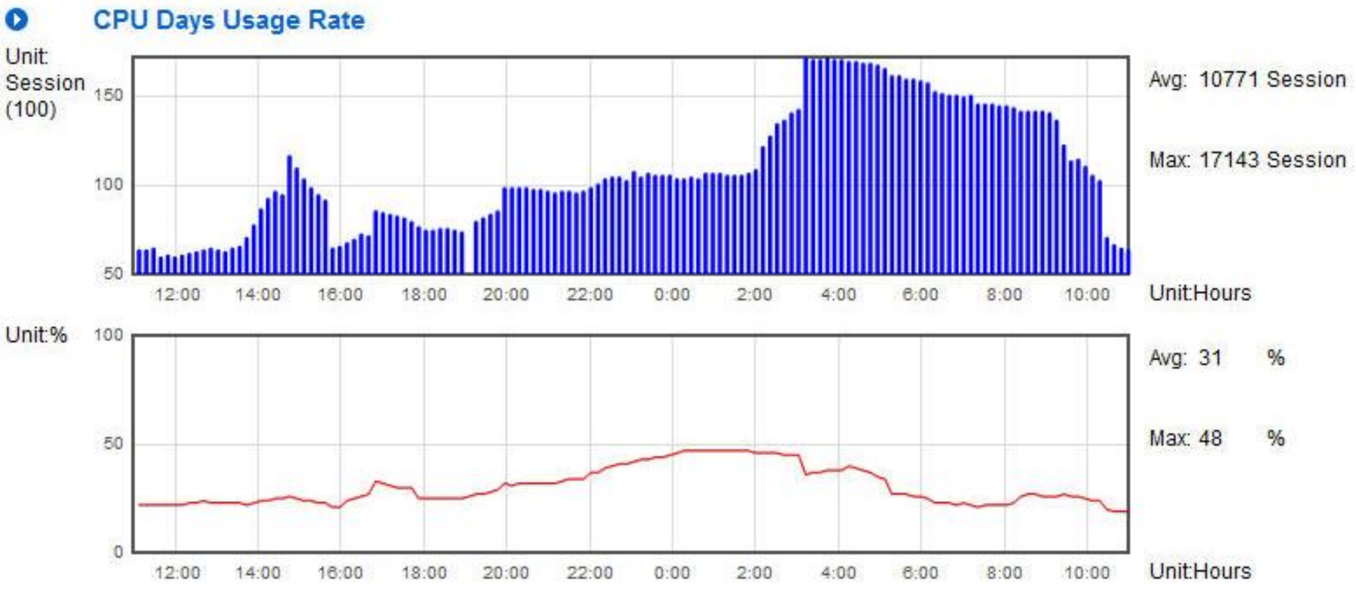
CPU Hours Usage Rate Total Session : 4942 Memory Usage : 22%

Avg: 5257 Session

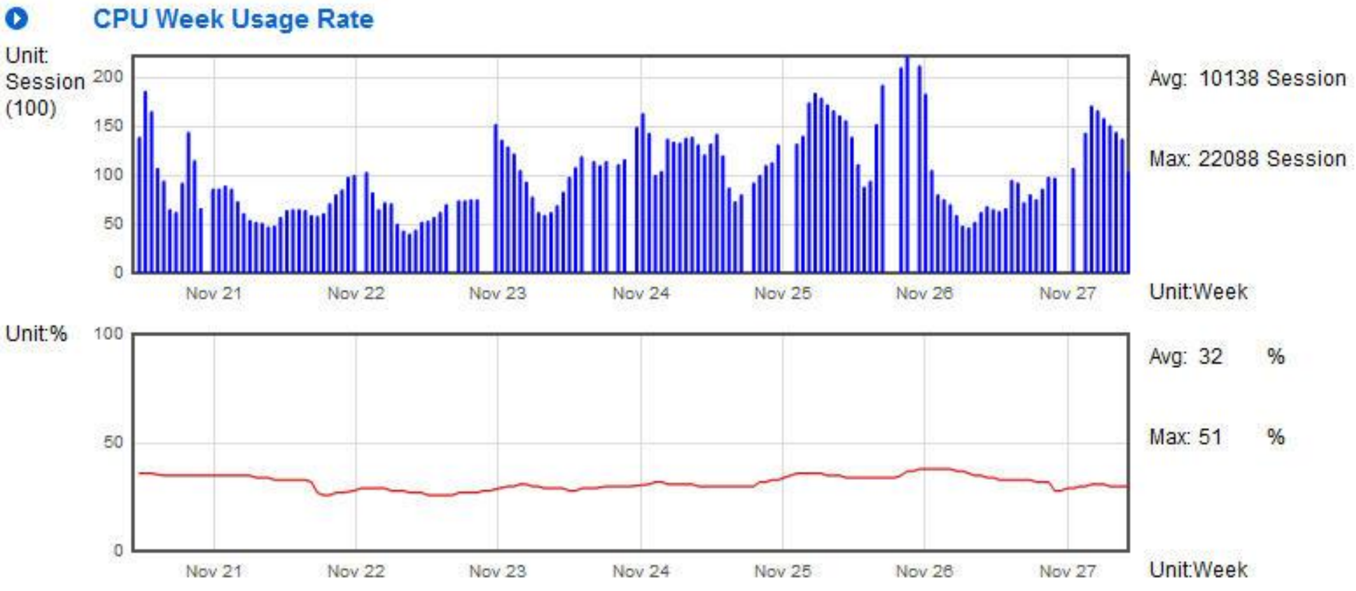
Max: 10416 Session

Avg: 17 %

Max: 36 %

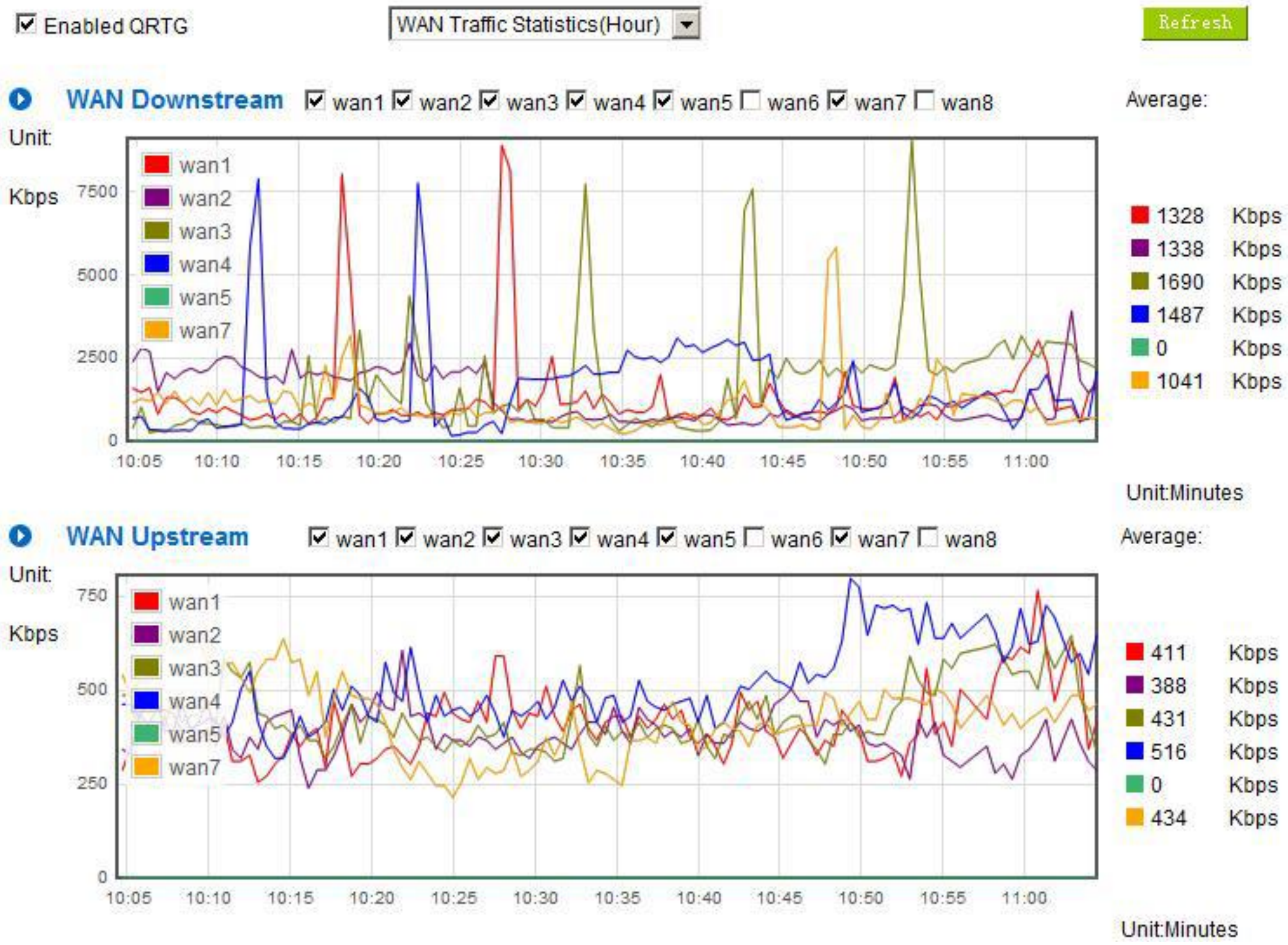


CPU Days Usage Rate
Unit: Session (100)
150
100
50
12:00
14:00
16:00
18:00
20:00
22:00
0:00
2:00
4:00
6:00
8:00
10:00
Avg: 10771 Session
Max: 17143 Session
Unit:Hours
Unit:%
100
50
0
12:00
14:00
16:00
18:00
20:00
22:00
0:00
2:00
4:00
6:00
8:00
10:00
Avg: 31 %
Max: 48 %
Unit:Hours



CPU Week Usage Rate
Unit: Session (100)
200
150
100
50
0
Nov 21
Nov 22
Nov 23
Nov 24
Nov 25
Nov 26
Nov 27
Avg: 10138 Session
Max: 22088 Session
Unit:Week
Unit:%
100
50
0
Nov 21
Nov 22
Nov 23
Nov 24
Nov 25
Nov 26
Nov 27
Avg: 32 %
Max: 51 %
Unit:Week

II. WAN Traffic Statistic (hourly) graphic and average (up/down stream) (As in the following figures)



☑ Enabled QRTG

WAN Traffic Statistics(Hour)

WAN Downstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 □ wan6 ☑ wan7 □ wan8

Average:

🟥	1328	Kbps
🟪	1338	Kbps
🟫	1690	Kbps
🟦	1487	Kbps
🟩	0	Kbps
🟧	1041	Kbps

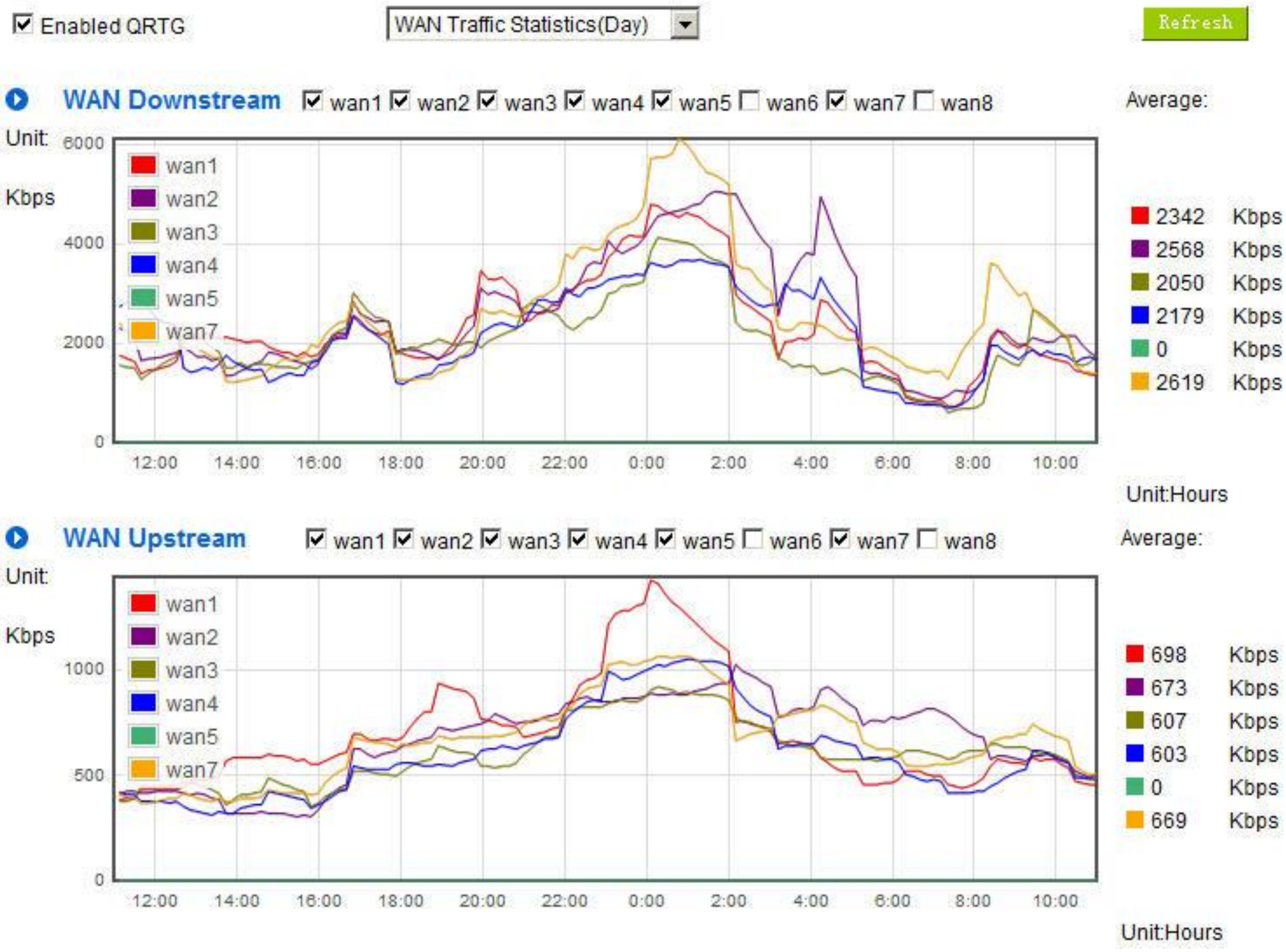
WAN Upstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 □ wan6 ☑ wan7 □ wan8

Average:

🟥	411	Kbps
🟪	388	Kbps
🟫	431	Kbps
🟦	516	Kbps
🟩	0	Kbps
🟧	434	Kbps

* The UI might vary from model to model, depending on different product lines.

III. WAN Traffic Statistic (Day) graphic and average (up/down stream)(As in the following figures)



☑ Enabled QRTG

WAN Traffic Statistics(Day)

Refresh

WAN Downstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 ☐ wan6 ☑ wan7 ☐ wan8

Average:

🟥 2342	Kbps
🟪 2568	Kbps
🟫 2050	Kbps
🟦 2179	Kbps
🟩 0	Kbps
🟧 2619	Kbps

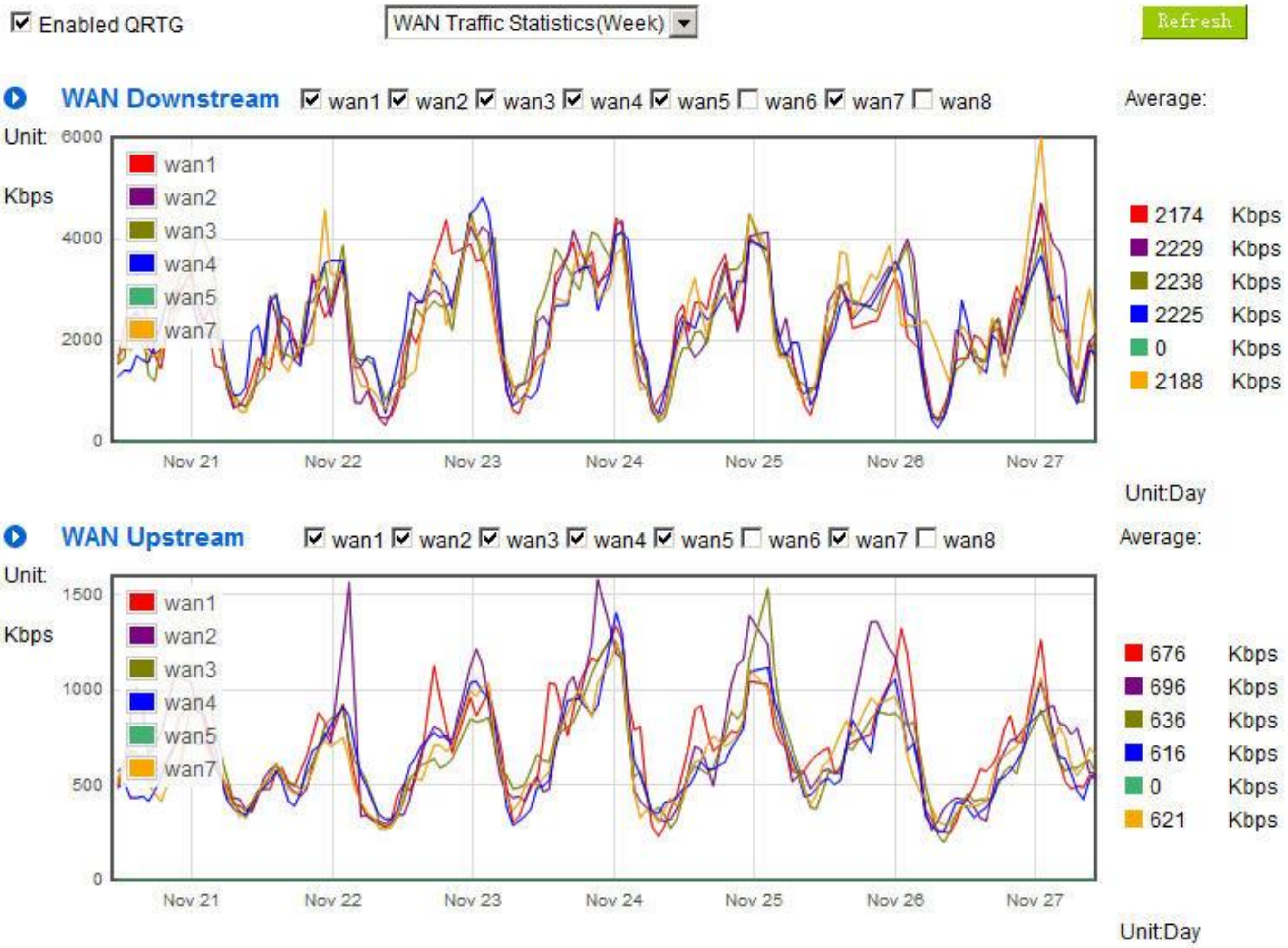
WAN Upstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 ☐ wan6 ☑ wan7 ☐ wan8

Average:

🟥 698	Kbps
🟪 673	Kbps
🟫 607	Kbps
🟦 603	Kbps
🟩 0	Kbps
🟧 669	Kbps

* The UI might vary from model to model, depending on different product lines.

IV. WAN Traffic Statistic (Week) graphic and average (up/down stream)(As in the following figures)



☑ Enabled QRTG   WAN Traffic Statistics(Week) ▾   Refresh

WAN Downstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 □ wan6 ☑ wan7 □ wan8

Average:

🟥	2174	Kbps
🟪	2229	Kbps
🟫	2238	Kbps
🟦	2225	Kbps
🟩	0	Kbps
🟧	2188	Kbps

Unit:Day

WAN Upstream ☑ wan1 ☑ wan2 ☑ wan3 ☑ wan4 ☑ wan5 □ wan6 ☑ wan7 □ wan8

Average:

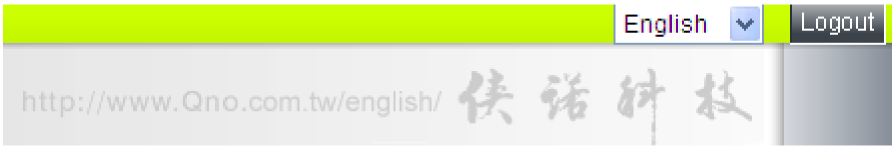
🟥	676	Kbps
🟪	696	Kbps
🟫	636	Kbps
🟦	616	Kbps
🟩	0	Kbps
🟧	621	Kbps

Unit:Day

* The UI might vary from model to model, depending on different product lines.

XIII. Log out

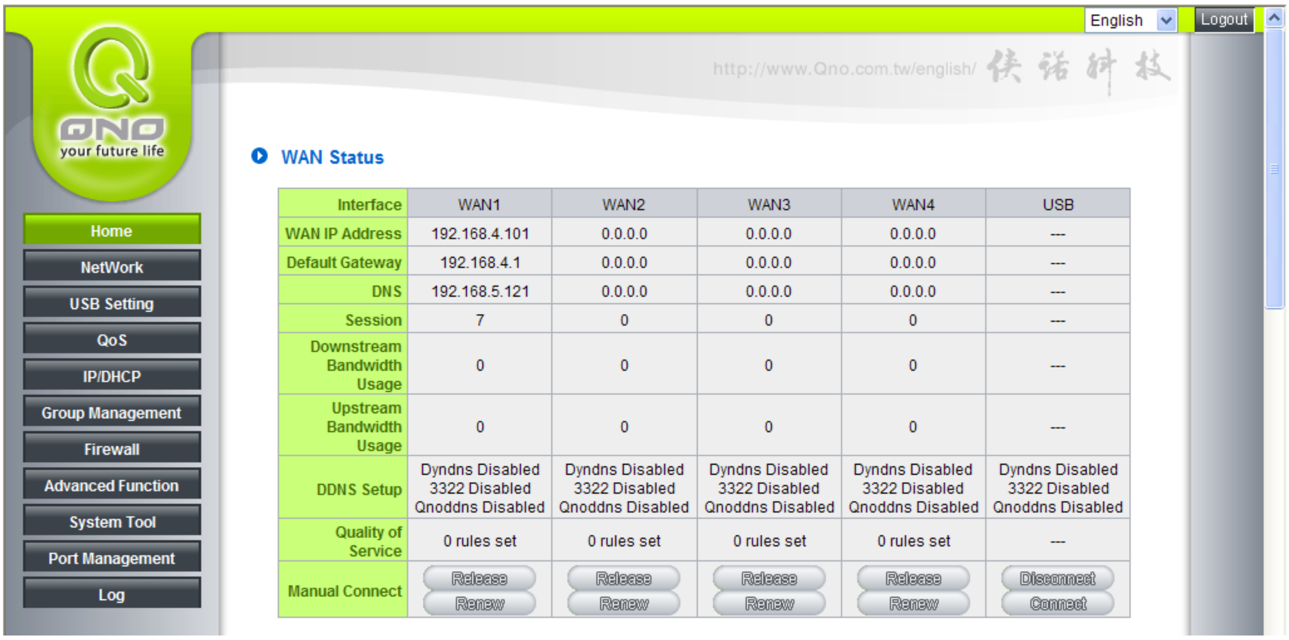
On the top right corner of the web- based UI, there is a Logout button. Click on it to log out of the web-based UI. To enter next time, open the Web browser and enter the IP address, user name and password to log in.



Appendix I: User Interface and User Manual Chapter Cross Reference

This appendix is to show the corresponding index for each chapter and user interface.   Users can find how to setup quickly and understand the Router capability at the same time.

Router overall interface is as below.



WAN Status

Interface	WAN1	WAN2	WAN3	WAN4	USB
WAN IP Address	192.168.4.101	0.0.0.0	0.0.0.0	0.0.0.0	---
Default Gateway	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0	---
DNS	192.168.5.121	0.0.0.0	0.0.0.0	0.0.0.0	---
Session	7	0	0	0	---
Downstream Bandwidth Usage	0	0	0	0	---
Upstream Bandwidth Usage	0	0	0	0	---
DDNS Setup	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled
Quality of Service	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connect	Release Renew	Release Renew	Release Renew	Release Renew	Disconnect Connect

Category	Sub- category	Chapter
Home		V. Device Spec Verification, Status Display and Login Password and Time Setting 5.1 Home
Basic Setting		VI. Network
	Network Connection	6.1 Network Connection
	Traffic Management	6.2 Multi- WAN Setting
	Protocol Binding	6.2 Multi- WAN Setting
USB Setting		Please download user manual on Qno official webpage. http://www.qno.com.tw
QoS		VIII. QoS
	Bandwidth Management	8.1 QoS/Smart QoS

	Session Control	8.2 Session Limit
	Hardware Optimization	8.3 Hardware Optimization
IP/DHCP		VII. Port Management
	Setup	7.3 DHCP/ IP
	Status	7.4 DHCP Status
	IP & MAC Binding	7.5 IP & MAC Binding
Group Management		VII. Port Management
	Local IP Group	7.6 IP Grouping
	Remote IP Group	7.6 IP Grouping
	Port Group	7.7 Port Group Management
Firewall		IX. Firewall
	General Policy	9.1 General Policy
	Access Rule	9.2 Access Rule
	Content Filter	9.3 Content Filter
Advanced Function		XI. Advanced Setting
	DMZ/Forwarding	11.1 DMZ Host/ Port Range Forwarding
	UPnP	11.2 UPnP- Universal Plug and Play
	Routing	11.3 Routing
	One to One NAT	11.4 One to One NAT
	DDNS	11.5 DDNS
	MAC Clone	11.6 MAC Clone
	Inbound Load Balance	11.7 Inbound Load Balance
System Tool		XII. System Tool V. Device Spec Verification, Status Display and Login Password and Time Setting
	Password	5.2 Change and Set Login Password and Time
	Diagnostic	12.1 Diagnostic
	Firmware Upgrade	12.2 Firmware Upgrade
	Setting Backup	12.3 Setting Backup
	SNMP	12.4 SNMP
	Time	5.2 Change and Set Login Password and Time

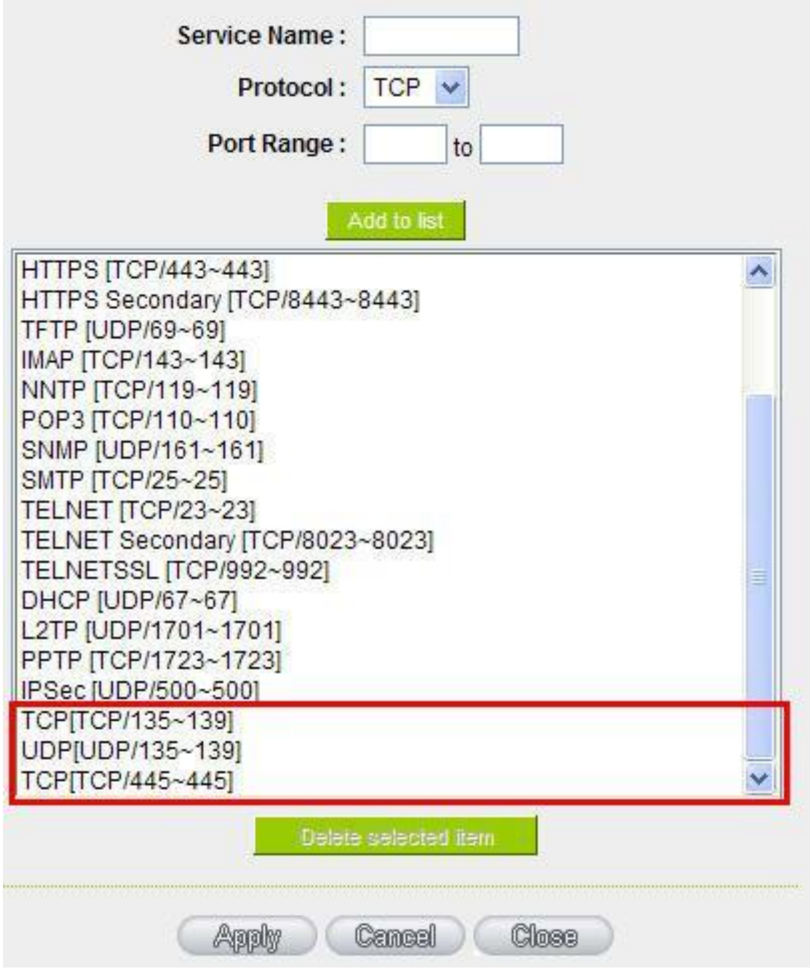
	System Recover	12.5 System Recover
	High Availability	13.6 High Availability
	License Key	13.7 License Key
Port Management		VII. Port Management
	Setup	7.1 Setup
	Status	7.2 Status
Log		XIII. Log
	System Log	13.1 System Log
	System Status	13.2 System Statistic
	Traffic Statistic	13.3 Traffic Statistic
	Connection Statistic	13.4 Connection Statistic
	IP/Port statistic	13.5 IP/Port statistic
	QRTG	13.6 QRTG

Appendix II: Troubleshooting

（1） Shock Wave and Worm Virus Prevention

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

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



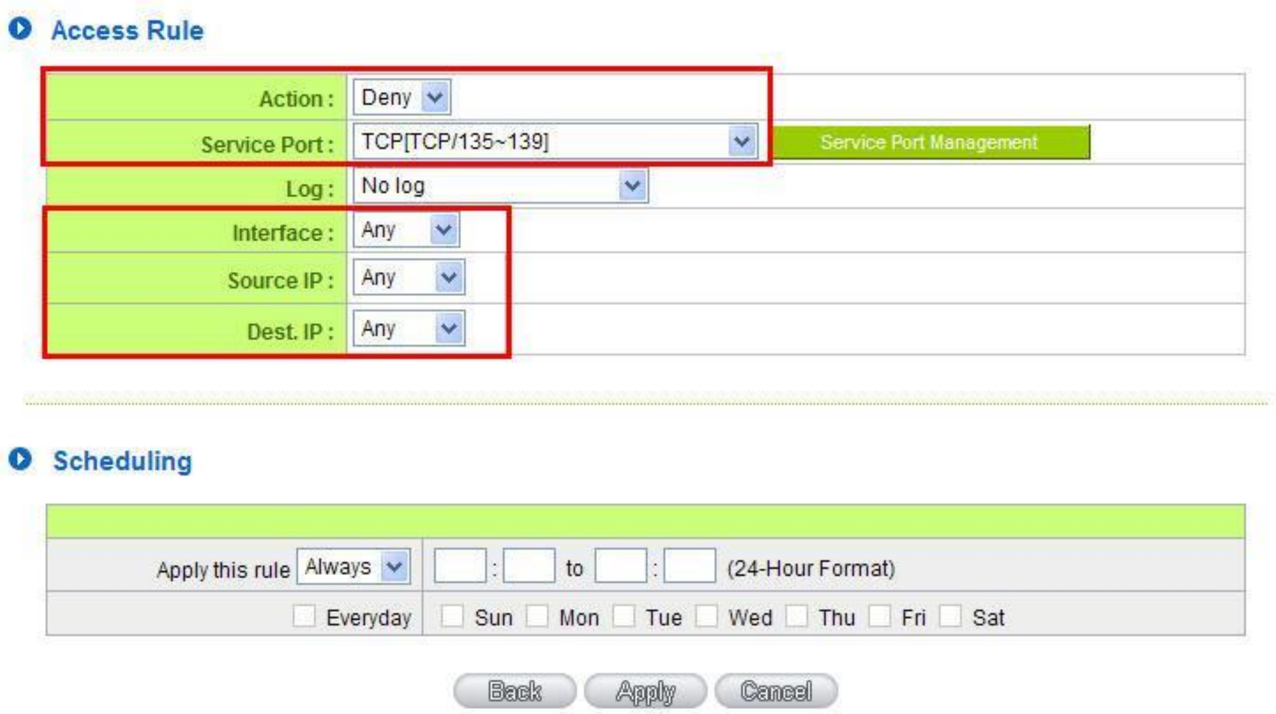
Service Name :

Protocol : TCP

Port Range : to

HTTPS [TCP/443~443]
HTTPS Secondary [TCP/8443~8443]
TFTP [UDP/69~69]
IMAP [TCP/143~143]
NNTP [TCP/119~119]
POP3 [TCP/110~110]
SNMP [UDP/161~161]
SMTP [TCP/25~25]
TELNET [TCP/23~23]
TELNET Secondary [TCP/8023~8023]
TELNETSSL [TCP/992~992]
DHCP [UDP/67~67]
L2TP [UDP/1701~1701]
PPTP [TCP/1723~1723]
IPSec [UDP/500~500]
TCP[TCP/135~139]
UDP[UDP/135~139]
TCP[TCP/445~445]

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



Access Rule

Action :	Deny
Service Port :	TCP[TCP/135~139]
Log :	No log
Interface :	Any
Source IP :	Any
Dest. IP :	Any

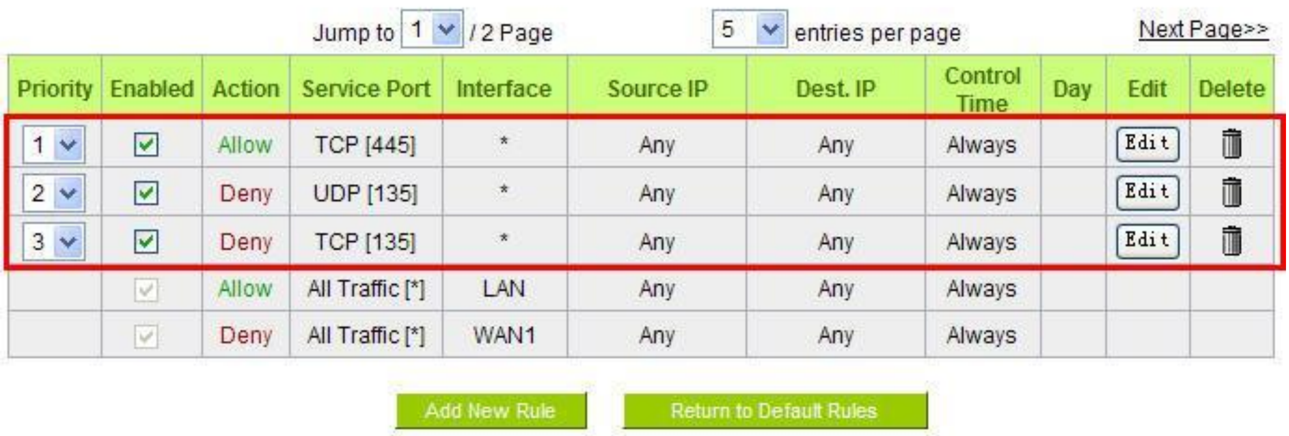
Scheduling

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

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

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

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



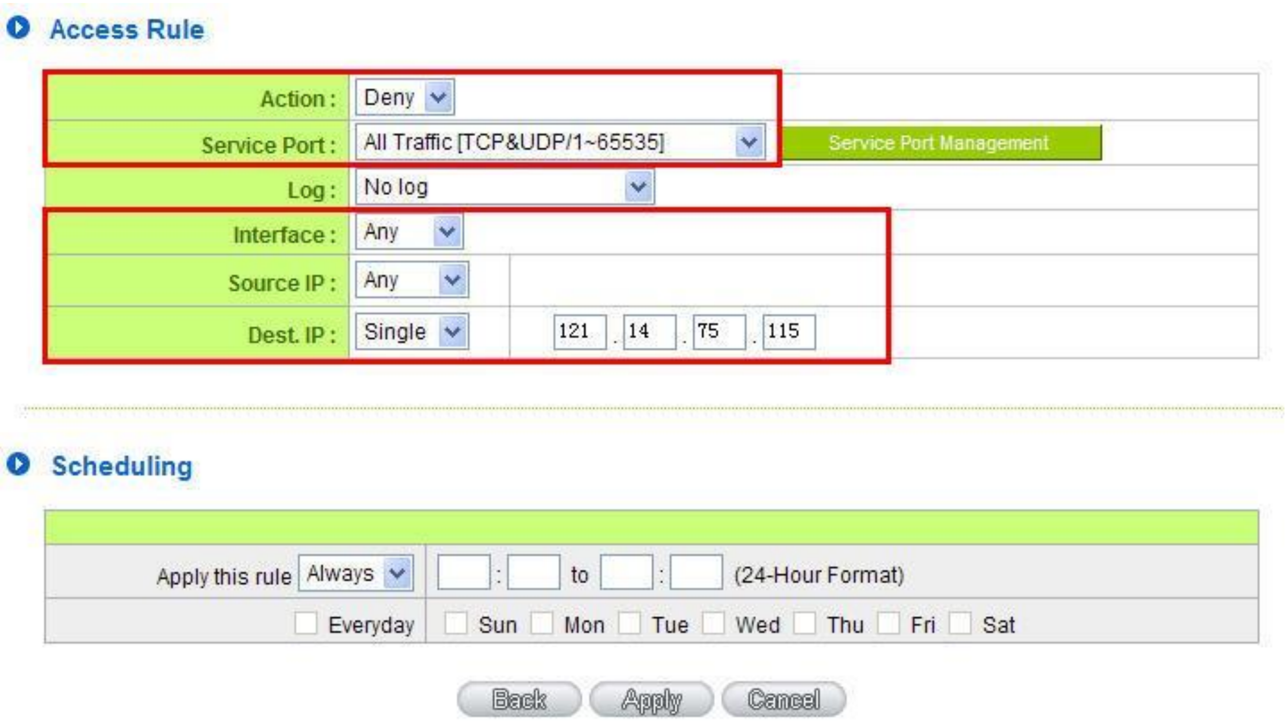
Jump to 1 / 2 Page 5 entries per page Next Page>>

Priority	Enabled	Action	Service Port	Interface	Source IP	Dest. IP	Control Time	Day	Edit	Delete
1	☑	Allow	TCP [445]	*	Any	Any	Always		Edit	🗑
2	☑	Deny	UDP [135]	*	Any	Any	Always		Edit	🗑
3	☑	Deny	TCP [135]	*	Any	Any	Always		Edit	🗑
	☑	Allow	All Traffic [*]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [*]	WAN1	Any	Any	Always			

（2） Block QQLive Video Broadcast Setting

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

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



Access Rule

Action :	Deny
Service Port :	All Traffic [TCP&UDP/1~65535]
Log :	No log
Interface :	Any
Source IP :	Any
Dest. IP :	Single 121 . 14 . 75 . 115

Scheduling

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

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

b). Click "Add New Rule" under "Access Rule" page. Select "Deny" in "Action" under the "Service” rule setting, followed by the selection of "All Traffic [TCP&UDP/1~65535]" from "the service" and select "Any" for Interface, "Any" for source IP address (users with relevant needs may select either "Single" or "Range" to block any QQLive login by using one single IP or IP range), followed by the selection of "Single" of the "Dest. IP and enter the IP address as 121.14.75.155" for the QQLive Server (note that there are more than one IP address for QQLive server. Repeated addition may be needed). Lastly, select "Always" under the Scheduling setting so that the QQLive Login Time can be set. (If necessary, specific time setting may be undertaken). Click "Apply" to move to the next step.

c). Input the following IP address in **Dest. IP** repeatedly.

cache.tv.qq.com

58.60.11.145

58.60.11.146

58.60.11.147

59.36.97.5

59.36.97.7

59.36.97.37

219.133.63.48

loginqqlivedx.qq.com

219.133.49.159

loginqqlivewt.qq.com

58.251.63.13

loginqqlivexy.qq.com

202.205.3.218

qqlive.qq.com

219.133.62.70

tv1-3t.qq.com

221.236.11.40

tv2.qq.com

218.17.209.17

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

（3） ARP Virus Attack Prevention

1. ARP Issue and Information

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

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

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

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

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

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

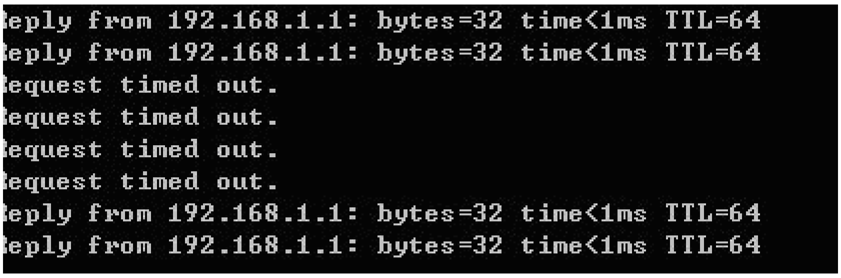
Such virus program as PWSteal. lemir or its transformation is worm virus of the Trojan programs affecting Windows 95/ 98/ Me/ NT/ 2000/ XP/ 2003. There are two attack methods affecting the network connection speed: cheat on the ARP table in the device or LAN PC. The former intercepts the gateway data and send ceaselessly a series of wrong MAC messages to the device, which sends out wrong MAC address. The PC thus cannot receive the messages. The later is ARP attack by fake gateways. A fake gateway is established. The PC which is cheated sends data to this gateway and doesn't go online through the normal device. From the PC end, the situation is "disconnection“.

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

2. ARP Diagnostic

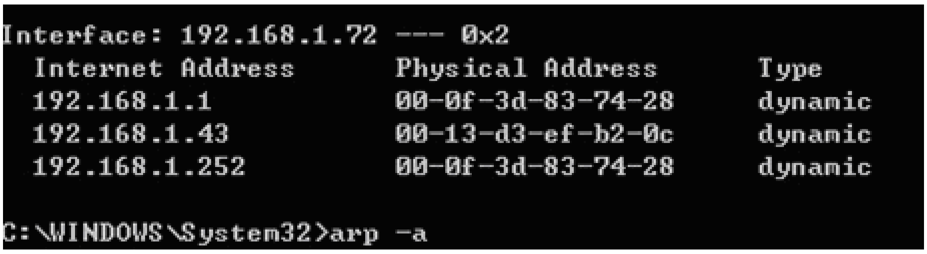
If one or more computers are affected by the ARP virus, we must learn how to diagnose and take appropriate measures. The following is experience shared by Qno technical engineers with regard to the ARP prevention.

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



```
eply from 192.168.1.1: bytes=32 time<1ms TTL=64
eply from 192.168.1.1: bytes=32 time<1ms TTL=64
equest timed out.
equest timed out.
equest timed out.
equest timed out.
eply from 192.168.1.1: bytes=32 time<1ms TTL=64
eply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

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



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

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

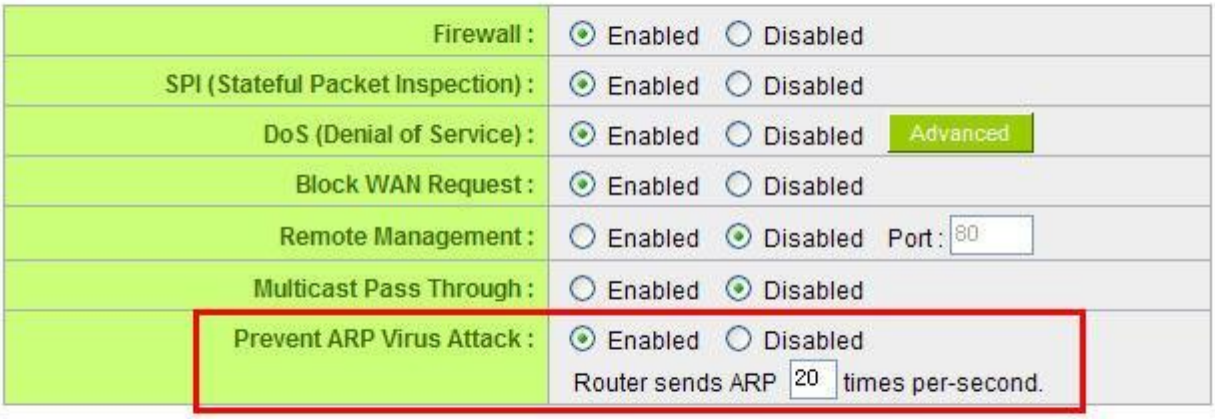
It is found that the IP of 192.168.1.1 and 192.168.252 points to the same MAC address as 00-0f-3d-83-74-28. Evidently, this is a cheat by ARP.

3. ARP Solution

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

a) Enable “Prevent ARP Virus Attack”:

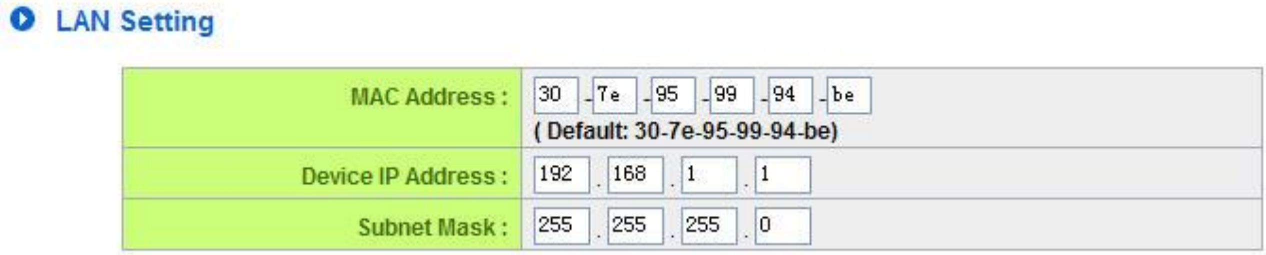
Enter the device IP address to log in the management webpage of the device. Enter ”Firewall-> General” and find the option "Prevent ARP Virus Attack" to the right of the page. Click on the option to activate it and click "Apply" at the bottom of the page (see illustrated).



Firewall :	● Enabled ○ Disabled
SPI (Stateful Packet Inspection) :	● Enabled ○ Disabled
DoS (Denial of Service) :	● Enabled ○ Disabled Advanced
Block WAN Request :	● Enabled ○ Disabled
Remote Management :	○ Enabled ● Disabled Port : 80
Multicast Pass Through :	○ Enabled ● Disabled
Prevent ARP Virus Attack :	● Enabled ○ Disabled Router sends ARP 20 times per-second.

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

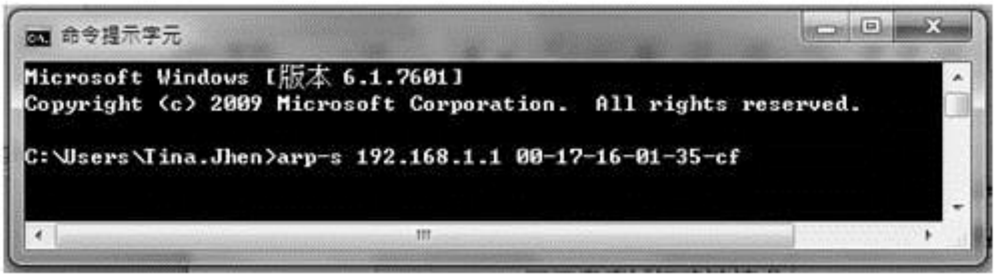
This prevents the ARP from cheating IP and its MAC address. First, find out the gateway IP and MAC address on the device end.



LAN Setting

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

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



```
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Tina.Jhen>arp-s 192.168.1.1 00-17-16-01-35-cf
```

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

@echo off

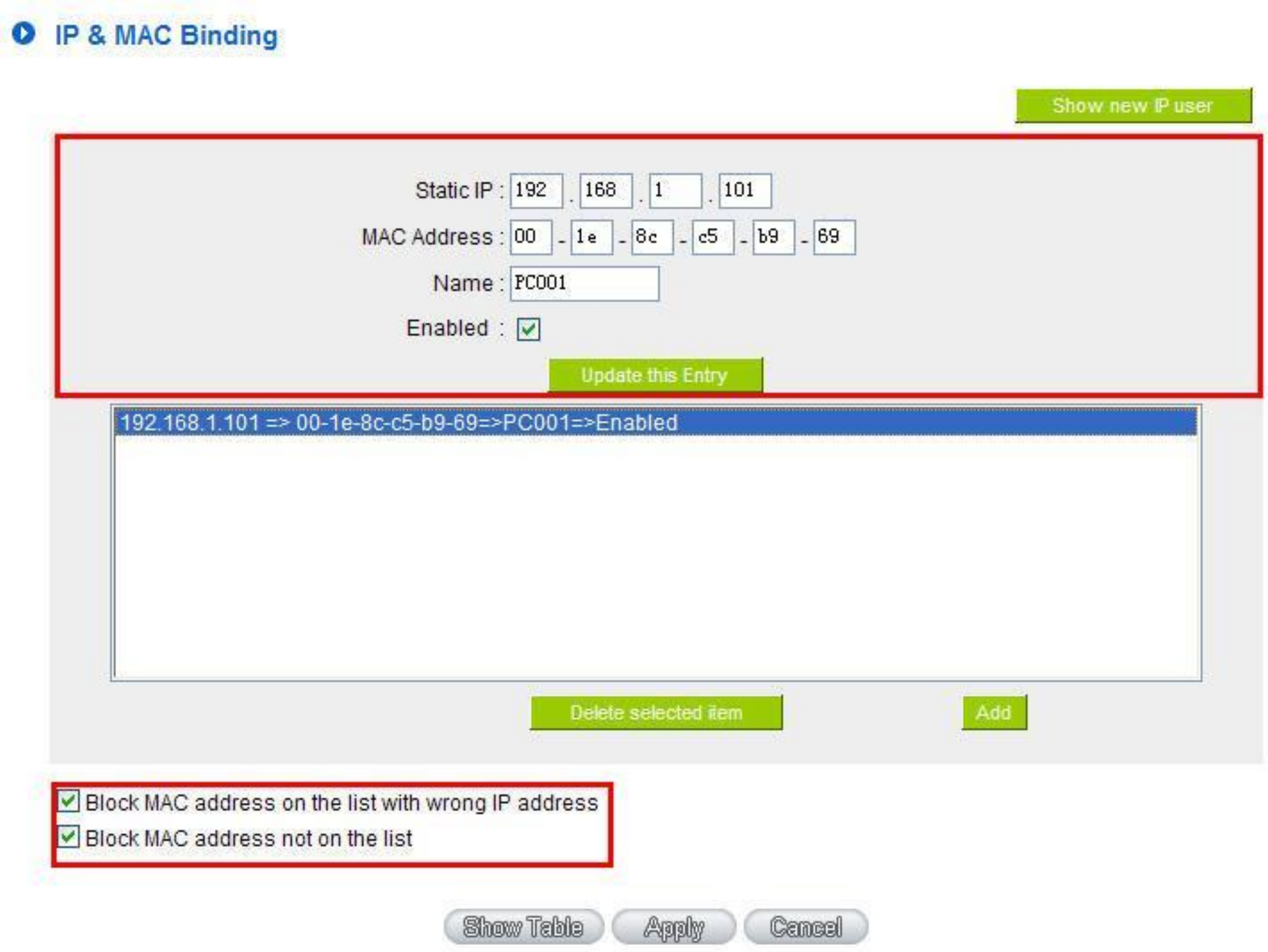
```
arp -d
arp -s Router LAN IP     Router LAN MAC
```

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

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

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

Enter “Setup” under DHCP page. On the down right corner of the screen, there is “IP and MAC Binding,” where users may create IP and MAC binding. On “Enabled,” click on “√” and select “Add to List.” Repeat these steps to add other IP addresses and MAC binding, followed by clicking “Apply” at the bottom of the page.



Static IP : 192 . 168 . 1 . 101

MAC Address : 00 - 1e - 8c - c5 - b9 - 69

Name : PC001

Enabled : ☑

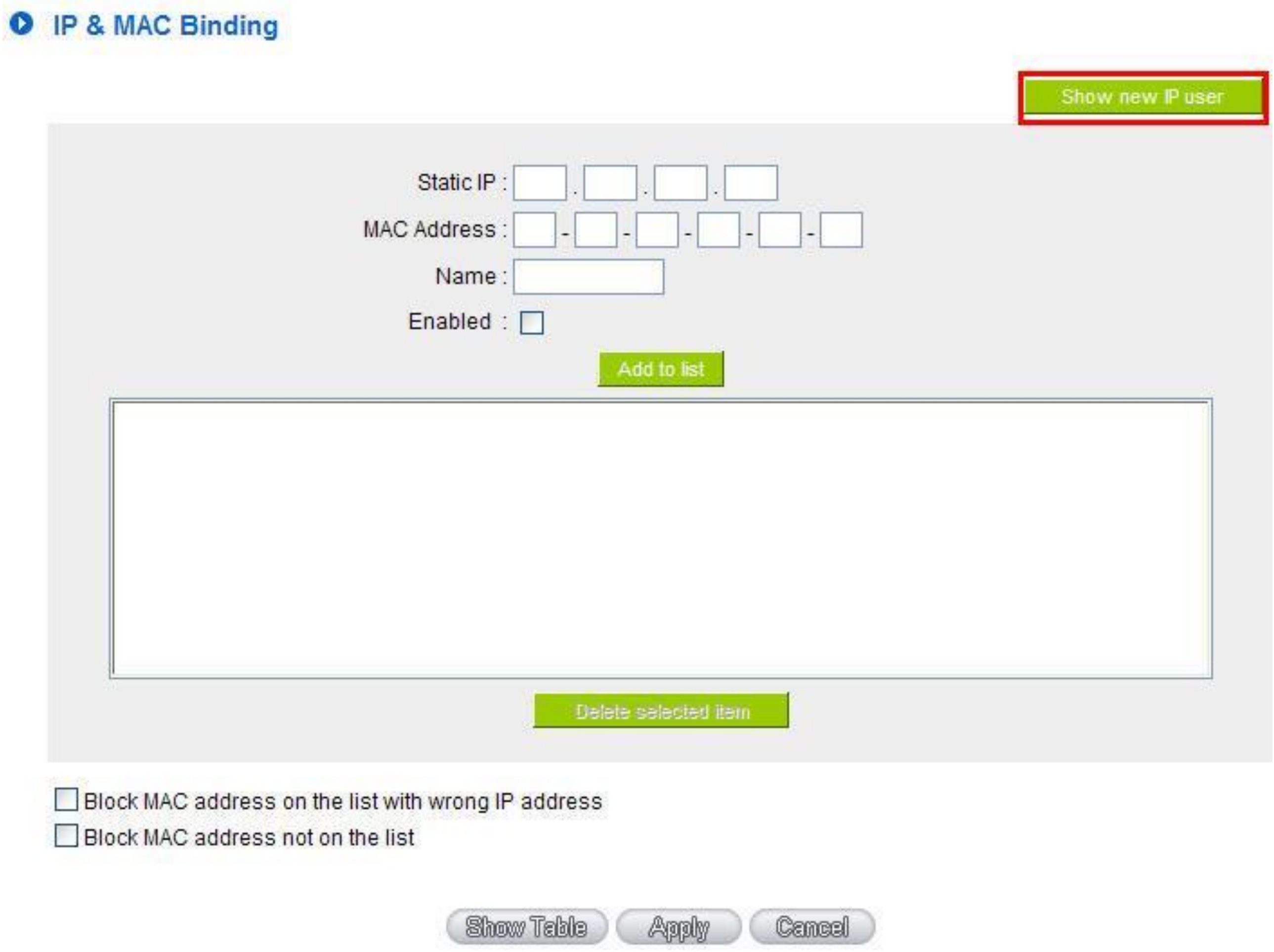
192.168.1.101 => 00-1e-8c-c5-b9-69=>PC001=>Enabled

☑ Block MAC address on the list with wrong IP address

☑ Block MAC address not on the list

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

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



IP & MAC Binding

Static IP : . . .

MAC Address : - - - - -

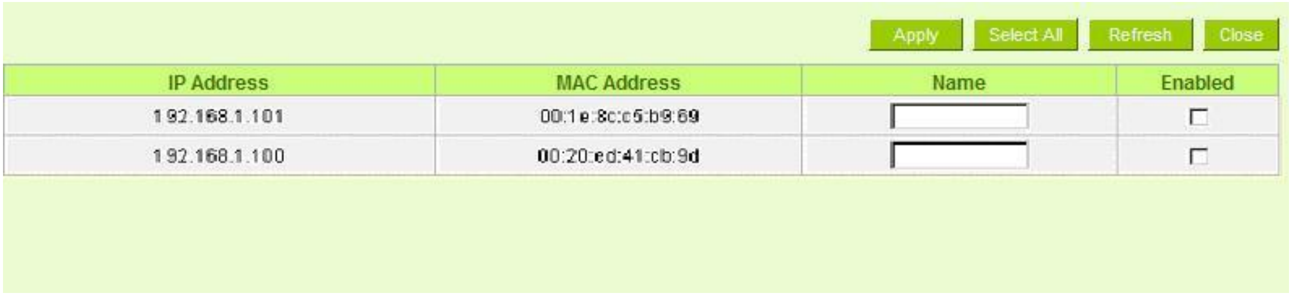
Name :

Enabled : □

□ Block MAC address on the list with wrong IP address

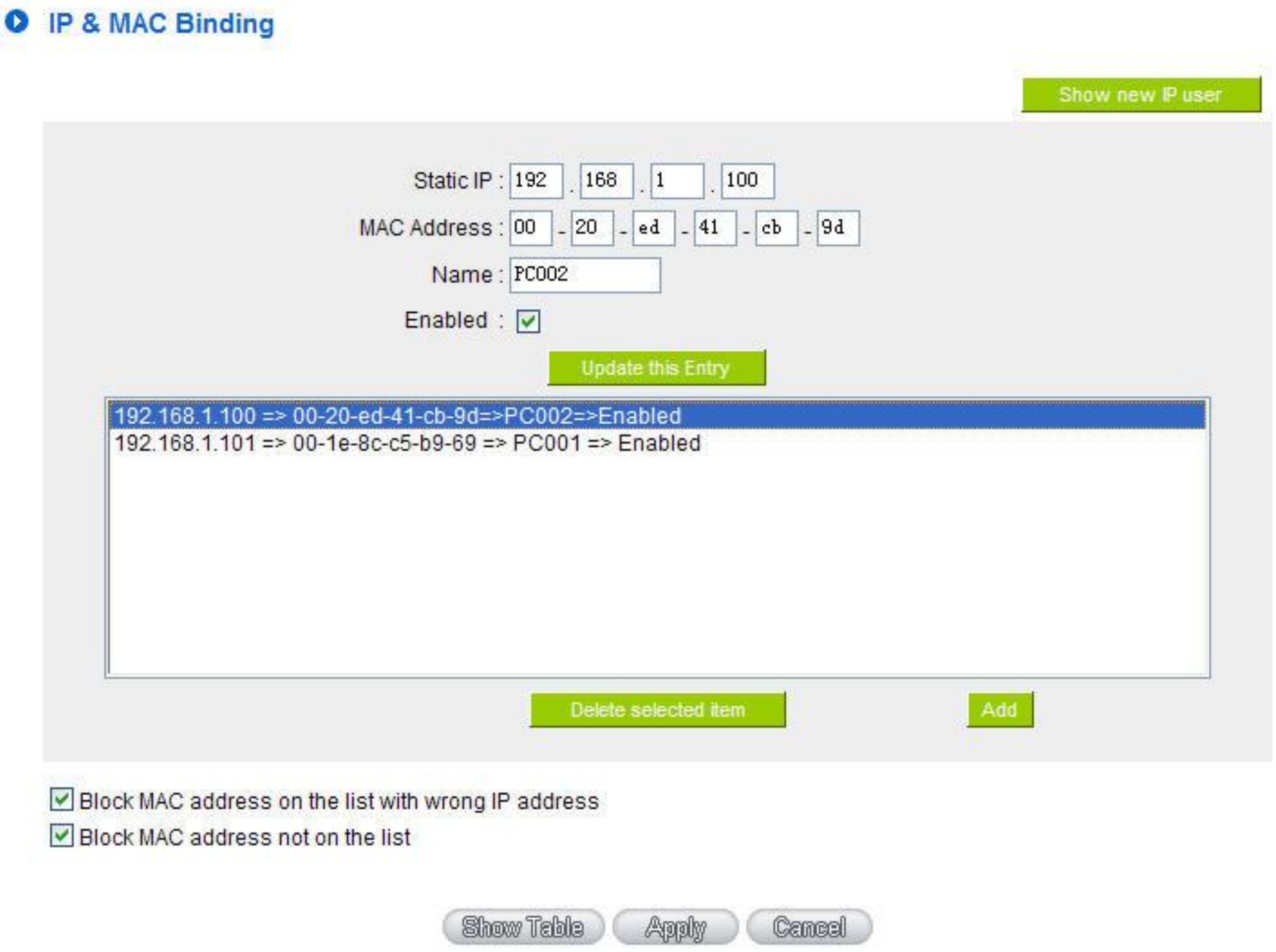
□ Block MAC address not on the list

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



IP Address	MAC Address	Name	Enabled
192.168.1.101	00:1e:8c:c5:b9:69		□
192.168.1.100	00:20:ed:41:cb:9d		□

Now the bound options will display on the IP and MAC binding list (as illustrated in Figure 5) and click "Apply” to finish binding.



IP & MAC Binding

Static IP : 192 . 168 . 1 . 100

MAC Address : 00 - 20 - ed - 41 - cb - 9d

Name : PC002

Enabled : ☑

```
192.168.1.100 => 00-20-ed-41-cb-9d=>PC002=>Enabled
192.168.1.101 => 00-1e-8c-c5-b9-69 => PC001 => Enabled
```

☑ Block MAC address on the list with wrong IP address

☑ Block MAC address not on the list

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

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

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

3. Install the patch program for the system. Through Windows Update, the system patch program (critical update, security update and Service Pack)

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

and delete some redundant accounts.

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

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

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

4. Summary

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

Appendix III: Qno Technical Support Information

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

Qno Official Website

http：//www.Qno.com.tw

Dealer Contact

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

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

Taiwan Support Center：

E- mail：QnoFAE@qno.com.tw