



4/5WAN 8LAN Gigabit Network QoS Router

Load Balance, Bandwidth Management, and Network Security

English User's Manual

Contents

I. Introduction	4
II. Multi-WAN Router Installation	6
2.1 Systematic Setting Process.....	6
2.2 Setting Flow Chart.....	6
III. Hardware Installation	9
3.1 Router LED Signal.....	9
3.2 GIGABIT Router Network Connection.....	12
IV. Login Router	13
V. Device Spec Verification, Status Display and Login Password and Time Setting	15
5.1 Home Page.....	15
5.2 Change and Set Login Password and Time.....	20
VI. Network Configuration	23
6.1 Network Connection	23
6.2 Multi- WAN Setting	35
VII. Intranet Configuration	53
7.1 Port Management.....	53
7.2 Port Status	55
7.3 IP/ DHCP	56
7.4 DHCP Status	58
7.5 IP & MAC Binding.....	60
7.6 IP Grouping	64
VIII. QoS (Quality of Service)	65
8.1 Bandwidth Management.....	66
8.2 Session control	75
IX. Firewall	78
9.1 General Policy	78
9.2 Access Rule.....	81
9.3 Content Filter	86
X. Advanced Function	92
10.1 DMZ/Forwarding.....	92
10.2 Routing	96
10.3 One to One NAT	99
10.4 DDNS- Dynamic Domain Name Service	101

10.5 MAC Clone	104
XI. System Tool	105
11.1 Diagnostic	105
11.2 Firmware Upgrade	107
11.3 Setting Backup	108
11.4 System Recover	109
XII. Log.....	111
12.1 System Log.....	111
12.2 System Statistic	115
12.3 Traffic Statistic	116
12.4 IP/ Port Statistic	119
XIII. Log out	121
Appendix I: User Interface and User Manual Chapter Cross Reference	122
Appendix II: Troubleshooting	124
(1) Block BT Download	125
(2) Shock Wave and Worm Virus Prevention	125
(3) Block QQLive Video Broadcast Setting	127
(4) ARP Virus Attack Prevention	129
Appendix III: Qno Technical Support Information	138

Product Manual Using Permit Agreement

[Product Manual (hereafter the "Manual") Using Permit Agreement] hereafter the "Agreement" is the using permit of the Manual, and the relevant rights and obligations between the users and Qno Technology Inc (hereafter "Qno"), and is the exclusion to remit or limit the liability of Qno. The users who obtain the file of this manual directly or indirectly, and users who use the relevant services, must obey this Agreement.

Important Notice: Qno would like to remind the users read the clauses of the "Agreement" before downloading and reading this Manual. Unless you accept the clauses of this "Agreement", please return this Manual and relevant services. The downloading or reading of this Manual is regarded as accepting this "Agreement" and the restriction of clauses in this "Agreement".

【1】 Statement of Intellectual Property

Any text and corresponding combination, diagram, interface design, printing materials or electronic file are protected by copyright of our country, clauses of international copyright and other regulations of intellectual property. When the user copies the "Manual", this statement of intellectual property must also be copied and indicated. Otherwise, Qno regards it as tort and relevant duty will be prosecuted as well.

【2】 Scope of Authority of "Manual"

The user may install, use, display and read this "Manual on the complete set of computer.

【3】 User Notice

If users obey the law and this Agreement, they may use this "Manual" in accordance with "Agreement". If the users violate the "Agreement", Qno will terminate the using authority and destroy the copy of this "Manual". The "hardcopy or softcopy" of this Manual is restricted using for information, non-commercial and personal purpose. Besides, it is not allowed to copy or announce on any network computer. Furthermore, it is not allowed to disseminate on any media. It is not allowed to modify any part of the "file". Using for other purposes is prohibited by law and it may cause serious civil and criminal punishment. The transgressor will receive the accusation possibly.

【4】 Legal Liability and Exclusion

【4-1】 Qno will check the mistake of the texts and diagrams with all strength. However, Qno, distributors and resellers do not bear any liability for direct or indirect economic loss, data loss or other corresponding commercial loss to the user or relevant personnel due to the possible omission.

【4-2】 In order to protect the autonomy of the business development and adjustment of Qno, Qno reserves

the right to adjust or terminate the software / Manual any time without informing the users. There will be no further notice regarding the product upgrade or change of technical specification. If it is necessary, the change or termination will be announced in the relevant block of the Qno website.

【4-3】 All the set parameters are examples and they are for reference only. You may also purpose your opinion or suggestion. We will take it as reference and they may be amended in the next version.

【4-4】 This Manual explains the configuration of all functions for the products of the same series. The actual functions of the product may vary with the model. Therefore, some functions may not be found on the product you purchased.

【4-5】 Qno reserves the right to change the file content of this Manual and the Manual content may not be updated instantly. To know more about the updated information of the product, please visit Qno official website.

【4-6】 Qno (and / or) distributors hereby declares that no liability will be born for any guarantee and condition of the corresponding information. The guarantee and condition include tacit guarantee and condition about marketability, suitability for special purposes, ownership and non-infringement. The name of the companies and products mentioned may be the trademark of the owners. Qno (and/or) the distributors do not provide the product or software of any third party company. Under any circumstance, Qno and / or distributors bear no liability for special, indirect, derivative loss or any type of loss in the lawsuit caused by usage or information on the file, no matter the lawsuit is related to agreement, omission or other tort.

【5】 Other Clauses

【5-1】 The potency of this Agreement is over any other verbal or written record. The invalidation of part or whole of any clause does not affect the potency of other clauses.

【5-2】 The power of interpretation, potency and dispute are applicable for the law of Taiwan. If there is any dissension or dispute between the users and Qno, it should be attempted to solve by consultation first. If it is not solved by consultation, user agrees that the dissension or dispute is brought to trial in the jurisdiction of the court in the location of Qno. In Mainland China, the "China International Economic and Trade Arbitration Commission" is the arbitration organization.

I. Introduction



New generation GIGABIT Network QoS Router is a high efficiency Router owing to the market requirement. It is designed as economical, high efficiency with all functions integrated for network QoS Router that fulfills the requirement of internet cafe, bandwidth application increase and bandwidth management. New generation GIGABIT Network QoS Router focuses on multiple operators environment and user bandwidth management requirement to integrate the gigabit backbone networking, it can support hardware port mirror, smart QoS, Multi-WAN load balance, Voice alert, Gateway redundancy, Intelligent Firewall.

GIGABIT Network QoS Router uses a 64-bit multi-core hardware acceleration, high-level processor and maximum 2Gbps-two way forwarding rate that can support 300,000 connections, built-in 512MB RAM allows the stability and reliability for long-time operation.

It provides 4Gigabit WAN port and high-efficiency load balance mode for out-bound load balance. WAN side outbound connection performance can fulfill most of the standards for broadband market. In addition, independent DMZ port can connect to the public server by public IP address. It has a built-in 8Gigabit backbone LAN port to appropriate for 10/100/1000Mbps Ethernet switch and each port can connect with other switches for more network devices that can build up a Gigabit backbone conveniently to accelerate the network availability and scalable bandwidth enterprise.

Individual QoS bandwidth management with powerful and easy-to-setup functions allows manager to arrange the limited network resource rational and efficiently. It is not needed to extend the bandwidth to unlimited settings which would increase spending cost; it can also avoid the complaint of few people to force whole bandwidth. Simple user configuration can be the best efficiency application; it allows the optimization of bandwidth utilization based on the whole utility rate without setting rules step-by-step and only to limit the users who occupy the bandwidth for resource savings. Moreover, intelligence bandwidth management is provided, through the simple deployment to complete LAN side bandwidth management for efficiency utility rate, simple management and improvement performance.

Load balancing function supports Auto Load Balance mode, Specify WAN Binding mode and Strategy

Routing mode to allow deployment of flexible network connection required to control traffic flow to guarantee that whole connections are unobstructed. Strategy Routing mode is simply to configure the network without the input of IP address, it can auto detect outbound packets and filter telecom connection to ensure quick response and packet pass through without obstruction, it can aggregate the same operators bandwidth for load balancing control and increase flexibility of network resource.

Built-in Firewall system can fulfill market requirement in defense of internet attacks for most enterprise. Initiative packet inspection via the network layer dynamic detection to deny or block proprietary protocol connection. It can easily employ complete protective functions to ensure network security, as required for any kind of hack attacks, worm & Virus and ARP attacks by one-way control. Firewall system has not only NAT function but also DoS attack. Complete Functions of Access Rules can allow manager to select the network service level to deny or allow access, it can also limit or deny LAN users to use the network and to avoid the network resource being occupied or threaten due to improper uses.

NAT function can provide the translation between private IP and public IP, it can allow multi-user to connect to the internet with one public IP at the same time. LAN IP supports four Class C connections, DHCP server is also supported, as well as an easy-to-configure IP-MAC binding function allowing network structure to be flexible and easy to deploy and managed ◦

This manual is to introduce every function, configuration and specifics of the router. We recommend you to read our “Quick Installation Guide” if you have any questions. When you buy this router, it should help you connect to the internet quickly.

To obtain remote technical support, you can log on to our Web site www.Qno.com.tw, and find technical support information on the appendix or contact our technical support engineers via email. You can also get the newest Qno’s product information and application examples from the web site.

II. Multi-WAN Router Installation

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

2.1 Systematic Setting Process

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

1. Hardware installation
2. Login
3. Verify device specification and set up password and time
4. Set WAN connection
5. Set LAN connection: physical port and IP address settings
6. Set QoS bandwidth management: avoid bandwidth occupation
7. Set Firewall: prevent attack and improper access to network resources
8. Other settings: UPnP, DDNS, MAC Clone
9. Management and maintenance settings: Syslog, SNMP, and configuration backup
10. Logout

2.2 Setting Flow Chart

Below is the description for each setting process, and the crospndent contents and purposes. For detailed functions, please refer to Appendix I: Setting Interface and Chapter Index.

#	Setting	Content	Purpose
---	---------	---------	---------

1	Hardware installation	Configure the network to meet user's demand.	Install VPN Firewall hardware based on user physical requirements.
2	Login	Login the device with Web Browser.	Login VPN Firewall web- based UI.
3	Verify device specification	Verify Firmware version and working status.	Verify VPN firewall specification, Firmware version and working status.
	Set password and time	Set time and re- new password.	Modify the login password considering safe issue. Synchronize the VPN Firewall time with WAN.
4	Set WAN connection	Verify WAN connection setting, bandwidth allocation, and protocol binding.	Connect to WAN. Configure bandwidth to optimize data transmission.
5	Set LAN connection: physical port and IP address settings	Set mirror port and VLAN. Allocate and manage LAN IP.	Provide mirror port, port management and VLAN setting functions. Support Static/DHCP IP allocation to meet different needs. IP group will simplify the management work.
6	Set QoS bandwidth management: avoid bandwidth occupation	Restrict bandwidth and session of WAN ports, LAN IP and application.	To assure transmission of important information, manage and allocate the bandwidth further to achieve best efficiency.
7	Set Firewall: prevent attack and improper access to network resources	Block attack, Set Access rule and restrict Web access.	Administrators can block BT to avoid bandwidth occupation, and enable access rules to restrict employee accessing internet improperly or using MSN, QQ and Skype during working time. They can also protect network from Worm or ARP attacking.

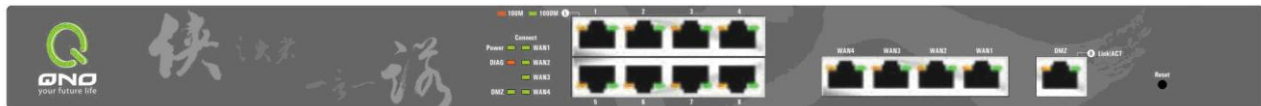
8	Advanced Settings : DMZ/Forwarding, UPnP, DDNS, MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone	DMZ/Forwarding, UpnP, Routing Mode, multiple WAN IP, DDNS and MAC Clone
9	Management and maintenance settings: Syslog, SNMP, and configuration backup	Monitor VPN Firewall working status and configuration backup.	Administrators can look up system log and monitor system status and inbound/outbound flow in real time.
11	Logout	Close configuration window.	Logout VPN Firewall web- based UI.

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

III. Hardware Installation

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

3.1 Router LED Signal



LED Signal Description

LED	Color	Description
Power	Green	Green LED on: Power ON
DIAG	Amber	Amber LED on: System self-test is running. Amber LED off: System self-test is completed successfully.
Link/Act	Green	Green LED on: Ethernet connection is fine. Green LED blinking: Packets are transmitting through Ethernet port.
100M- Speed	Amber	Amber LED on: Ethernet is running at 100Mbps. Amber LED off: Ethernet is running at 10Mbps.
Connect	Green	Green LED on: WAN is connected and gets the IP address.
1000M-Speed	Green	Green LED on : Ethernet is running at 1000Mbps.
WAN1	Green	Green LED on : WAN1 is connected and IP address has been obtained
WAN2	Green	Green LED on : WAN2 is connected and IP address has been obtained
WAN3	Green	Green LED on : WAN3 is connected and IP address has been obtained
WAN4	Green	Green LED on : WAN4 is connected and IP address has been obtained

Reset

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

System Built-in Battery

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

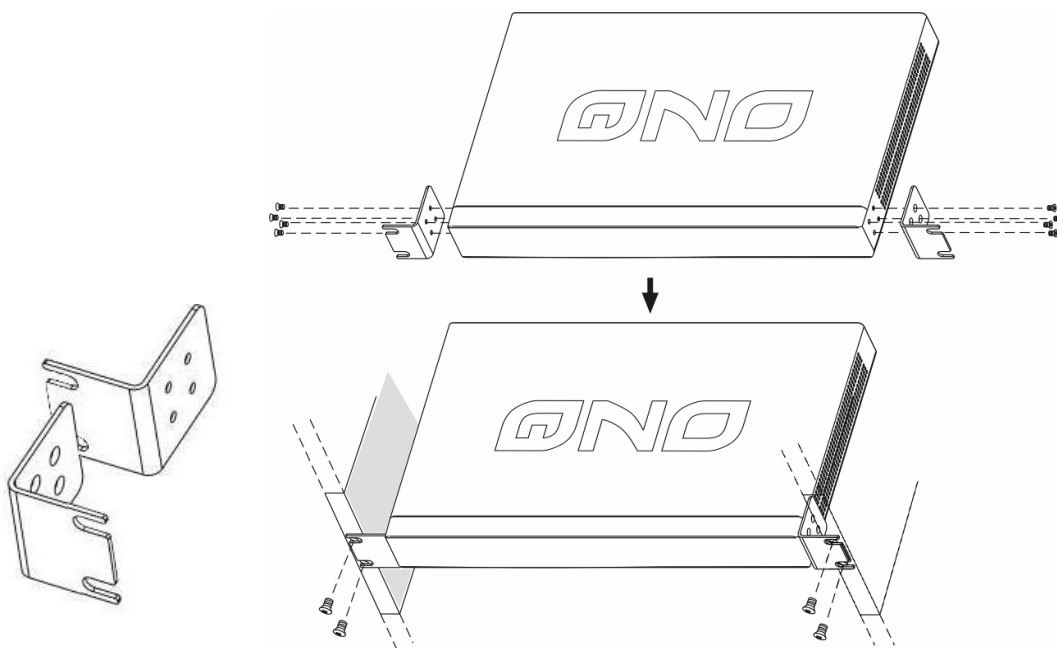
Attention!

Do not replace the battery yourself; otherwise irreparable damage to the product may be caused.

Installing GIGABIT Router on a Standard 19" Rack

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

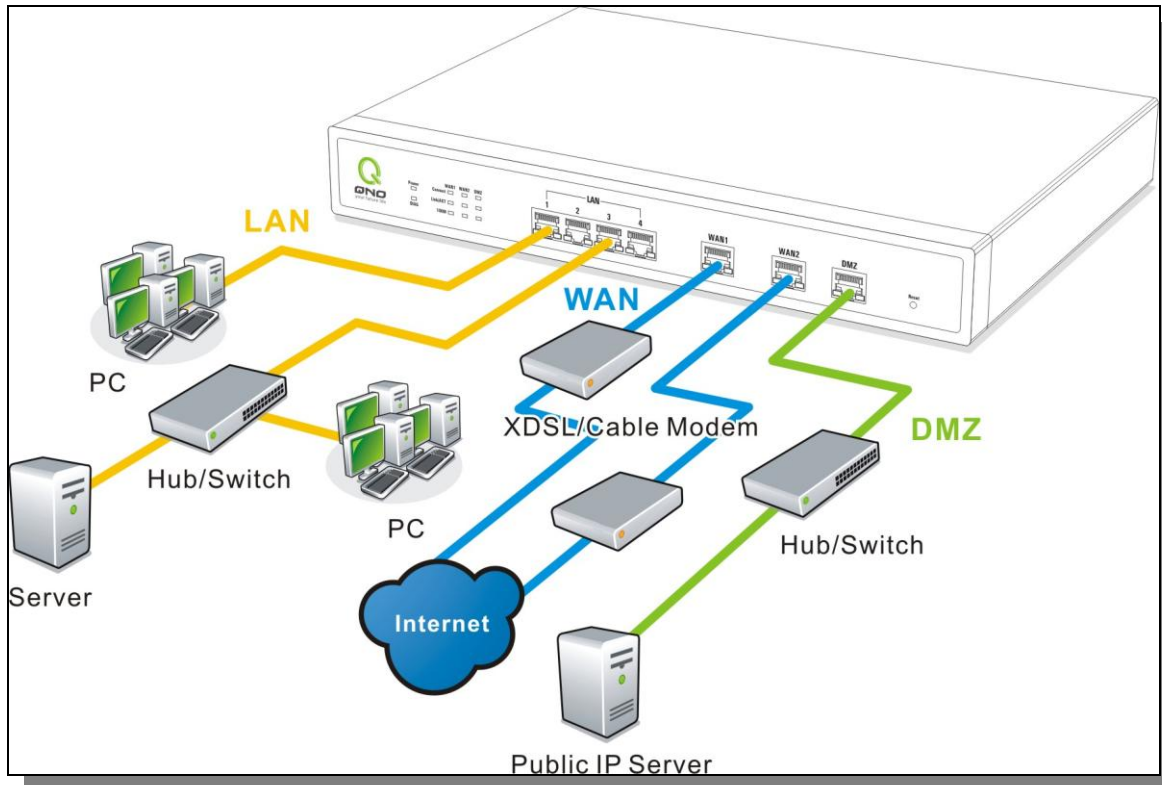
Each GIGABIT Router comes with a set of rack installation accessories, including 2 L- shaped brackets and 8 screws. Users can rack- mount the device onto the chassis. Please refer to the figure below for the installation onto a 19" rack:



Attention!

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

3.2 GIGABIT Router Network Connection



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

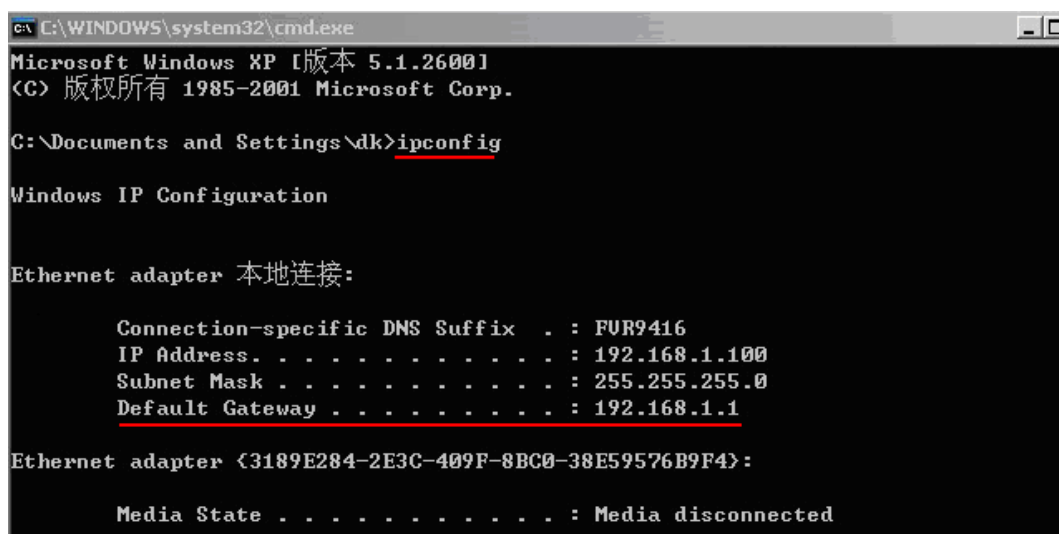
LAN Connection: The LAN port can be connected to a Switching Hub or directly to a PC. Users can use servers for monitoring or filtering through the port after “Physical Port Mangement” configuration is done.

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

IV. Login Router

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

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\dk>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : FUR9416
    IP Address. . . . .                : 192.168.1.100
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 192.168.1.1

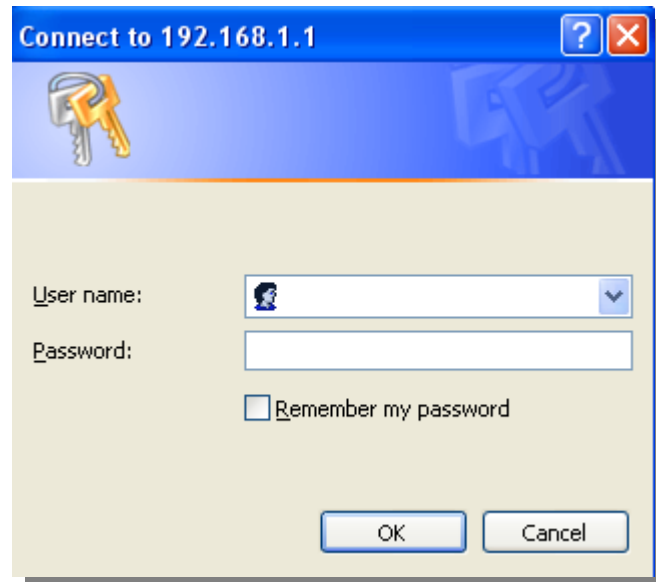
Ethernet adapter {3189E284-2E3C-409F-8BC0-38E59576B9F4}:

    Media State . . . . .              : Media disconnected
```

Attention!

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

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



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

Attention!

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

After login, VPN Firewall web- based UI will be shown. Select the language on the upper right corner of the webpage. The language chosen will be in blue. Please select “English’ as below.



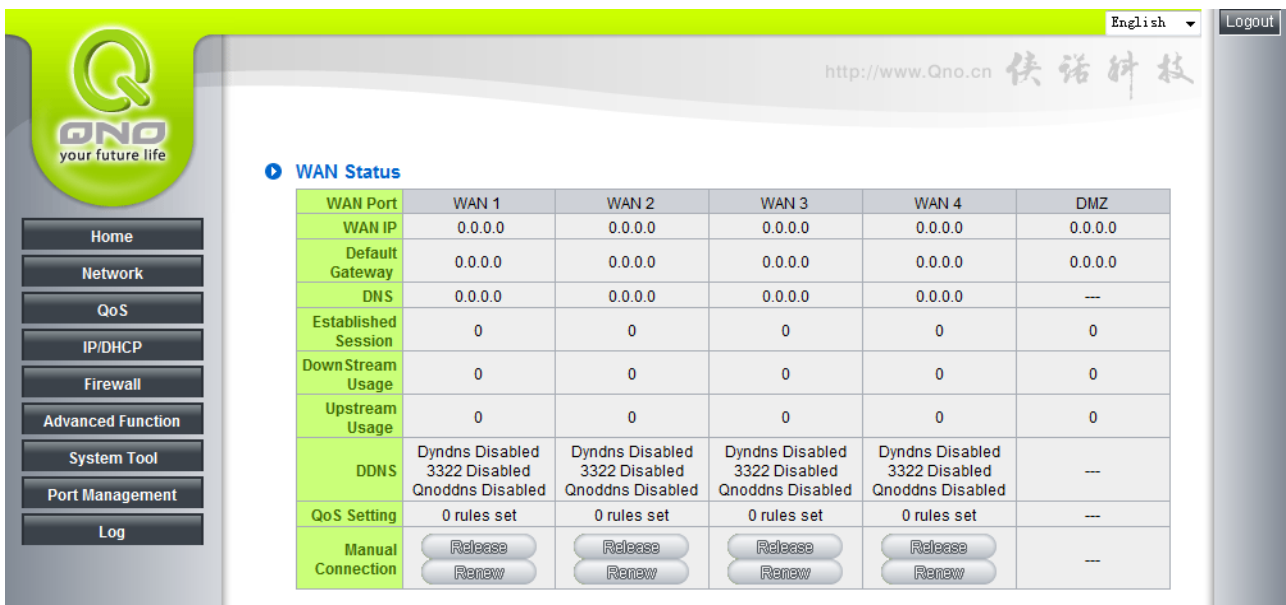
V. Device Spec Verification, Status Display and Login Password and Time Setting

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

5.1 Home Page

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

5.1.1 WAN Status



WAN Port	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
WAN IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
Established Session	0	0	0	0	0
DownStream Usage	0	0	0	0	0
Upstream Usage	0	0	0	0	0
DDNS	Dyndns Disabled 3322 Disabled Qnodns Disabled	Dyndns Disabled 3322 Disabled Qnodns Disabled	Dyndns Disabled 3322 Disabled Qnodns Disabled	Dyndns Disabled 3322 Disabled Qnodns Disabled	---
QoS Setting	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connection	Release Renew	Release Renew	Release Renew	Release Renew	---

IP Address :	Indicates the current IP configuration for WAN port.
Default Gateway :	Indicates current WAN gateway IP address from ISP.
DNS Server :	Indicates the current DNS IP configuration.
Session :	Indicates the current session number for each WAN in VPN Firewall.
Downstream Bandwidth Usage(%) :	Indicates the current downstream bandwidth usage(%) for each WAN.
Upstream Bandwidth Usage(%) :	Indicates the current upstream bandwidth usage(%) for each WAN.
DDNS :	Indicates if Dynamic Domain Name is activated. The default

	configuration is "Off".
Quality of Service :	Indicates how many QoS rules are set.
Manual Connect :	When "Obtain an IP automatically" is selected, two buttons (Release and Renew) will appear. If a WAN connection, such as PPPoE or PPTP, is selected, "Disconnect" and "Connect" will appear.
DMZ IP Address :	Indicates the current DMZ IP address.

5.1.2 Physical Port Status

▶ Physical Port Status

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

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

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

Port1 Information	
Summary:	
Type	10Base-T / 100Base-TX / 1000Base-T
Interface	LAN
Link Status	Up
Port Activity	Port Enabled
Priority	Normal
Speed Status	1000 Mbps
Duplex Status	Full
Auto negotiation	Enabled
VLAN	VLAN1
Statistics:	
Port Receive Packet Count	2066
Port Receive Packet Byte Count	915748
Port Transmit Packet Count	336
Port Transmit Packet Byte Count	212548
Port Packet Error Count	0
<input type="button" value="Refresh"/> <input type="button" value="Close"/>	

The current port setting status information will be shown in the Port Information Table. Examples: type (10Base-T/100Base-TX) , ininterface (WAN 1 ~4/LAN 1 ~8/DMZ) , link status (Up/ Down) , physical port status (Port Enabled/ Port Disabled) , priority (high or normal) , speed status (10Mbps/100Mbps) , duplex status (Half/ Full) , auto negotiation (Enabled or Disabled). The table also shows statistics of Receive/ Transmit Packets, Receive/Transmit Packets Byte Count as well as Error Packets Count.

5.1.3 System Information

System Information

LAN IP Address/Subnet Mask	192.168.1.1/255.255.255.0	Serial Number	XXXXXXXXXXXX
Mode	Gateway (Router Mode)	Firmware	v1.0.15.02 (Nov 5 2008 08:42:32)
Working Time	10 Days 3 Hours 4 Minutes 28 Seconds	Current Time	Tue Jan 11 2000 11:04:27

Device IP Address : Identifies the current device IP address. The default is 192.168.1.1.

Working Mode : Indicates the current working mode. Can be NAT Gateway or Router mode. The default is "NAT Gateway" mode.

System active time: Indicates how long the GIGABIT Router has been running.

Serial Number: This number is the GIGABIT Router serial number.

Firmware Version : Information about the GIGABIT Router present software version.

Current Time: Indicates the device present time. Please note: To have the correct time, users must synchronize the device with the remote NTP server first.

5.1.4 Firewall Status

▶ Security Status

Firewall Setting	Status
SPI (Stateful Packet Inspection)	Enabled
DoS Protect	Enabled
Block WAN Request	Enabled
ARP Attack Prevetion	Enabled
Remote Management	Closed
Access Rule	0 rules set

SPI (Stateful Packet Inspection) : Indicates whether SPI (Stateful Packet Inspection) is on or off. The default configuration is “On”.

DoS (Denial of Service) : Indicates if DoS attack prevention is activated. The default configuration is “On”.

Block WAN Request : Indicates that denying the connection from Internet is activated. The default configuration is “On”.

Prevent ARP Virus Attack : Indicates that preventing Arp virus attack is acitvated. The default configuration is “Off”.

Remote Management: Indicates if remote management is activated (on or off). Click the hyperlink to enter and manage the configuration. The default configuration is “Off”.

Access Rule : Indicates the number of access rule applied in VPN Firewall.

5.1.5 Log Setting Status

▶ Log Status

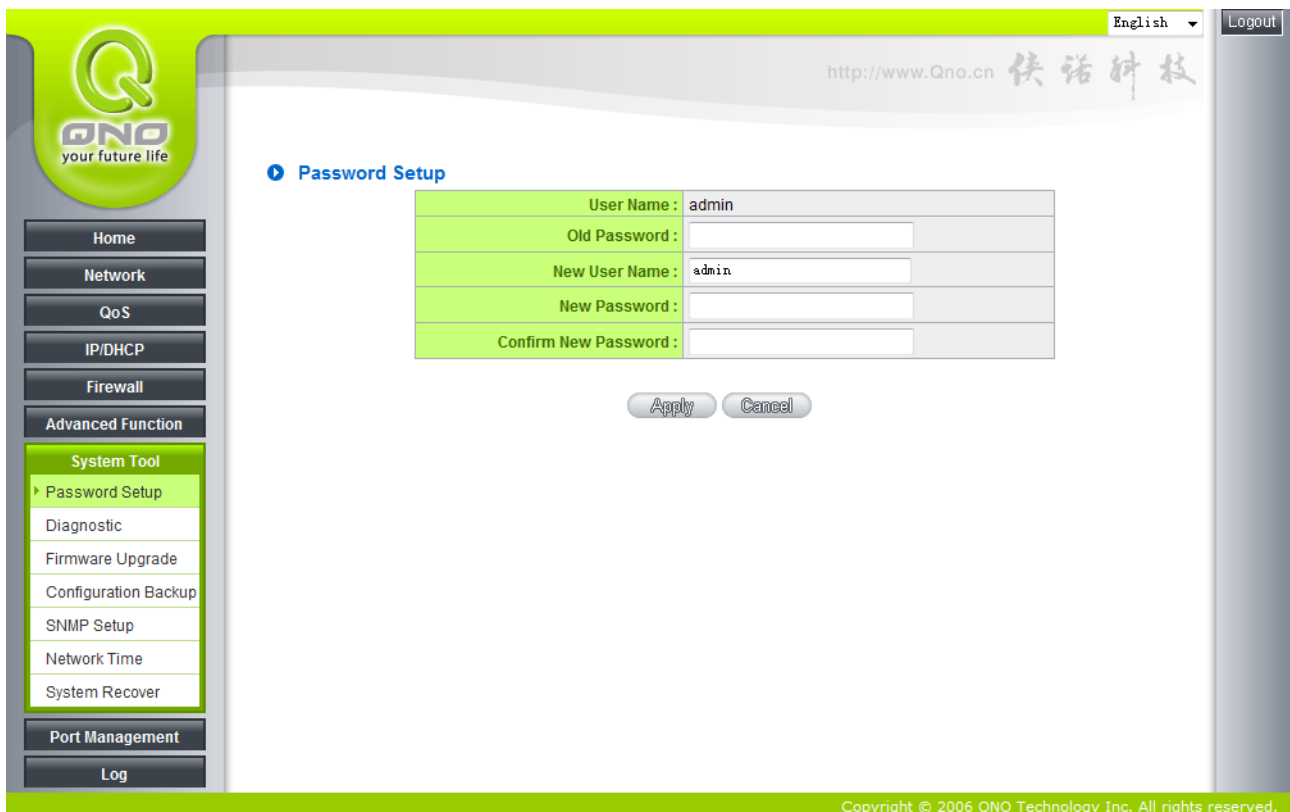
Send Log to	Closed ()
-------------	------------

Send Log to : (Future)	Indicates if Syslog Server is Enabled or Closed.
------------------------	--

5.2 Change and Set Login Password and Time

5.2.1 Password Setting

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



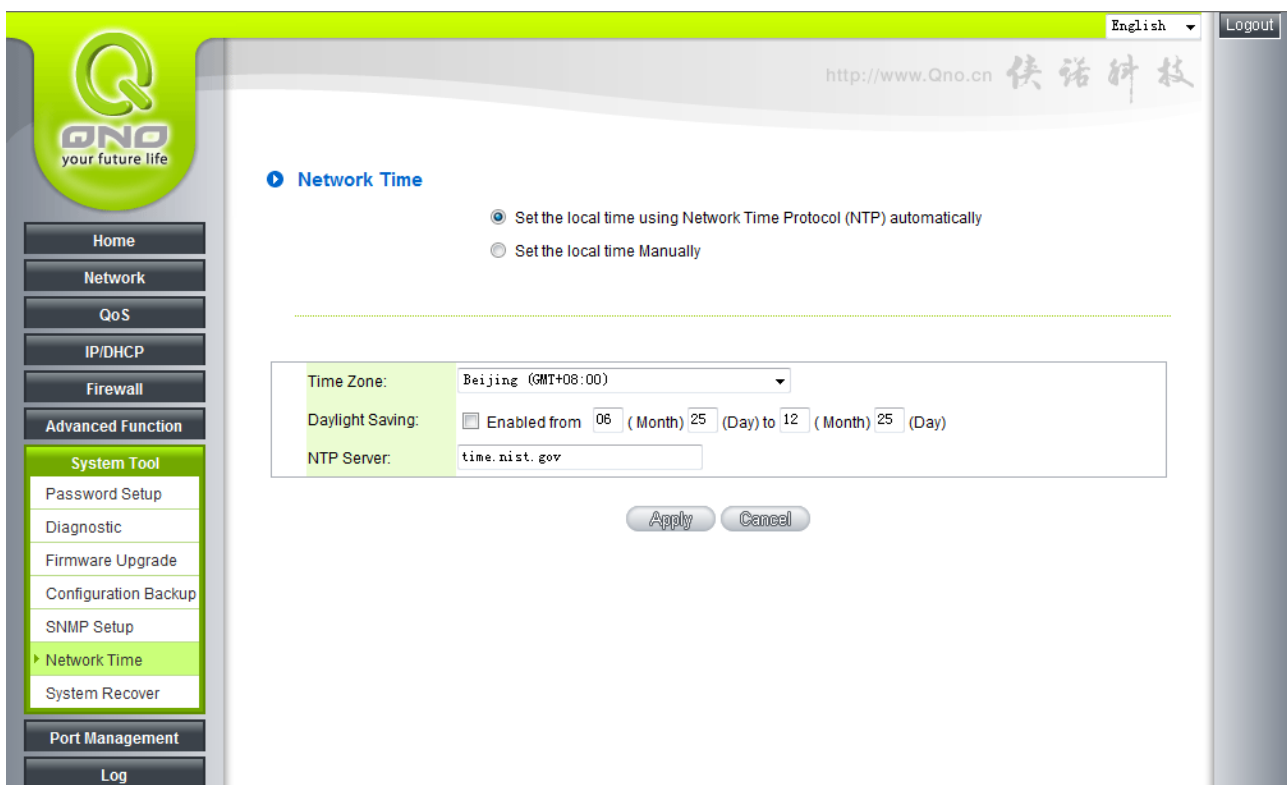
User Name :	The default is “admin”.
Old Password :	Input the original password. (The default is “admin”.)
New User Name :	Input the new user name. i.e.Qno
New Password :	Input the new password.
Confirm New Password :	Input the new password again for verification.
Apply :	Click “ Apply ” to save the configuration.

Cancel :	Click “ Cancel ” to leave without making any change. This action will be effective before ”Apply” to save the configuration.
----------	---

5.2.2 Time

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

Synchronize with external NTP server : GIGABIT Router has embedded NTP server, which will update the time spontaneously.



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

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

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

Network Time

- Set the local time using Network Time Protocol (NTP) automatically
- Set the local time Manually

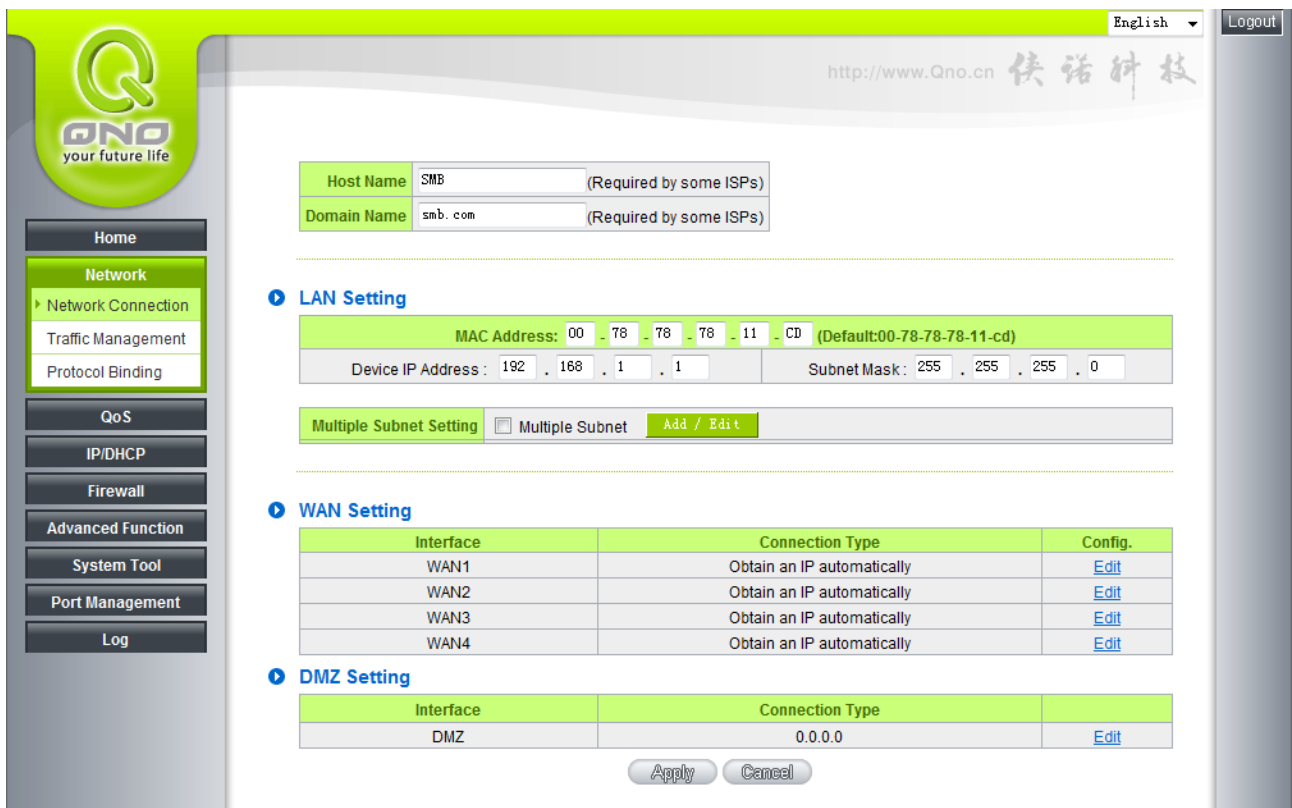
16	Hours	56	Minutes	20	Seconds
2	Month	24	Day	2009	Year

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

VI、Network Configuration

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

6.1 Network Connection



English Logout

http://www.Qno.cn 快诺科技

Host Name: SMB (Required by some ISPs)

Domain Name: smb.com (Required by some ISPs)

LAN Setting

MAC Address: 00 - 78 - 78 - 78 - 11 - CD (Default:00-78-78-78-11-cd)

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

Multiple Subnet Setting Multiple Subnet [Add / Edit](#)

WAN Setting

Interface	Connection Type	Config.
WAN1	Obtain an IP automatically	Edit
WAN2	Obtain an IP automatically	Edit
WAN3	Obtain an IP automatically	Edit
WAN4	Obtain an IP automatically	Edit

DMZ Setting

Interface	Connection Type	
DMZ	0.0.0.0	Edit

[Apply](#) [Cancel](#)

6.1.1 Host Name and Domain Name

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

6.1.2 LAN Setting

This is configuration information for the GIGABIT Router current LAN IP address. The default

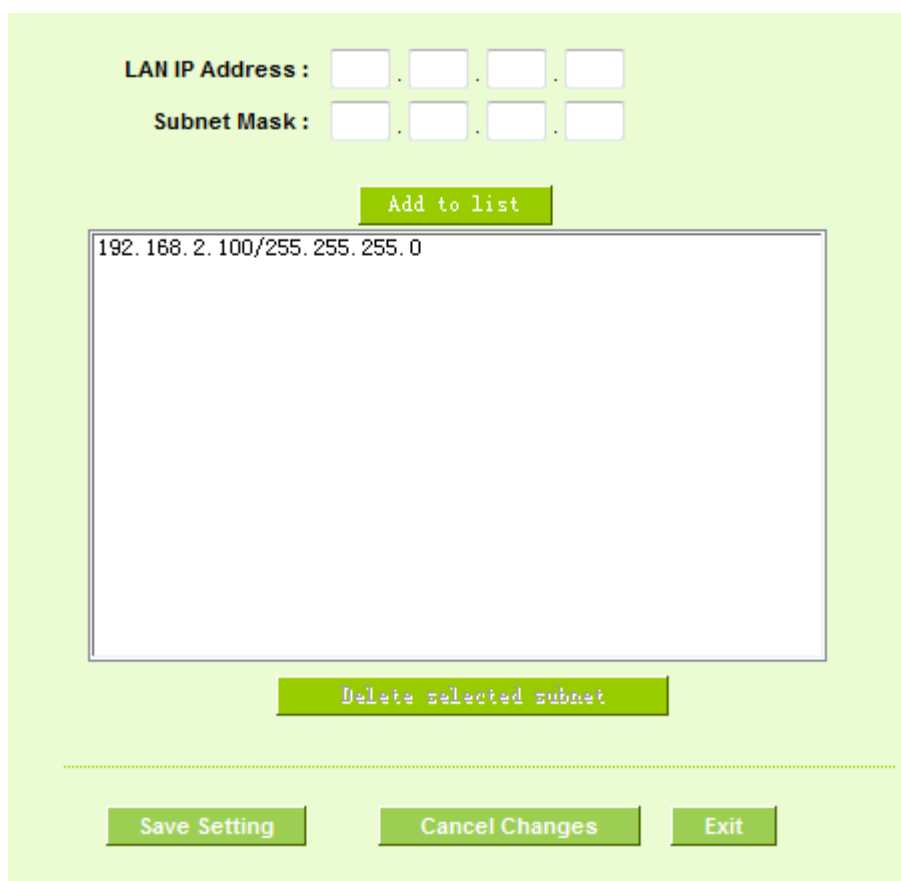
configuration is 192.168.1.1 and the default Subnet Mask is 255.255.255.0. It can be changed according to the actual network structure.

LAN Setting

MAC Address: 00 - 78 - 78 - 78 - 11 - CD (Default:00-78-78-78-11-cd)	
Device IP Address : 192 . 168 . 1 . 1	Subnet Mask : 255 . 255 . 255 . 0
Multiple Subnet Setting	<input checked="" type="checkbox"/> Multiple Subnet <input type="button" value="Add / Edit"/>
Subnet 1 : 192.168.2.100	

Multiple-Subnet Setting :

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



LAN IP Address : . . .

Subnet Mask : . . .

192.168.2.100/255.255.255.0

This function enables users to input IP segments that differ from the router network segment to the multi-net segment configuration; the Internet will then be directly accessible. In other words, if there are

already different IP segment groups in the Intranet, the Internet is still accessible without making any changes to internal PCs. Users can make changes according to their actual network structure.

6.1.3 WAN & DMZ Settings

WAN Setting :

▶ WAN Setting

Interface	Connection Type	Config.
WAN1	Obtain an IP automatically	Edit
WAN2	Obtain an IP automatically	Edit
WAN3	Obtain an IP automatically	Edit
WAN4	Obtain an IP automatically	Edit

Interface: An indication of which port is connected.

Connection Type: Obtain an IP automatically, Static IP connection, PPPoE (Point-to-Point Protocol over Ethernet), PPTP (Point-to-Point Tunneling Protocol) or Transparent Bridge.

Config.: A modification in an advanced configuration: Click Edit to enter the advanced configuration page.

Obtain an Automatic IP automatically:

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

Interface : WAN1

WAN Connection Type : Obtain an IP automatically ▼

Use the Following DNS Server Addresses:

DNS Server(Main) . . .

DNS Server(Sub) . . .

Back Apply Cancel

Use the following DNS Server Select a user-defined DNS server IP address.

Addresses:

DNS Server: Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable groups is two IP groups.

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

Static IP :

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

Interface : WAN1

WAN Connection Type : Static IP

WAN IP Address 220 . 130 . 188 . 42

Subnet Mask 255 . 255 . 255 . 240

WAN Default Gateway 220 . 130 . 188 . 33

DNS Server(Main) 168 . 95 . 1 . 1

DNS Server(Sub) 0 . 0 . 0 . 0

Back Apply Cancel

WAN IP address:	Input the available static IP address issued by ISP.
Subnet Mask:	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway:	Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.
DNS Server:	Input the DNS IP address issued by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.

After the changes are completed, click **“Apply”** to save the configuration, or click **“Cancel”** to leave

without making any changes.

PPPoE :

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

Interface : WAN1

WAN Connection Type : PPPoE

User Name:

Password:

Connect on Demand: Max Idle Time Min.

Keep Alive: Redial Period Sec.

User Name:	Input the user name issued by ISP.
Password	Input the password issued by ISP.
Connect on Demand:	This function enables the auto-dialing function to be used in a PPPoE dial connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break-off resulting from no packet transmissions is five minutes).
Keep Alive:	This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is disconnected. It also enables a user to set up a time for redialing. The default is 30 seconds.

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

PPTP :

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

Interface : WAN1

WAN Connection Type : PPTP

WAN IP Address: 220 . 130 . 188 . 42

Subnet Mask: 255 . 255 . 255 . 240

WAN Default Gateway: 220 . 130 . 188 . 33

User Name:

Password:

Connect on Demand: Max Idle Time Min.

Keep Alive: Redial Period Sec.

WAN IP Address:	This option is to configure a static IP address. The IP address to be configured could be one issued by ISP. (The IP address is usually provided by the ISP when the PC is installed. Contact ISP for relevant information).
Subnet Mask:	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway Address:	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
User Name:	Input the user name issued by ISP.
Password:	Input the password issued by ISP.
Connect on Demand:	This function enables the auto-dialing function to be used for a PPTP dial connection. When the client port attempts to connect with the Internet, the device will automatically connect with the default ISP auto dial

	connection; when the network has been idle for a period of time, the system will break the connection automatically. (The default time for automatic break off when no packets have been transmitted is five minutes).
Keep Alive:	This function enables the PPTP dial connection to redial automatically when the connection has been disconnected. Users can set up the redialing time. The default is 30 seconds.

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

Transparent Bridge :

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

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

Interface : WAN1

WAN Connection Type : Transparent Bridge

WAN IP Address: 220 . 130 . 188 . 42

Subnet Mask: 255 . 255 . 255 . 240

WAN Default Gateway: 220 . 130 . 188 . 33

DNS Server(Main): 168 . 95 . 1 . 1

DNS Server(Sub): 0 . 0 . 0 . 0

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

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

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

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

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

Back Apply Cancel

WAN IP Address:	Input one of the static IP addresses issued by ISP.
Subnet Mask :	Input the subnet mask of the static IP address issued by ISP, such as: Issued eight static IP addresses: 255.255.255.248 Issued 16 static IP addresses: 255.255.255.240
Default Gateway Address :	Input the default gateway of the static IP address issued by ISP. For ADSL users, it is usually an ATU-R IP address.
DNS Server :	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.
Internal LAN IP Range :	Input the available IP range issued by ISP. If ISP issued two discontinuous IP address ranges, users can input them into Internal LAN IP Range 1 and Internal LAN IP Range 2 respectively.

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

Router Plus NAT Mode :

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

reach the Internet.

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

Interface :

WAN Connection Type : Router Plus NAT Mode ▾

WAN IP Address . . .

Subnet Mask: . . .

WAN Default Gateway . . .

DNS Server(Main) . . .

DNS Server(Sub) . . .

LAN Default Gateway1: . . .

LAN (Public) IP Range1: . . . to

LAN (Public) IP Range2: . . . to

LAN Default Gateway2: . . .

LAN (Public) IP Range1: . . . to

LAN (Public) IP Range2: . . . to

LAN Default Gateway3: . . .

LAN (Public) IP Range1: . . . to

LAN (Public) IP Range2: . . . to

- WAN IP address :** Enter the public IP address.
- Subnet mask :** Enter the public IP address subnet mask.
- WAN default gateway :** Enter the WAN default gateway, which provided by your ISP.
- DNS Servers :** Enter the DNS server IP address, you must have to enter a DNS server IP address, maximum two DNS servers IP addresses available..
- Intranet routing default gateway :** Enter one of IP addresses that provide by the ISP as your default gateway.

Intranet IP addresses range : Enter your IP addresses range, which IP addresses are provided by ISP. If you have multiple IP ranges, you need setup group1 and group 2.
You can also setup the default gateway and IP range in the group 2.

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

DMZ Setting :

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

For some Qno models, the WAN5 and DMZ port can be configurable each other. You can depend on the real environment to choose which the port is WAN5 or DMZ.

enable DMZ

DMZ Setting

Interface	Connection Type	
DMZ	0.0.0.0	Edit

IP address: Indicates the current default static IP address.

Config.: Indicates an advanced configuration modification: Click **Edit** to enter the advanced configuration page.

The DMZ configuration can be classified by Subnet, Range and DMZ IP ranges are the same with WAN IP ranges in Router Plus NAT mode :

Subnet :

The DMZ and WAN located in different Subnets

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

group with the other group in the DMZ.

Interface :

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

Specify DMZ IP Address: . . .

Subnet Mask: . . .

DMZ IP Address: Enter the DMZ Port IP Address
Subnet Mask: Enter the DMZ Port Subnet Mask

Range :

DMZ and WAN are within same Subnet

Interface :

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

Interface :

IP Range for DMZ port: . . . to

Interface : Select a WAN Port witch is the same subnet with DMZ
IP Range : Input the IP range located at the DMZ port.

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

Interface :

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

Interface :

LAN Default Gateway1: . . .

LAN (Public) IP Range . . . to

LAN Default Gateway2: . . .

LAN (Public) IP Range . . . to

LAN Default Gateway3: . . .

LAN (Public) IP Range . . . to

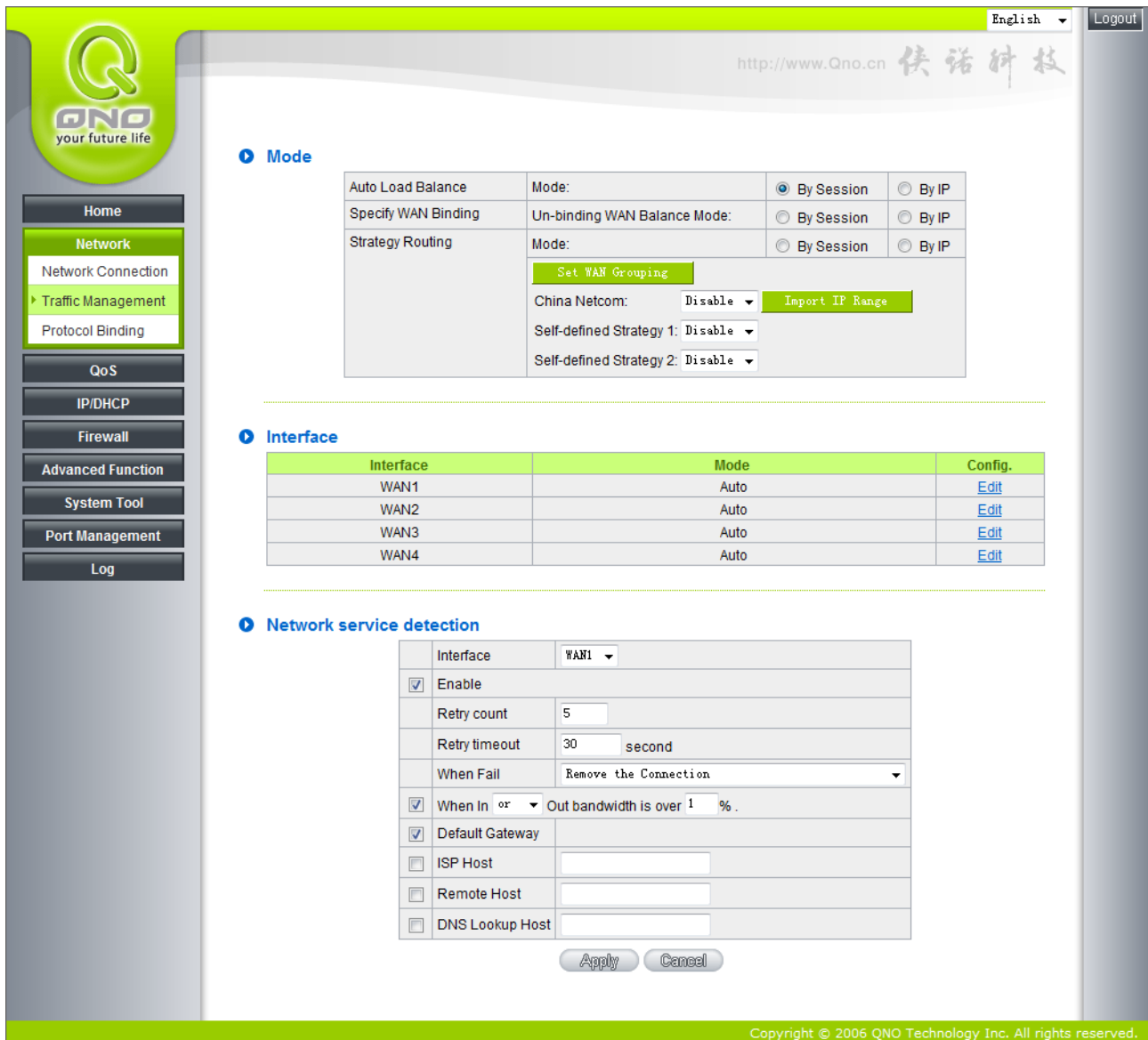
LAN Default Gateway : Enter the LAN Default Gateway that you configured at Router Plus NATMode

LAN IP Range : Enter the usable static IP range that provide by ISP into the DMZ service IP range.
If you have other IP range, you can setup the default gateway and IP range into group 2.

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

6.2 Multi- WAN Setting

When you have multiple WAN gateways, you can use Traffic Mangement and Protocol Binding function to fullfil WAN road balancing, so that we can have highest network bandwidth efficiency.



The screenshot shows the QNO router's web management interface. The left sidebar contains navigation buttons: Home, Network (with sub-items: Network Connection, Traffic Management, Protocol Binding), QoS, IP/DHCP, Firewall, Advanced Function, System Tool, Port Management, and Log. The main content area is titled 'Mode' and contains the following settings:

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session	<input type="radio"/> By IP
Specify WAN Binding	Un-binding WAN Balance Mode:	<input type="radio"/> By Session	<input type="radio"/> By IP
Strategy Routing	Mode:	<input type="radio"/> By Session	<input type="radio"/> By IP

Below these are 'Set WAN Grouping' options:

- China Netcom:
- Self-defined Strategy 1:
- Self-defined Strategy 2:

The 'Interface' section shows a table of WAN interfaces:

Interface	Mode	Config.
WAN1	Auto	Edit
WAN2	Auto	Edit
WAN3	Auto	Edit
WAN4	Auto	Edit

The 'Network service detection' section is configured for WAN1:

- Interface: WAN1
- Enable
- Retry count: 5
- Retry timeout: 30 second
- When Fail: Remove the Connection
- When In or Out bandwidth is over 1 %
- Default Gateway
- ISP Host
- Remote Host
- DNS Lookup Host

Buttons for 'Apply' and 'Cancel' are at the bottom of the detection settings.

Copyright © 2006 QNO Technology Inc. All rights reserved.

6.2.1 Load Balance Mode

Mode

Auto Load Balance	Mode:	<input checked="" type="radio"/> By Session	<input type="radio"/> By IP
Specify WAN Binding	Un-binding WAN Balance Mode:	<input type="radio"/> By Session	<input type="radio"/> By IP
Strategy Routing	Mode:	<input type="radio"/> By Session	<input type="radio"/> By IP
Set WAN Grouping			
	China Netcom:	Disable ▾	Import IP Range
	Self-defined Strategy 1:	Disable ▾	
	Self-defined Strategy 2:	Disable ▾	

Auto Load Balance Mode :

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

- **Session Balance:** If “By Session” is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.

IP Session Balance: If “By IP” is selected, the WAN bandwidth will automatically allocate connections based on IP amount to achieve network load balance.

Note!

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

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

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

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

Exclusive Mode

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

Un-binding interfaces load balancing mode:

If you don't specified IP address、TCP/UDP port or destination IP addresses in WAN ports, you can still use "Session Balance" and "IP Balance" mechanisms to fullful load balancing. Detail of these two mechanisms are as following.

Session Balance: If "By Session" is selected, the WAN bandwidth will automatically allocate connections based on session number to achieve network load balance.

IP Balance: If "By IP" is selected, the WAN bandwidth will automatically allocate connections based on the number of IP addresses to achieve network load balance.

Note!

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

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

other WAN ports to connect with the Internet.

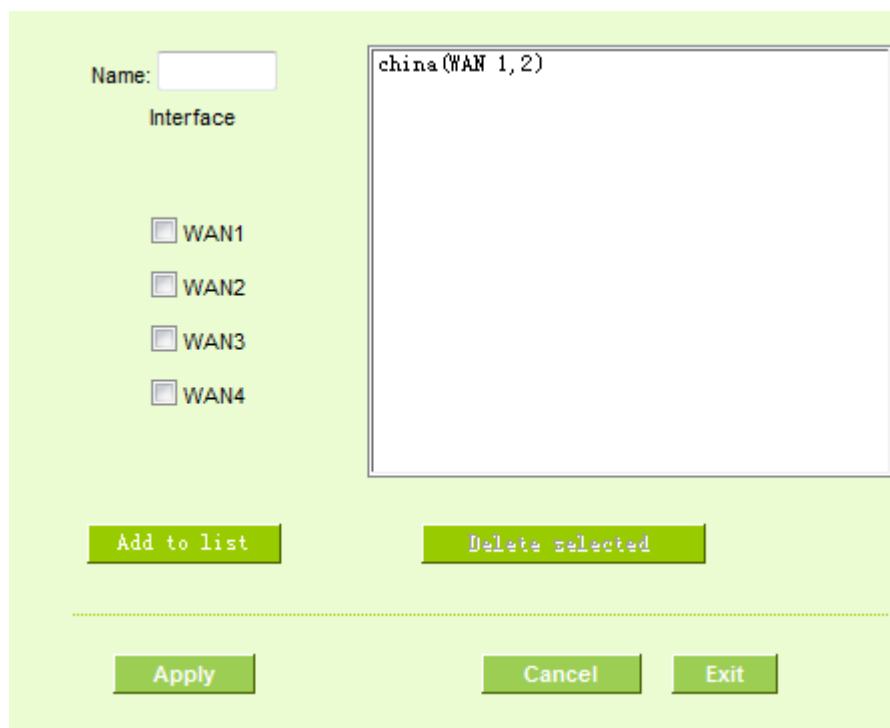
Please refer to the explanations in **6.2.3 Configuring Protocol Binding** for setting up Protocol Binding and for examples of collocating router mode with Protocol Binding.

Strategy Routing Mode :

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

Set WAN Grouping:

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



The screenshot shows a configuration window with a light green background. At the top left, there is a 'Name:' label followed by an empty text input box. Below this is the label 'Interface'. Underneath, there are four checkboxes labeled 'WAN1', 'WAN2', 'WAN3', and 'WAN4', all of which are currently unchecked. To the right of these checkboxes is a large rectangular text area containing the text 'china(WAN 1,2)'. Below the text area, there are two buttons: 'Add to list' on the left and 'Delete selected' on the right. At the bottom of the window, there are three buttons: 'Apply' on the left, 'Cancel' in the middle, and 'Exit' on the right.

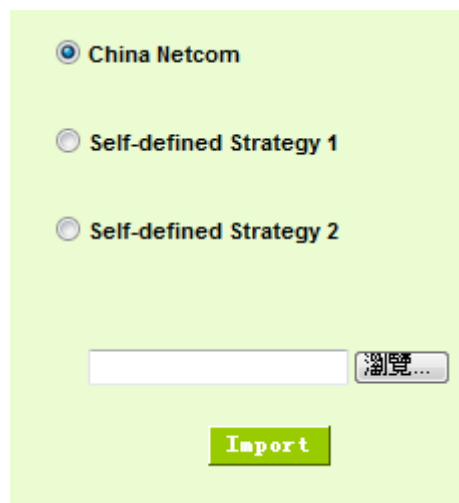
Name:	To define a name for the WAN grouping in the box, such as
-------	---

	“Education” etc. The name is for recognizing different WAN groups.
Interface:	Check the boxes for the WANs to be added into this combination.
Add To List:	To add a WAN group to the grouping list.
Delete selected Item:	To remove selected WANs from the WAN grouping.
Apply:	Click “Apply” to save the modification.
Close:	Click “Cancel” to cancel the modification. This only works before “Apply” is clicked.

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

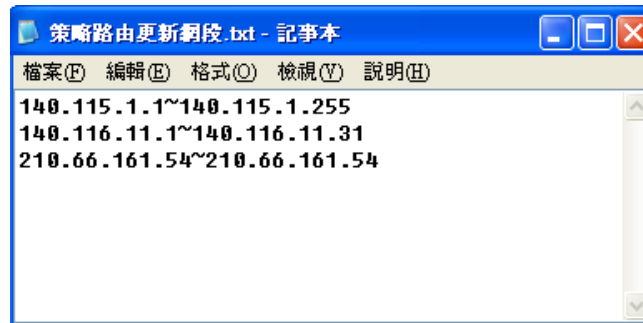
Import Strategy: :

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



To build a policy document users can use a text-based editor, such as Notepad, which is included with Windows system. Follow the text format in the figure below to key in the destination IP addresses users want to assign. For example, if the destination IP address range users want to designate is 140.115.1.1 ~ 140.115.1.255, key in 140.115.1.1 ~ 140.115.1.255 in Notepad. The next destination IP address range should

be keyed in the next line. Attention! Even if only one destination IP address is to be assigned, it should follow the same format. For example, if the destination IP address is 210.66.161.54, it should be keyed in as 210.66.161.54~210.66.161.54. After the document has been saved (the extension file name is .txt), users can import the IP range of self-defined strategy.



Note!

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

6.2.2 Network Detection Service

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

Network service detection

Interface	WAN1
<input checked="" type="checkbox"/> Enable	
Retry count	5
Retry timeout	30 second
When Fail	Remove the Connection
<input checked="" type="checkbox"/> When In or Out bandwidth is over 1 %	
<input checked="" type="checkbox"/> Default Gateway	
<input type="checkbox"/> ISP Host	
<input type="checkbox"/> Remote Host	
<input type="checkbox"/> DNS Lookup Host	

Apply Cancel

Interface:	Select the WAN Port that enables Network Service Detection.
Retry:	This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured "Retry Times", it will be judged as "External Connection Disconnected".
Retry Timeout:	Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.
When Fail:	<p>(1) Generate the Error Condition in the System Log: If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections.</p> <p>This option is suitable under the condition that one of the WAN connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination. For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 is not to support these destinations, users should select this option. When the WAN1 connection is disconnected, packets for 10.0.0.1~10.254.254.254 cannot be transmitted through WAN 2, and there is no need to remove the connection when WAN 1 is disconnected.</p> <p>(2) Keep System Log and Remove the Connection: If an ISP</p>

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

Note !

In the load balance mode for Assigned Routing, the first WAN port (WAN1) will be saved for the traffic of the IP addresses or the application service ports that are not assigned to other WANs (WAN2, WAN3, and WAN4). Therefore, in this mode, we recommend assigning one of the connections to the

first WAN. When other WANs (WAN2, WAN3, or WAN4) are broken and connection error remove (Remove the Connection) has been selected for the connection detection system, traffic will be shifted to the first WAN (WAN1). In addition, if the first WAN (WAN1) is broken, the traffic will be shifted to other WANs in turn. For example, the traffic will be shifted to WAN2 first; if WAN2 is broken too, the traffic will be shifted to WAN3, and so on.

6.2.3 Protocol Binding

Interface Configuration

GIGABIT Router allows maximum four WAN interface, the bandwidth and real connection of every WAN will impact the load balance mechanism, therefore you need to set the Bandwidth and the Network service detection by each WAN Port correctly.

In “**Interface Configuration**”, click “**Edit**” to enter the WAN port configuration.

WAN Setting

Interface	Connection Type	Config.
WAN1	Static IP	Edit
WAN2	Obtain an IP automatically	Edit
WAN3	Obtain an IP automatically	Edit
WAN4	Obtain an IP automatically	Edit

Bandwidth Configuration

When Auto Load Balance mode is selected, the device will select sessions or IP and the WAN bandwidth will automatically allocate connections to achieve load balancing for external connections. The network bandwidth is set by what users input for it. For example, if the upload bandwidth of both WANs is 512Kbit/sec, the automatic load ratio will be 1:1; if one of the upload bandwidths is 1024Kbit/sec, while the other is 512Kbit/sec, the automatic load ratio will be 2:1. Therefore, to ensure that the device can balance the actual network load, please input real upload and download bandwidths. The section refers to QoS configuration. Therefore, it should be set in QoS page. Please refer to 8.1 QoS bandwidth configuration.

Interface :

The Max. Bandwidth provided by ISP : Upstream Kbit/Sec Downstream Kbit/Sec

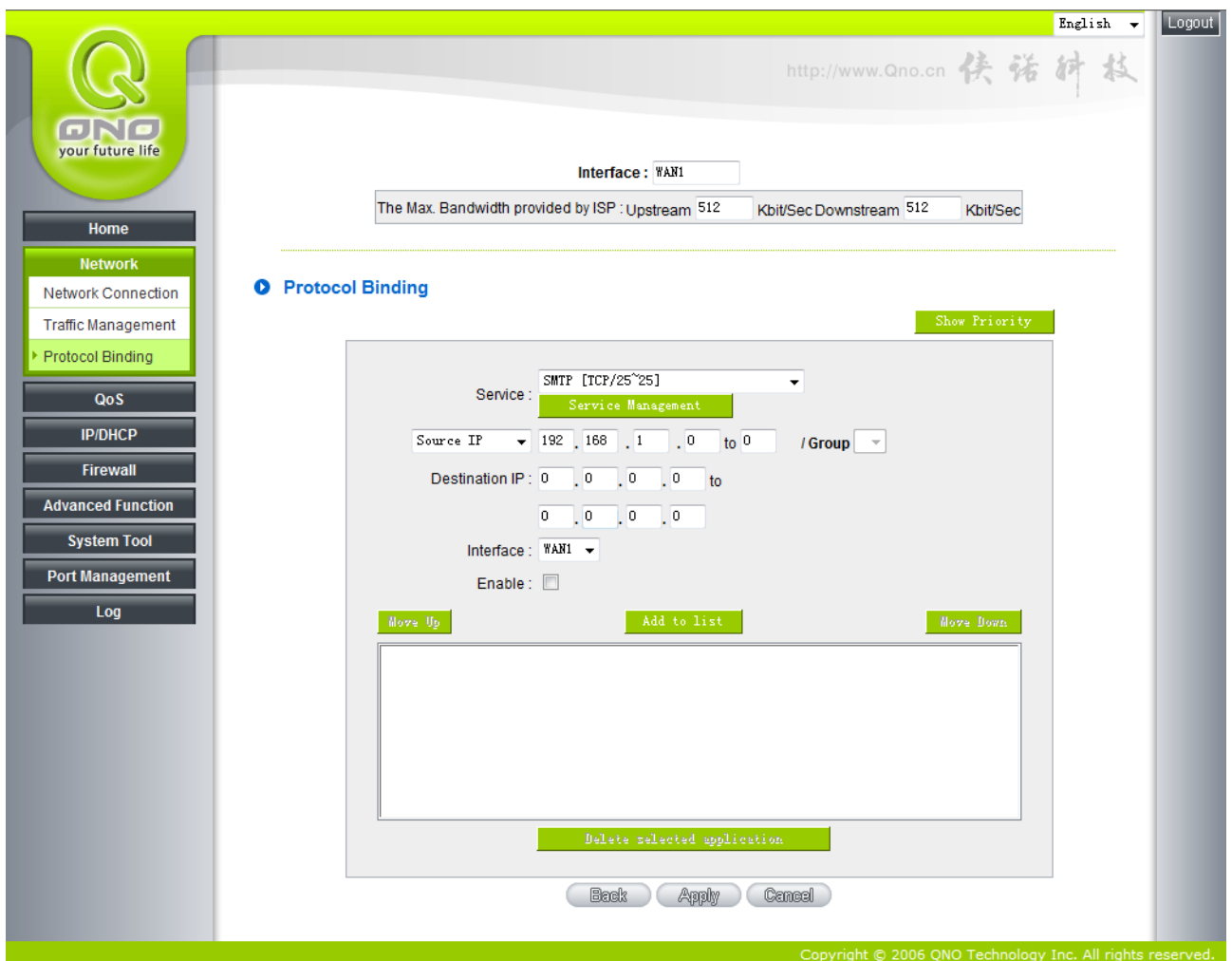
Protocol Binding

Users can define specific IP addresses or specific application service ports to go through a user-assigned

WAN for external connections. For any other unassigned IP addresses and services, WAN load balancing will still be carried out.

Note !

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



The screenshot displays the QNO router's web management interface. On the left is a sidebar with a navigation menu containing: Home, Network (with sub-items: Network Connection, Traffic Management, Protocol Binding), QoS, IP/DHCP, Firewall, Advanced Function, System Tool, Port Management, and Log. The main content area is titled 'Protocol Binding' and shows configuration for interface 'WAN1'. It includes a 'Service' dropdown set to 'SMTP [TCP/25~25]', a 'Source IP' field set to '192.168.1.0 / Group', and a 'Destination IP' field set to '0.0.0.0'. Below these are 'Interface' (WAN1) and 'Enable' (unchecked) options. Action buttons include 'Move Up', 'Add to list', 'Move Down', and 'Delete selected application'. At the bottom are 'Back', 'Apply', and 'Cancel' buttons. The footer contains the copyright notice: 'Copyright © 2006 QNO Technology Inc. All rights reserved.'

Service:	This is to select the Binding Service Port to be activated. The default (such as ALL-TCP&UDP 0~65535, WWW 80~80, FTP 21 to 21, etc.) can be selected from the pull-down option list. The default Service is All 0~65535. Option List for Service Management: Click the button to enter the Service Port configuration page to add or remove default Service Ports on the option list.
Source IP:	Users can assign packets of specific Intranet virtual IP to go through a specific WAN port for external connection. In the boxes here, input the Intranet virtual IP address range; for example, if 192.168.1.100~150 is input, the binding range will be 100~150. If only specific Service Ports need to be designated, while specific IP designation is not necessary, input "0" in the IP boxes.
Destination IP:	In the boxes, input an external static IP address. For example, if connections to destination IP address 210.11.1.1 are to be restricted to WAN1, the external static IP address 210.1.1.1 ~ 210.1.1.1 should be input. If a range of destinations is to be assigned, input the range such as 210.11.1.1 ~ 210.11.255.254. This means the Class B Network Segment of 210.11.x.x will be restricted to a specific WAN. If only specific Service Ports need to be designated, while a specific IP destination assignment is not required, input "0" into the IP boxes.
Interface:	Select the WAN for which users want to set up the binding rule.
Enable:	To activate the rule.
Add To List:	To add this rule to the list.
Delete selected application:	To remove the rules selected from the Service List.
Moving Up & Down:	The priority for rule execution depends on the rule order in the list. A rule located at the top will be executed prior to those located below it. Users can arrange the order according to their priorities.

Note !

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

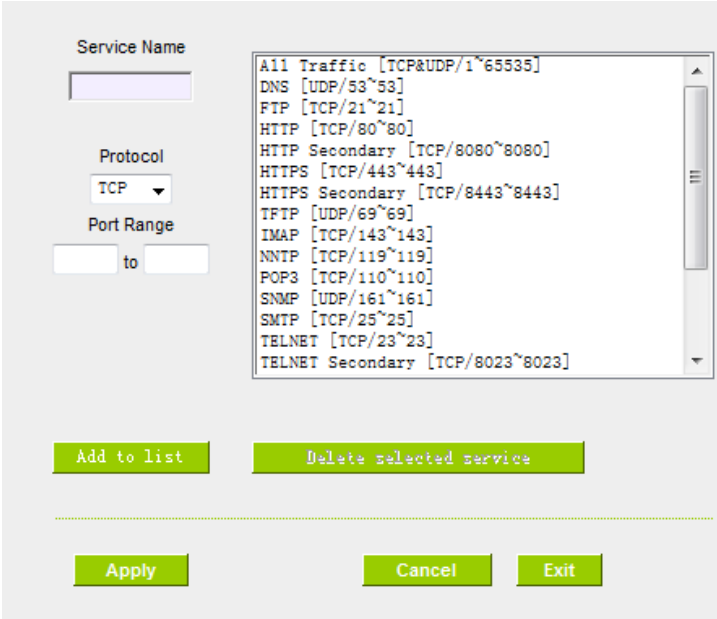
Show Table :

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

Summary						
		<input checked="" type="radio"/> Priority <input type="radio"/> Interface			<input type="button" value="Refresh"/> <input type="button" value="Close"/>	
Priority	Interface	Service	Source IP	Destination IP	Enable	Edit
1	WAN1	All Traffic[TCP&UDP/1~65535]	192.168.1.100~192.168.1.100	0.0.0.0~0.0.0.0	Enabled	Edit

Add or Remove Service Port

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



Service Name:	In this box, input the name of the Service Port which users want to activate, such as BT, etc.
Protocol:	This option list is for selecting a packet format, such as TCP or UDP for the Service Ports users want to activate.

Port range:	In the boxes, input the range of Service Ports users want to add.
Add To List:	Click the button to add the configuration into the Services List. Users can add up to 100 services into the list.
Delete selected service:	To remove the selected activated Services.
Apply:	Click the “Apply” button to save the modification.
Cancel:	Click the “Cancel” button to cancel the modification. This only works before “Apply” is clicked.
Close:	To quit this configuration window.

Auto Load Balancing mode when enabled :

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

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

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

Show Priority

Service: SMTP [TCP/25~25] Service Management

Source IP: 192 . 168 . 1 . 0 to 0 / Group ▼

Destination IP: 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Interface: WAN1 ▼

Enable:

Move Up
Add to list
Move Down

```
All Traffic [TCP&UDP/1~65535]->192.168.1.100~100 (0.0.0.0~0.0.0.0)WAN1
```

Delete selected application

Back Apply Cancel

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

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

[Show Priority](#)

Service: HTTP [TCP/80~80] Service Management

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

Destination IP: 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Interface: WAN2

Enable:

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

HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN2

[Delete selected application](#)
[Add New](#)

[Back](#)
[Apply](#)
[Cancel](#)

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

As in the figure below, there are two rules to be configured. The first rule: select “HTTP [TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of Source IP input “192.168.1.0” to “0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets to Port 80 through WAN2. However, with only the above rule, packets that do not go to Port 80 may be transmitted through WAN2; therefore, a second rule is necessary. The second rule: Select “All Ports [TCP&UDP/1~65535]” from the pull-down option list “Service”, and then input “192.168.1.2 ~ 254” in the boxes of “Source IP”. Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (which means to include all Internet IP addresses). Select WAN1 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. The device will transmit packets that are not going to Port 80 to the Internet through WAN1.

[Show Priority](#)

Service: HTTP [TCP/80~80] [Service Management](#)

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

Destination IP: 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Interface: WAN2

Enable:

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

```
HTTP [TCP/80~80]->192.168.1.150~200(0.0.0.0~0.0.0.0)WAN2
All Traffic [TCP&UDP/1~65535]->192.168.1.2~254(0.0.0.0~0.0.0.0)WAN1
```

[Delete selected application](#)
[Add New](#)

[Back](#)
[Apply](#)
[Cancel](#)

Configuring “Assigned Routing Mode” for load Balance :

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

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

As in the figure below, select “HTTP[TCP/80~80]” from the pull-down option list “Service”, and then in the boxes of “Source IP” input “192.168.1.0 ~ 0” (which means to include all Intranet IP addresses). Retain the original numbers “0.0.0.0” in the boxes of “Destination IP” (Which means to include all Internet IP addresses). Select WAN2 from the pull-down option list “Interface”, and then click “Enable”. Finally, click “Add New” and the rule will be added to the mode. After the rule is set up, only packets that go to Port 80 will be transmitted through WAN2, while other traffics will be transmitted through WAN1.

Show Priority

Service: HTTP [TCP/80~80] Service Management

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

Destination IP: 0 . 0 . 0 . 0 to
0 . 0 . 0 . 0

Interface: WAN2

Enable:

Move Up
Update this Application
Move Down

HTTP [TCP/80~80]->192.168.1.0/24(0.0.0.0/0.0.0.0)WAN2

Delete selected application
Add New

Back Apply Cancel

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

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

[Show Priority](#)

Service: SMTP [TCP/25~25] [Service Management](#)

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

Destination IP: 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

Interface: WAN2

Enable:

[Move Up](#) [Add to list](#) [Move Down](#)

```
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0 (211.1.1.1~211.254.254.254)WAN2
All Traffic [TCP&UDP/1~65535]->192.168.1.0~0 (60.1.1.1~60.254.254.254)WAN2
```

[Delete selected application](#)

[Back](#) [Apply](#) [Cancel](#)

VII · Intranet Configuration

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

7.1 Port Management

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



Port Setup

Enable Port 1 as Mirror Port

Port ID	Interface	Disable	Priority	Speed	Duplex	Auto Neg.	VLAN
1	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
2	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
3	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
4	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
5	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
6	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
7	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
8	LAN	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	VLAN1
9	WAN4	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	
10	WAN3	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	
11	WAN2	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	
12	WAN1	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	
13	DMZ	<input type="checkbox"/>	Normal	<input type="radio"/> 10M <input checked="" type="radio"/> 100M	<input type="radio"/> Half <input checked="" type="radio"/> Full	<input checked="" type="checkbox"/> Enable	

Apply Cancel

Copyright © 2006 QNO Technology Inc. All rights reserved.

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

Physical Port Status

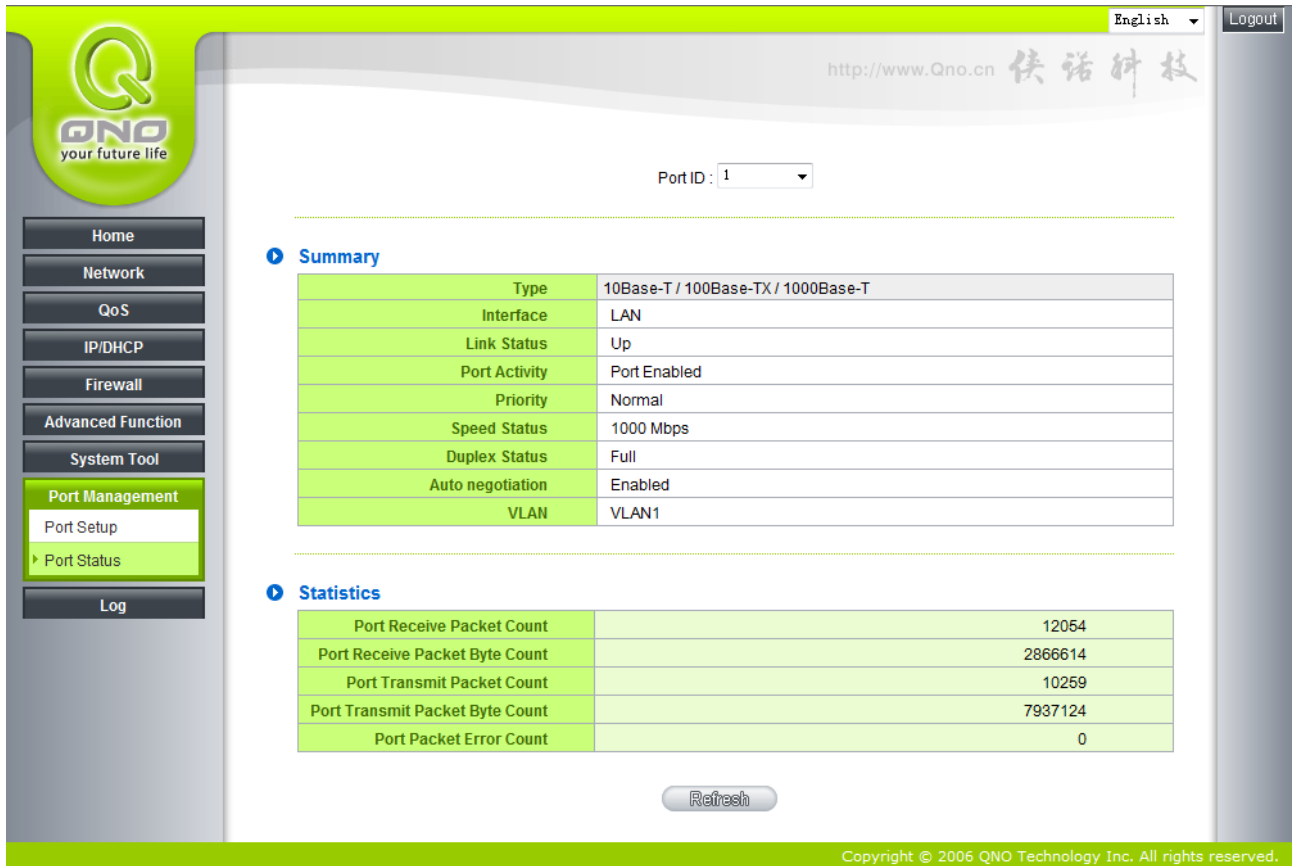
Port ID	1	2	3	4	5	6	7	8
Interface	Mirror Port	LAN						
Status	Connected	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

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

Disabled :	This feature allows users turn on/off the Ethernet port. If selected, the Ethernet port will be shut down immediately and no connection can be made. The default value is "on".
Priority :	This feature allows users to set the high/low priority of the packet delivery for the Ethernet port. If it is set as High, the port has the first priority to deliver the packet. The default value is "Normal".
Speed :	This feature allows users to select the network hardware connection speed for the Ethernet port. The options are 10Mbps and 100Mbps.
Duplex Status :	This feature allows users to select the network hardware connection speed working mode for the Ethernet. The options are full duplex and half duplex.
Auto Neg. :	The Auto-Negotiation mode can enable each port to automatically adjust and gather the connection speed and duplex mode. Therefore, if Enabled Auto-Neg. selected, the ports setup will be done without any manual setting by administrators.
VLAN :	This feature allows administrators to set the LAN port to be one or more disconnected network sessions. All of them will be able to log on to the Internet through the device. Members in the same network session (within the same VLAN) can see and communicate with each other. Members in different VLAN will not know the existence of other members.
VLAN All :	Set VLAN All port to be the public area of VLAN so that it can be connected to other VLAN networks. A server should be constructed for the intranet so that all VLAN group can visit this server. Set one of the network ports as VLAN All. Connect the server to VLAN All so that computers of different VLAN groups can be connected to this server. Moreover, the port where the administrator locates must be set as VLAN All so that it can be connected to the entire network to facilitate network management.

7.2 Port Status

This function allows network managers to review the detail information of each port. introduces how to configure ports and understand how to configure intranet IP addresses.



English Logout

http://www.Qno.cn 侠诺科技

Port ID: 1

Summary

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

Statistics

Port Receive Packet Count	12054
Port Receive Packet Byte Count	2866614
Port Transmit Packet Count	10259
Port Transmit Packet Byte Count	7937124
Port Packet Error Count	0

Refresh

Copyright © 2006 QNO Technology Inc. All rights reserved.

Summary :

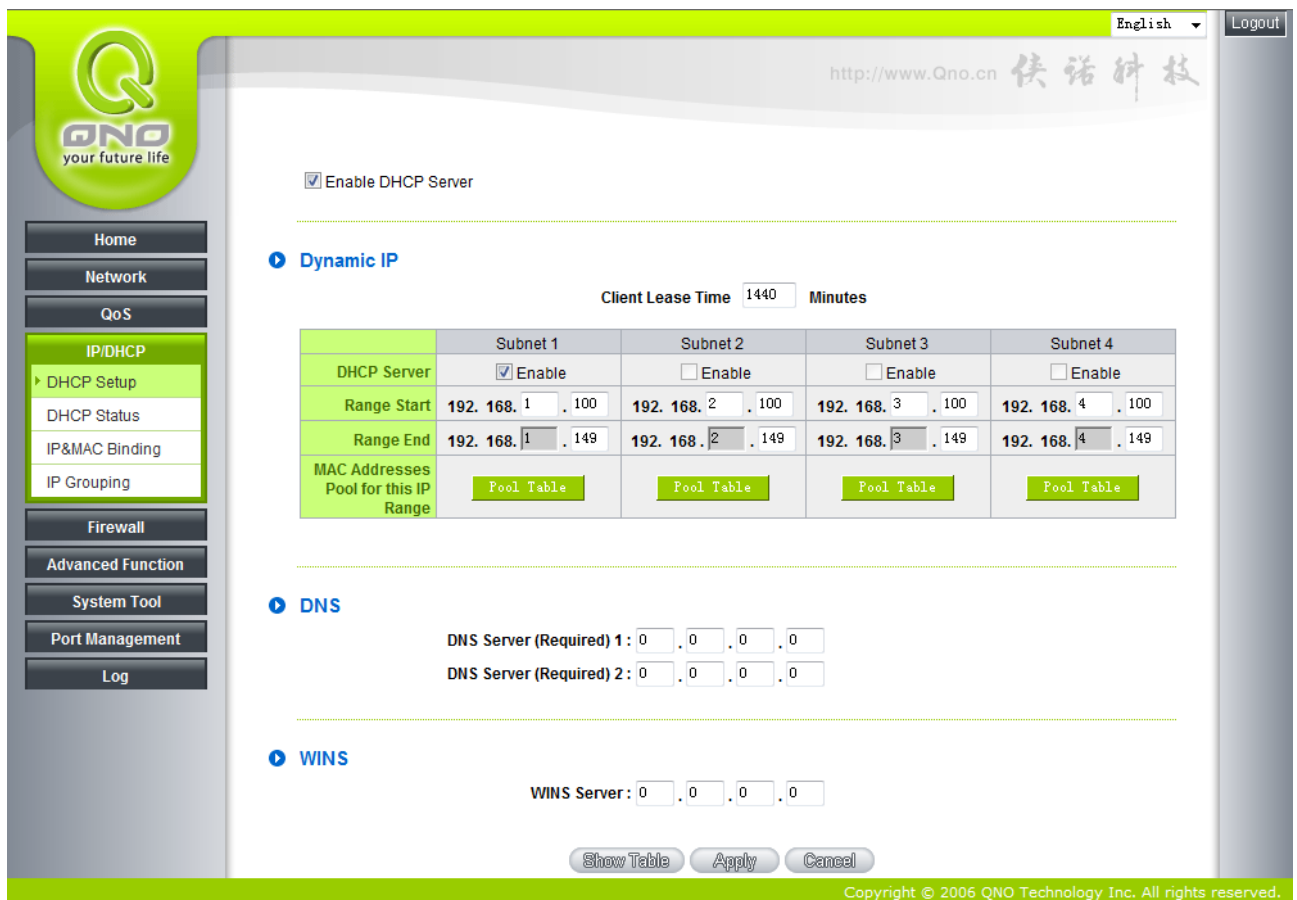
There are Network Connection Type, Interface(LAN/WAN1~4/DMZ), Link Status (Up/Down), Port Activity (Port Enabled), Priority Setting (High or Normal), Speed Status (10Mbps or 100Mbps), Duplex Status (half duplex or full duplex), Auto Neg. (Enabled/Disabled), and VLAN(VLAN1~8/VLAN All).

Statistics :

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

7.3 IP/ DHCP

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



English Logout
http://www.Qno.cn 供诺科技

Enable DHCP Server

Dynamic IP

Client Lease Time Minutes

	Subnet 1	Subnet 2	Subnet 3	Subnet 4
DHCP Server	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable
Range Start	192. 168. 1 . 100	192. 168. 2 . 100	192. 168. 3 . 100	192. 168. 4 . 100
Range End	192. 168. 1 . 149	192. 168. 2 . 149	192. 168. 3 . 149	192. 168. 4 . 149
MAC Addresses Pool for this IP Range	Pool Table	Pool Table	Pool Table	Pool Table

DNS

DNS Server (Required) 1 : . . .

DNS Server (Required) 2 : . . .

WINS

WINS Server : . . .

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

Copyright © 2006 QNO Technology Inc. All rights reserved.

Dynamic IP :

Client lease Time : This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Client PC will acquire again after the lease time is expiration. Users can change it according to their needs. The time unit is minute.

Range Start : This is to set up a lease time for the IP address which is acquired by a PC. The default is 1440 minutes (a day). Users can change it according to their needs. The time unit is minute.

Range End : This is an initial IP automatically leased by DHCP. It means DHCP will start the lease from this IP. The default initial IP is 192.168.1.100.

DNS (Domain Name Service) :

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

DNS Server (Required) 1 : Input the IP address of the DNS server.

DNS Server (Required) 2 : Input the IP address of the DNS server.

WINS :

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

WINS Server : Input the IP address of WINS.

Apply : Click "**Apply**" to save the network configuration modification.

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

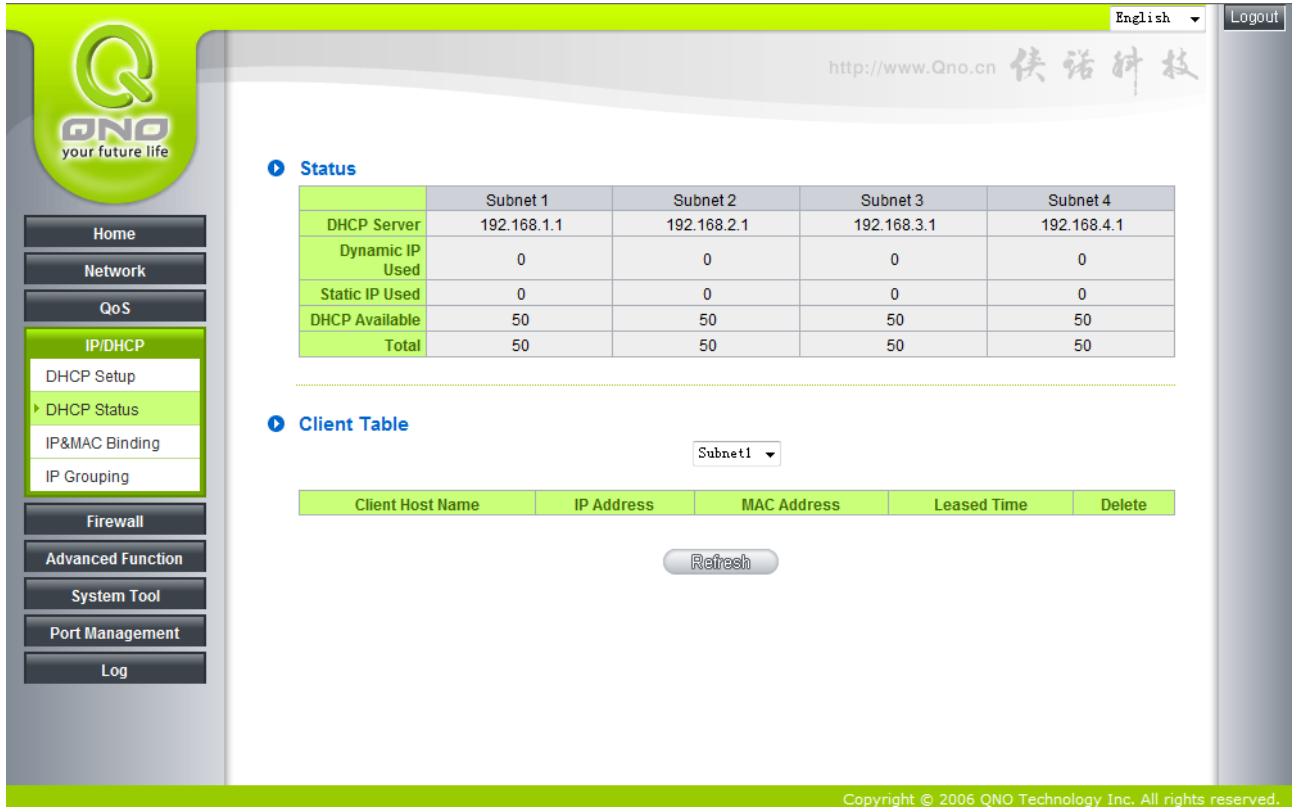
Show Table :

This is for the status of showing whole MAC/IP binding list that has configured and you can choose "Edit" to modify it.

IP & MAC binding List				Apply	Select All	Refresh	Close
IP	MAC	Name	Enable				
192.168.1.110	00:1f:c6:7b:8a:bd	<input type="text"/>	<input checked="" type="checkbox"/>				

7.4 DHCP Status

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



English Logout

http://www.Qno.cn 快诺科技

Status

	Subnet 1	Subnet 2	Subnet 3	Subnet 4
DHCP Server	192.168.1.1	192.168.2.1	192.168.3.1	192.168.4.1
Dynamic IP Used	0	0	0	0
Static IP Used	0	0	0	0
DHCP Available	50	50	50	50
Total	50	50	50	50

Client Table

Subnet1

Client Host Name	IP Address	MAC Address	Leased Time	Delete
------------------	------------	-------------	-------------	--------

Refresh

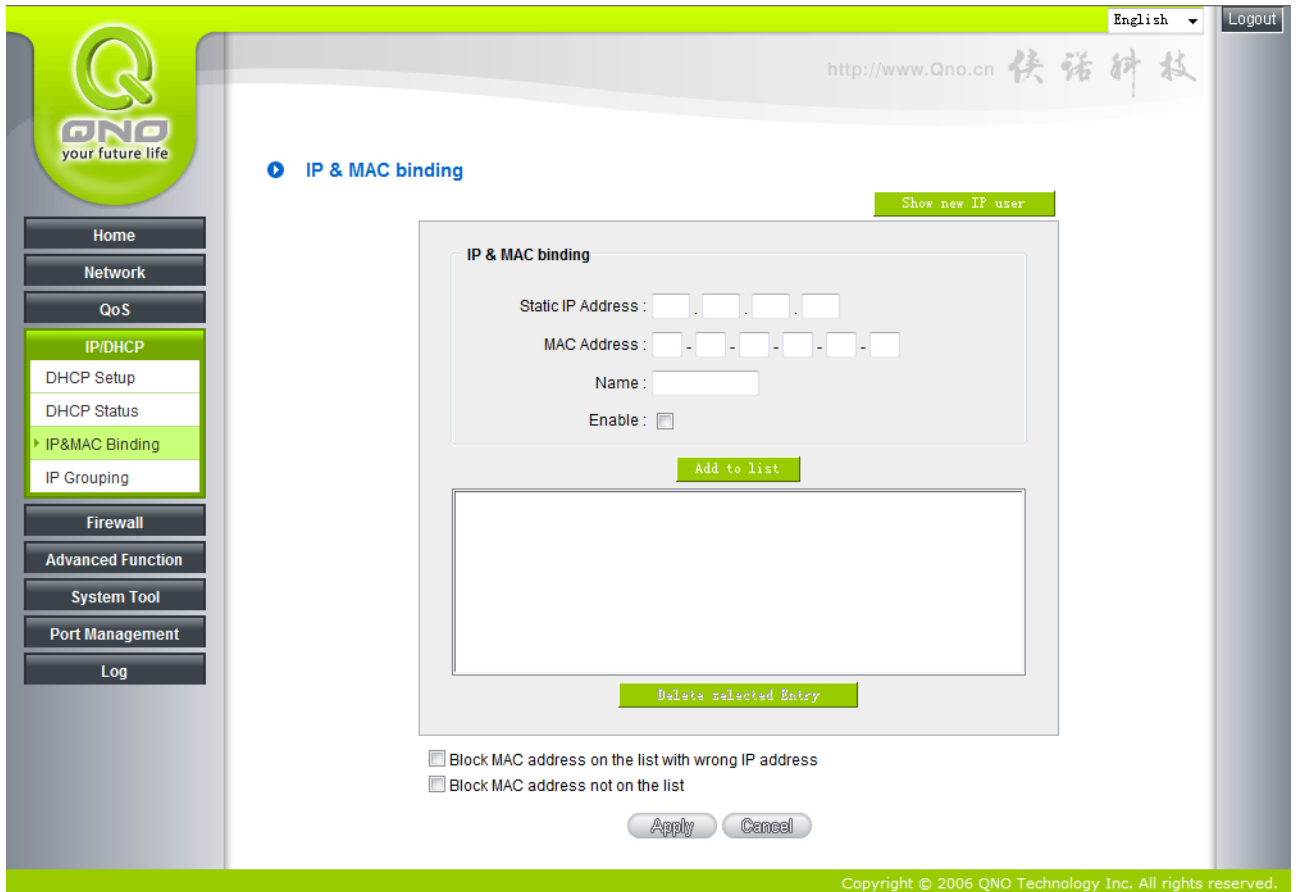
Copyright © 2006 QNO Technology Inc. All rights reserved.

DHCP Server :	This is the current DHCP IP.
Dynamic IP Used :	The amount of dynamic IP leased by DHCP.
Static IP Used :	The amount of static IP assigned by DHCP.
IP Available :	The amount of IP still available in the DHCP server.
Total IP :	The total IP which the DHCP server is configured to lease.
Host Name :	The name of the current computer.
IP Address :	The IP address acquired by the current computer.
MAC Address :	The actual MAC network location of the current computer.

Client Lease Time :	The lease time of the IP released by DHCP.
Delete :	Remove a record of an IP lease.

7.5 IP & MAC Binding

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



There are two methods for setting up this function :

Block MAC address on the list with wrong IP address : This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access.

Block MAC address not on the list : This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access. When this method is applied, please fill out Static IP with 0.0.0.0, as the figure

IP & MAC binding

Show new IP user

IP & MAC binding

Static IP Address : . . .

MAC Address : - - - - -

Name :

Enable :

Add to list

192.168.1.110 => 00-1f-c6-7b-8a-bd=>Enabled

Delete selected Entry

Block MAC address on the list with wrong IP address

Block MAC address not on the list

Apply Cancel

<p>Static IP :</p>	<p>There are two ways to input static IP:</p> <ol style="list-style-type: none"> 1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a specific assigned IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty.
--------------------	--

	2. If users want DHCP to assign a static IP for a PC every single time, users should input the IP address users want to assign to this computer in the boxes. The server or PC which is to be bound will then acquire a static virtual IP whenever it restarts.
MAC Address :	Input the static real MAC (the address on the network card) for the server or PC which is to be bound.
Name :	For distinguishing clients, input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
Enabled :	Activate this configuration.
Add to list :	Add the configuration or modification to the list.
Delete selected item :	Remove the selected binding from the list.
Add :	Add new binding.

Block MAC address on the list with wrong IP address : This method only allows MAC addresses on the list to receive IP addresses from DHCP and have Internet access.

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

Show New IP user :

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

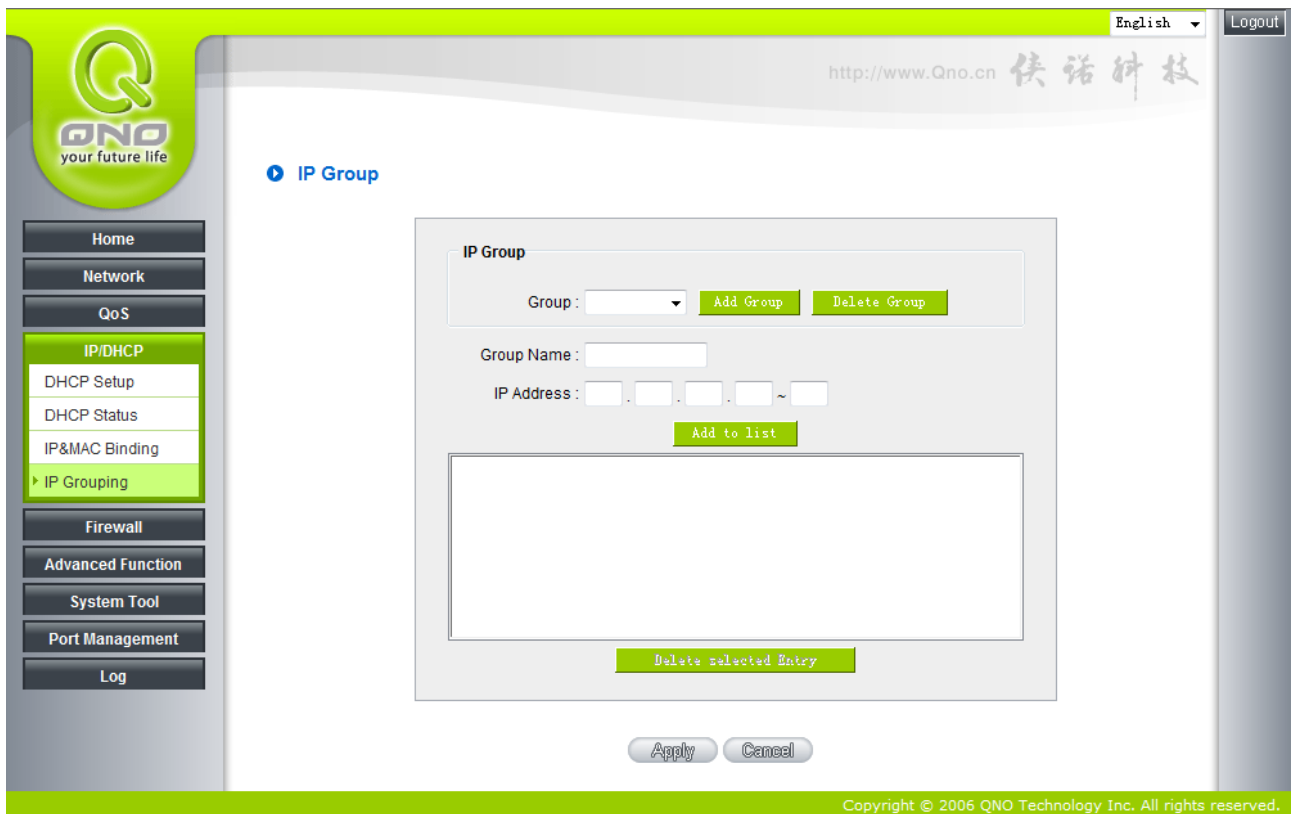
IP & MAC binding List			
		Apply	Select All
		Refresh	Close
IP	MAC	Name	Enable
192.168.1.110	00:1f:c6:7b:8a:bd	<input type="text"/>	<input checked="" type="checkbox"/>

Name :	Input the name or address of the client that is to be bound. The maximum acceptable characters are 12.
--------	--

Enabled :	Choose the item to be bound.
Apply :	Activate the configuration.
Select All :	Choose all items on the list for binding.
Refresh :	Refresh the list.
Close :	Close the list.

7.6 IP Grouping

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



IP Group :	Select a group to which the modification is to be made.
Add Group :	Click Add Group to create a new IP group.
Delete Group :	Delete the chosen IP group.
Group Name :	Input or change the name for the group.
IP Address :	Input the assigned IP range.
Add to list :	Add the configuration or modification to the list.
Delete selected item :	Remove the selected binding from the list.
Apply :	Click " Apply " to save the network configuration modification
Cancel :	Click " Cancel " to leave without making any changes.

VIII. QoS (Quality of Service)

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

8.1 Bandwidth Management (QoS)

English ▾

Logout

<http://www.Qno.cn> 快诺科技

▶ **The Maximum Bandwidth provided by ISP**

Interface	Upstream (Kbit/Sec)	Downstream (Kbit/Sec)
WAN1	512	512
WAN2	10000	10000
WAN3	10000	10000
WAN4	10000	10000

▶ **Quality of Service**

Type : Rate Control

Interface : WAN1 WAN2 WAN3 WAN4

Service : SMTP [TCP/25~25] Service Management

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

Group : ▾

Direction : Upstream ▾

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

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

Enable :

Move Up
Add to list
Move Down

Show Table Delete selected application

Home

Network

QoS

▶ Bandwidth Management

Session Control

IP/DHCP

Firewall

Advanced Function

System Tool

Port Management

Log

8.1.1 Bandwidth Management

▶ The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/Sec)	Downstream (Kbit/Sec)
WAN1	512	512
WAN2	10000	10000
WAN3	10000	10000
WAN4	10000	10000

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

Attention !

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

8.1.2 QoS

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

Rate Control :

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

▶ Quality of Service

Type : Rate Control

Interface : WAN1 WAN2 WAN3 WAN4

Service : SMTP [TCP/25~25] ▼
Service Management

IP : . . . to
 . . .

Group

Direction : Upstream ▼

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

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

Enable :

Move Up
 Add to list
 Move Down

Show Table
 Delete selected application

Interface :	Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.
Service Port :	Select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select "All (TCP&UDP) 1~65535". If only FTP uploads or downloads need to be controlled, select "FTP Port 21~21". Refer to the Default Service Port Number List.
IP Address :	This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the

	<p>range, such as “192.168.1.100 ~ 150”. The rule will control IP addresses from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input “0” in the boxes of IP address. This means all Intranet IP addresses will be restricted. QoS can also control the range of Class B.</p>
Direction :	<p>Upstream: Means the upload bandwidth for Intranet IP.</p> <p>Downstream: Means the download bandwidth for Intranet IP.</p> <p>Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server.</p> <p>Server in LAN, Downstream: If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.</p>
Min. & Max. Rate : (Kbit/Sec)	<p>The minimum bandwidth: The rule is to guarantee minimum available bandwidth.</p> <p>The maximum bandwidth: This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule.</p> <p>Attention! The unit of calculation used in this rule is Kbit. Some software indicates download/upload speed by the unit KB. 1KB = 8Kbit.</p>
Bandwidth Assign Type :	<p>Sharing total bandwidth with all IP addresses: If this option is selected, all IP addresses or Service Ports will share the bandwidth range (from minimum to maximum bandwidth).</p> <p>Assign bandwidth for each IP address: If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum.). For example, If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.</p> <p>Attention: If “Share-Bandwidth” is selected, be aware of the actual usage conditions and avoid an improper configuration that might cause a malfunction of the network when the bandwidth is too small. For example, if users do not</p>

	want an FTP to occupy too much bandwidth, users can select the “Share-Bandwidth Mode”, so that no matter how much users use FTPs to download information, the total occupied bandwidth is fixed.
Enable :	Activate the rule.
Add to list :	Add this rule to the list.
Move up & Move down :	QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. Usually the service ports which need to be restricted, such as BT, e-mule, etc., will be moved to the bottom of the list. The rules for certain IP addresses would then be moved upward.
Delete selected items :	Remove the rules selected from the Service List.
Show Table :	Display all the Rate Control Rules users made for the bandwidth. Click “ Edit ” to modify.
Apply :	Click “ Apply ” to save the configuration
Cancel :	Click “ Cancel ” to leave without making any change.

Show Table :

Click “ Show Table” botton, you can get a window as below. You can select “Rule” to display rules, or select Interface to display rules. Clieck update can re-flash window. Click “Close” can close this window. You can also click “Edit” to modify parameters.

<input checked="" type="radio"/> Rule <input type="radio"/> Interface Refresh Close								
Service Port	IP Address	Direction	Mini. Rate (Kbit/sec)	Max. Rate (Kbit/sec)	Bandwidth Assign Type	Enabled	Interface	Edit

8.1.3 Dynamic Intelligent QoS

With Dynamic Intelligent QoS, you can reach the traffic management without setup IP

addresses in the traffic management rule. This function detect LAN users automatically, fewer LAN users can use higher bandwidth, and too many LAN users can use user lower bandwidth, so that all LAN users can use bandwidth at average. This function is full flexible and simplify the management effort.

Enable Intelligent QoS
Smart QoS start condition 60 %

Upstream bandwidth threshold : 500 kbps
 Downstream bandwidth threshold : 1000 kbps
 Each IP's maximum bandwidth :

Upstream	WAN1: 200 kpbs , WAN2: 200 kpbs
	WAN3: 200 kpbs , WAN4: 200 kpbs
Downstream	WAN1: 400 kpbs , WAN2: 400 kpbs
	WAN3: 400 kpbs , WAN4: 400 kpbs

Penalty mechanism

Enable Intelligent QoS:

Click Enable Intelligent QoS

Smart QoS start condition___%

When the bandwidth usage is over the condition, the dynamic intelligent QoS will auto start. The default condition is 60%.

Upstream bandwidth threshold :

Setup the **Upstream bandwidth threshold**

Downstream bandwidth threshold :

Setup the **Downstream bandwidth threshold**

Each IP's maximum bandwidth :

When a IP address usage over above upstream or downstream thresholds, the penalty is triggered. Please setup penalty upstream / downstream bandwidth.

Penalty mechanism :

Select the second penalty, if one user triggered the internal condition, this user will has a second penalty.

Show IP Table :

Display penalty IP addresses · upstream limit · downstream limit and second penalty information.

8.1.4 Bandwidth Management Scheduling

You can use Time Schemer function to deploy difference traffic management scripts in difference time, so that we can use maximum bandwidth efficiency.

Enable bandwidth management scheduling

Date	Schedule(Military Time Scale)	Beside Schedule
Sun.	1 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	Bandwidth management <input type="text" value="Disable"/>
	2 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	
	3 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	
Mon.	1 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	Bandwidth management <input type="text" value="Disable"/>
	2 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	
	3 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	
	1 <input type="checkbox"/> Enable : From <input type="text" value="00"/> : <input type="text" value="00"/> to <input type="text" value="00"/> : <input type="text" value="00"/> <input type="text" value="Disable"/>	

Enable Bandwidth Management

Scheduling:

Date :

Enable Bandwidth Management Scheduling

From Sunday to Saturday

Schedule :

We have three time ranges can setup in one day, and the clock formula is 24H. If you select "All day" in the first time range, then others time range will blank and unable to setup. The time ranges can't overlap. We have "shutdown"、QoS and Intelligent QoS methods can be used.

Besides schedule:

Other unspecified time, we still can deploy "shutdown"、"QoS" or "Intelligent QoS" methods for traffic management.

Apply :

Click "Apply" button to saving configuration.

Cancel :

Click "Cancel" button to reject modification.

Leave :

Click "Leave" button to leaving this configuration page without saving.

8.1.5 Exempted IP address

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

▶ Exempted IP Address

WAN1 WAN2 WAN3 WAN4

Source IP . . . to / Group

. . .

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

Enable

Add to list

Delete selected range

Apply Cancel

- WAN :** Select WAN ports.
- Source IP :** Enter the exempted IP range, or select the exempted IP group.
- Do not control Direction :** Select do not control upload \ download, or both of them.
- Enable :** Enable this policy.
- Add to List :** Add this policy into the exempted list.

- Delete Selected** Delete selected list.
- Range :**
- Apply :** Click “Apply” button to saving configuration.
- Cancel :** Click “Cancel” button to reject modification.

8.2 Session control

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

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

Session Control and Scheduling :

▶ Session Control

<input checked="" type="radio"/> Disable	
<input type="radio"/> Single IP cannot exceed <input type="text" value="200"/> Session	
<input type="radio"/> When single IP exceed <input type="text" value="200"/> Session,	<input type="radio"/> block this IP to add new session for <input type="text" value="5"/> minutes
	<input type="radio"/> block this IP's all connection for <input type="text" value="5"/> minutes

▶ Scheduling

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

Disabled :	Disable Session Control function.
Single IP cannot exceed ___ session :	This option enables the restriction of maximum external sessions to each Intranet PC. When the number of external sessions reaches the limit, to allow new sessions to be built, some of the existing sessions must be closed. For example, when BT or P2P is being used to download information and the sessions exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.
When single IP exceed ___ :	<input checked="" type="radio"/> block this IP to add new session for <input type="text" value="5"/> Minutes

	<p>If this function is selected, when the user's port session reach the limit, this user will not be able to make a new session for five minutes. Even if the previous session has been closed, new sessions cannot be made until the setting time ends.</p> <p><input type="radio"/> block this IP's all connection for <input type="text" value="5"/> Minutes</p> <p>If this function is selected, when the user's port connections reach the limit, all the lines that this user is connected with will be removed, and the user will not be able to connect with the Internet for five minutes. New connections cannot be made until the delay time ends.</p>
Scheduling :	<p>If "Always" is selected, the rule will be executed around the clock.</p> <p>If "From..." is selected, the rule will be executed according to the configured time range. For example, if the time control is from Monday to Friday, 8:00am to 6:00pm, users can refer to the following figure to set up the rule.</p>
Apply :	Click "Apply" to save the configuration.
Cancel :	Click "Cancel" to leave without making any change.

Exempted Service Port or IP Address

Some IP addresses or specified services should be free in a environment, for example: SMTP service, you can use this function to avoid the session control.

Exempted Service Port or IP Address

Service : SMTP [TCP/25~25] ▼

Service Management

Source IP . . . 0 to / Group ▼

 . . . 0

Enable :

Add to list

Deleted selected application

Apply
Cancel

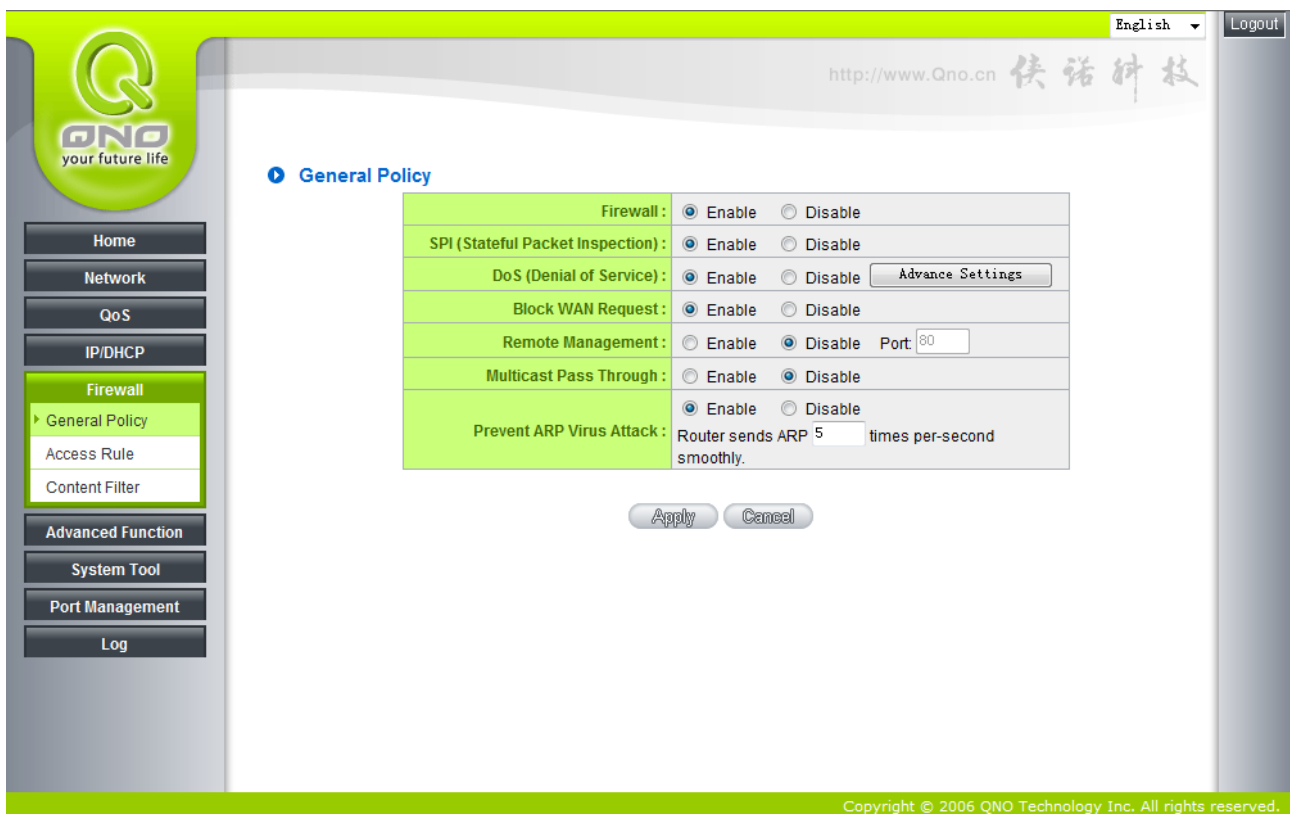
Service Port :	Choose the service port.
IP Address :	Input the IP address range or IP group.
Enabled :	Activate the rule.
Add to list :	Add this rule to the list.
Delete seleted item :	Remove the rules selected from the Service List.
Apply :	Click “ Apply ” to save the configuration.
Cancel :	Click “ Cancel ” to leave without making any change.

IX. Firewall

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

9.1 General Policy

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



English Logout

http://www.Qno.cn 快诺科技

General Policy

Firewall :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SPI (Stateful Packet Inspection) :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DoS (Denial of Service) :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Advance Settings"/>
Block WAN Request :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Remote Management :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable Port: <input type="text" value="80"/>
Multicast Pass Through :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Prevent ARP Virus Attack :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable Router sends ARP <input type="text" value="5"/> times per-second smoothly.

Copyright © 2006 QNO Technology Inc. All rights reserved.

Firewall :	This feature allows users to turn on/off the firewall.
SPI (Stateful Packet Inspection) :	This enables the packet automatic authentication detection technology. The Firewall operates mainly at the network layer. By executing the dynamic authentication for each connection, it will also perform an alarming function for application procedure. Meanwhile, the packet authentication firewall may decline the connections which use non-standard communication protocol.
DoS (Denial of	This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of

Service) :	Death, IP Spoofing and so on.																		
Block WAN request :	If set as Enabled, then it will shut down outbound ICMP and abnormal packet responses in connection. If users try to ping the WAN IP from the external, this will not work because the default value is set as activated in order to decline the outbound responses.																		
Remote Management :	To enter the device web- based UI by connecting to the remote Internet, this feature must be activated. In the field of remote browser IP, a valid external IP address (WAN IP) for the device should be filled in and the modifiable default control port should be adjusted (the default is set to 80, modifiable).																		
Multicast Pass Through :	There are many audio and visual streaming media on the network. Broadcasting may allow the client end to receive this type of packet message format. This feature is off by default.																		
Prevent ARP Virus Attack :	This feature is designed to prevent the intranet from being attacked by ARP spoofing, causing the connection failure of the PC. This ARP virus cheat mostly occurs in Internet cafes. When attacked, all the online computers disconnect immediately or some computers fail to go online. Activating this feature may prevent the attack by this type of virus.																		
Advanced Setting	<p>Advance DoS Settings</p> <table border="1"> <thead> <tr> <th>Packet Type</th> <th>WAN Threshold</th> <th>LAN Threshold</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> TCP_SYN_Flood</td> <td>Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes</td> <td>Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes</td> </tr> <tr> <td><input checked="" type="checkbox"/> UDP_Flood</td> <td>Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes</td> <td>Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes</td> </tr> <tr> <td><input checked="" type="checkbox"/> ICMP_Flood</td> <td>Threshold counted by all packets 200 Packets/Sec Threshold counted by single IP packet 50 Packets/Sec Block this IP when reach threshold 5 Minutes</td> <td>Threshold counted by all packets 200 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 50 Packets/Sec Block this IP when reach threshold 5 Minutes</td> </tr> <tr> <td><input type="checkbox"/> Exception Source IP</td> <td></td> <td>IP : 0 . 0 . 0 . 0 to /Group</td> </tr> <tr> <td><input type="checkbox"/> Exception Destination IP</td> <td></td> <td>0 . 0 . 0 . 0</td> </tr> </tbody> </table> <p>Stop Blocked IP Apply Cancel</p> <p>Packet Type: This device provides three types of data packet transmission:</p>	Packet Type	WAN Threshold	LAN Threshold	<input checked="" type="checkbox"/> TCP_SYN_Flood	Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	<input checked="" type="checkbox"/> UDP_Flood	Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	<input checked="" type="checkbox"/> ICMP_Flood	Threshold counted by all packets 200 Packets/Sec Threshold counted by single IP packet 50 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 200 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 50 Packets/Sec Block this IP when reach threshold 5 Minutes	<input type="checkbox"/> Exception Source IP		IP : 0 . 0 . 0 . 0 to /Group	<input type="checkbox"/> Exception Destination IP		0 . 0 . 0 . 0
Packet Type	WAN Threshold	LAN Threshold																	
<input checked="" type="checkbox"/> TCP_SYN_Flood	Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes																	
<input checked="" type="checkbox"/> UDP_Flood	Threshold counted by all packets 15000 Packets/Sec Threshold counted by single IP packet 2000 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 15000 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 2000 Packets/Sec Block this IP when reach threshold 5 Minutes																	
<input checked="" type="checkbox"/> ICMP_Flood	Threshold counted by all packets 200 Packets/Sec Threshold counted by single IP packet 50 Packets/Sec Block this IP when reach threshold 5 Minutes	Threshold counted by all packets 200 Packets/Sec Single Destination IP Threshold 2000 Packets/Sec Single Source IP Threshold 50 Packets/Sec Block this IP when reach threshold 5 Minutes																	
<input type="checkbox"/> Exception Source IP		IP : 0 . 0 . 0 . 0 to /Group																	
<input type="checkbox"/> Exception Destination IP		0 . 0 . 0 . 0																	

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

9.2 Access Rule

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

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

9.2.1 Default Access Rule

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

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

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

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

▶ Access Rule

Jump to 1 / page 5 entries per page

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	220.130.188.45 ~ 220.130.188.45	Any	Always		Edit	
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always			

Add New Rule

Restore to Default Rules

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

Edit : Define the network access rule item

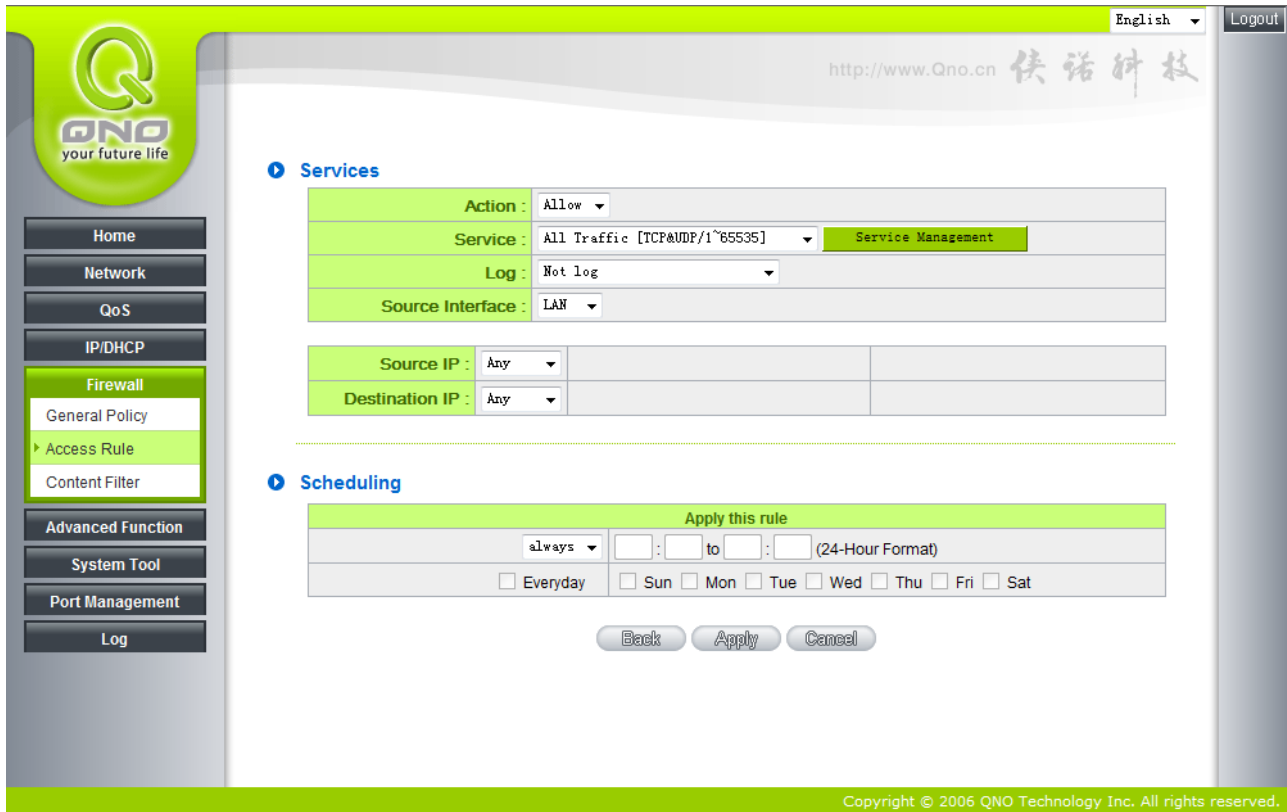
Delete : Remove the item.

Add New Rule : Create a new network access rule

Return to Default Rule : Restore all settings to the default values and delete all the self-defined

settings.

9.2.2 Add New Access Rule



English | Logout

http://www.Qno.cn 快诺科技

Services

Action : Allow

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

Log : Not log

Source Interface : LAN

Source IP : Any

Destination IP : Any

Scheduling

Apply this rule

always : : to : : (24-Hour Format)

Everyday Sun Mon Tue Wed Thu Fri Sat

Back Apply Cancel

Copyright © 2006 QNO Technology Inc. All rights reserved.

Action :	Allow: Permits the pass of packets compliant with this control rule Deny: Prevents the pass of packets not compliant with this control rule
Service Port :	From the drop-down menu, select the service that users grant or do not give permission.
Service Port Management :	If the service that users wish to manage does not exist in the drop-down menu, press – Service Management to add the new service. From the pop-up window, enter a service name and communications protocol and port, and then click the “Add to list” button to add the new service.
Log :	No Log : There will be no log record. Create Log when matched : Event will be recorded in the log.
Interface :	Select the source port whether users are permitted or not (for example: LAN, WAN1, WAN2 or Any). Select from the drop-down menu.
Source IP :	Select the source IP range (for example: Any, Single, Range, or preset IP group name). If Single or Range is selected, please enter a single IP address or an IP address within a session.

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

Example1: How to block TCP 135-139 ports

First, add a new TCP 135-139 service port object(please refer the service port chapter), and the finish below configurations.

Action: Deny

Service: TCP135-139

Source Interface: Any

Source IP address: Any

Destination IP address: Any

Services

Action :	Deny	
Service :	IMAP [TCP/143~143]	Service Management
Log :	Not log	
Source Interface :	Any	
Source IP :	Any	
Destination IP :	Any	

Example2: How to block LAN IP addresses from 192.168.1.200-192.168.1.230 to access the TCP 80 port ?

Action: Deny

Service: TCP 80

Source Interface: Range

Source IP address: range from 192.168.1.200 to 192.168.1.230

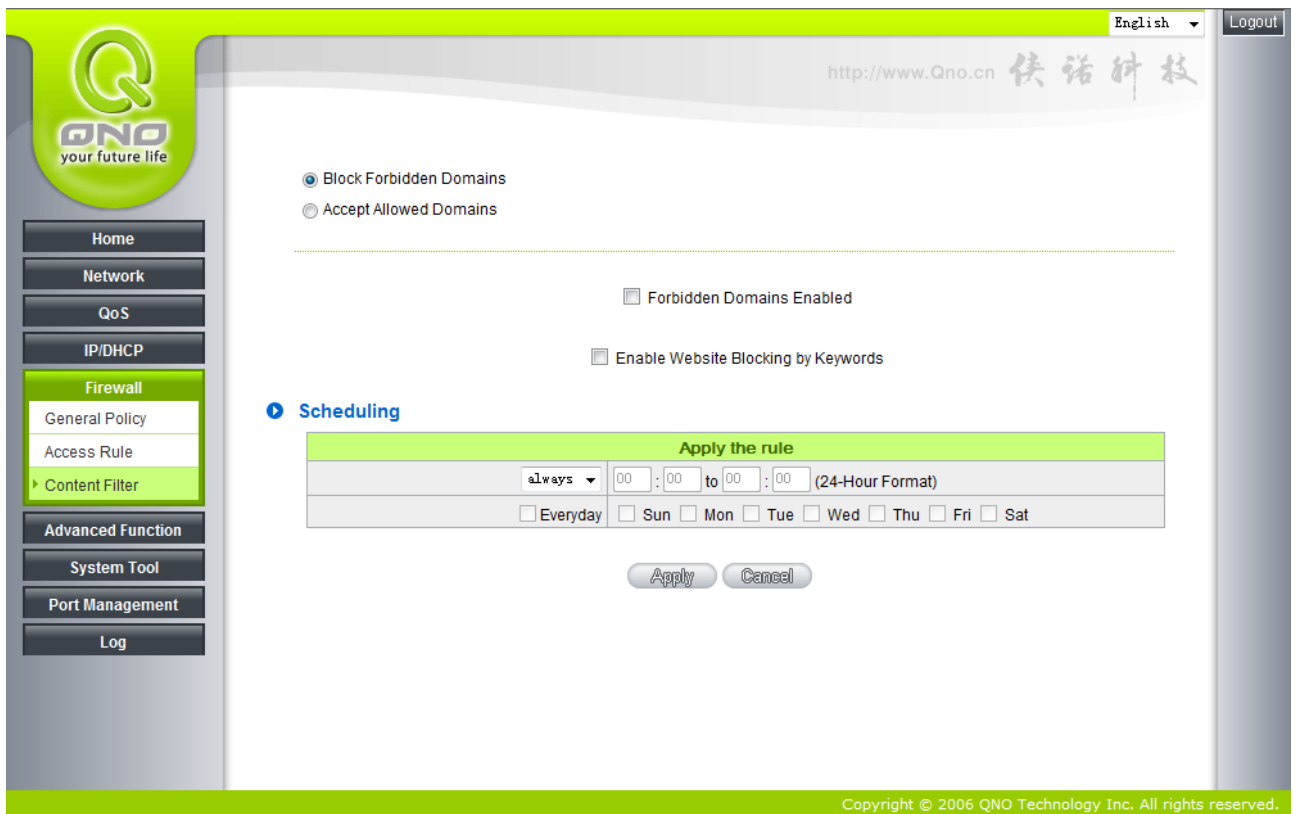
Destination address: Any

Services

Action :	Deny <input type="button" value="v"/>
Service :	HTTP [TCP/80~80] <input type="button" value="v"/> Service Management
Log :	Not log <input type="button" value="v"/>
Source Interface :	Any <input type="button" value="v"/>
Source IP :	<input type="button" value="Range"/> <input type="button" value="v"/> <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="200"/> to <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="230"/>
Destination IP :	Any <input type="button" value="v"/>

9.3 Content Filter

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



Block Forbidden Domain

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

- Block Forbidden Domains
- Accept Allowed Domains

Forbidden Domains

Forbidden Domains Enabled

Forbidden Domains

Add:

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

Group ▼

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

Website Blocking by Keywords :

Website Blocking by Keywords

Enable Website Blocking by Keywords

Keywords

Add:

Exception IP address ▼ : . . . to

Group ▼ IP Grouping

Add to list

Delete selected keywords

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

Accept Allowed Domains

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

Select "Accept Allowed Domains" check box, you will see below setup windows:

- Block Forbidden Domains
- Accept Allowed Domains

Allowed Domains

Allowed Domains Enabled

Allowed Domains

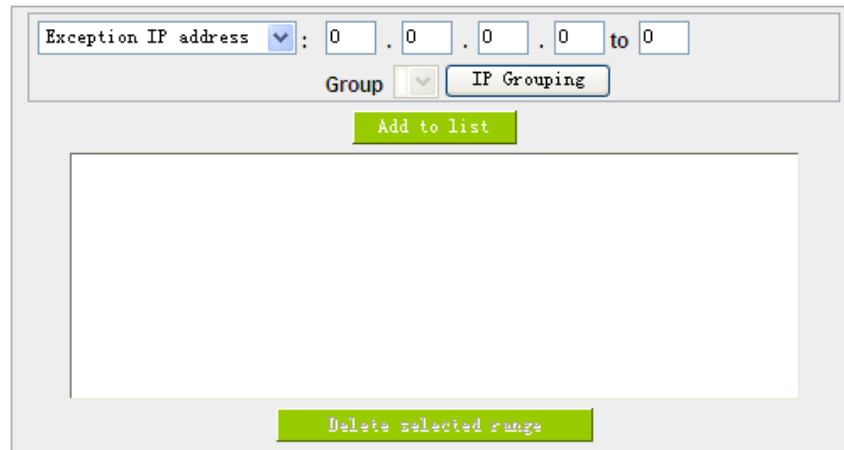
Add:

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

Exception IP address

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

▶ Exception

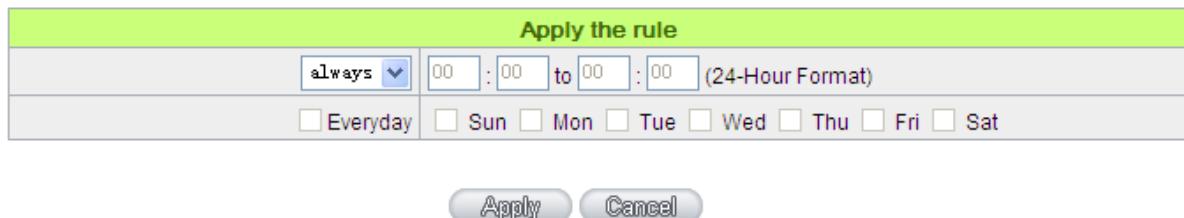


- Exception IP address/Group** Enter the exempted IP addresses or IP group.
- Add to list** Click this button to add exempted IP addresses or IP group.
- Delete selected range** Click this button to delect selected exempted IP address or IP group.

Content Filter Scheduling

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

▶ Scheduling



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

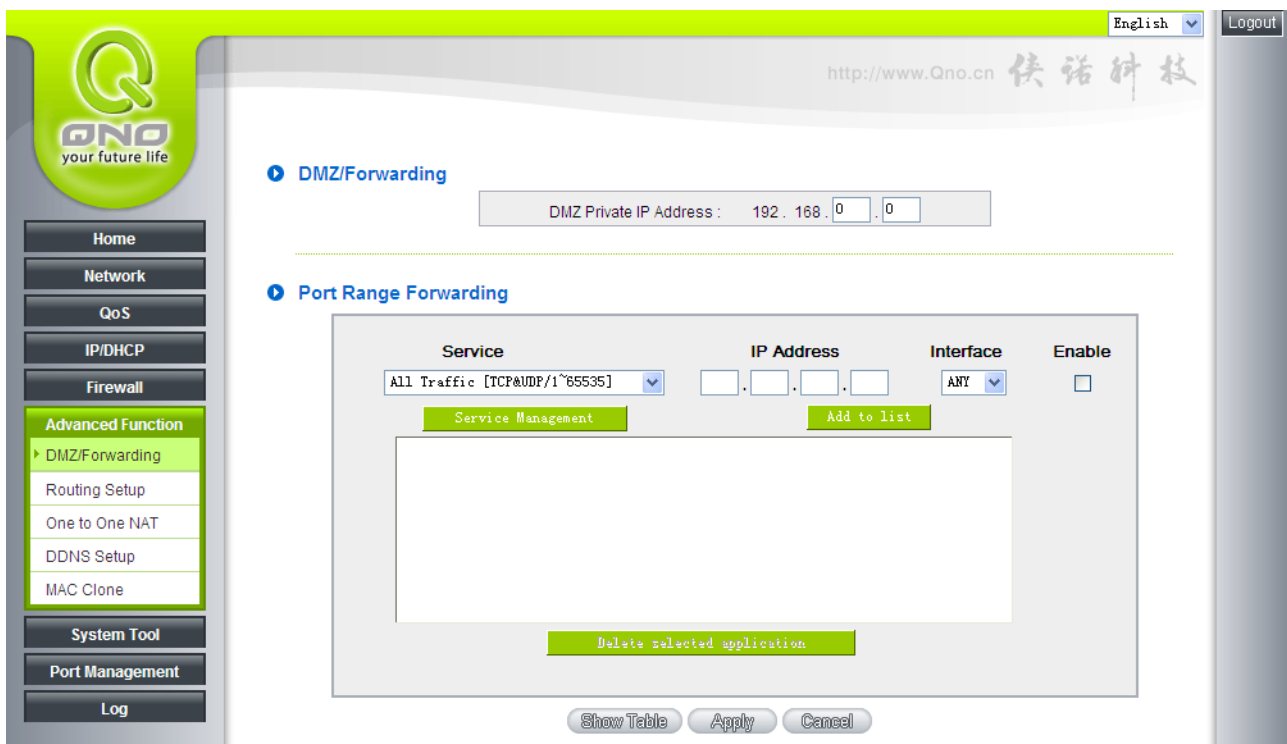
Day Control : This control rule has time limitation. The setting method is in 24-hour format, such as 08:00 ~ 18:00 (8 a.m. to 6 p.m.)

X. Advanced Function

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

1. Setup DMZ servers forwarding to WAN, for example, the Web or FTP servers.
2. Setup static routing entries or dynamic routing protocol.
3. Setup one to one NAT function to mapping public IP address and private IP address.
4. Setup dynamic DNS service.
5. Setup MAC address in interfaces.

10.1 DMZ/Forwarding



The screenshot shows the QNO router's web management interface. The top navigation bar includes 'English' and 'Logout'. The main content area is titled 'DMZ/Forwarding' and contains two sections: 'DMZ/Forwarding' and 'Port Range Forwarding'. The 'DMZ/Forwarding' section has a field for 'DMZ Private IP Address' set to '192.168.0.0'. The 'Port Range Forwarding' section features a table with columns for 'Service', 'IP Address', 'Interface', and 'Enable'. The 'Service' dropdown is set to 'All Traffic [TCP&UDP/1~65535]'. Below the table are buttons for 'Service Management', 'Add to list', and 'Delete selected application'. At the bottom of the interface are 'Show Table', 'Apply', and 'Cancel' buttons.

10.1.1 DMZ Configuration

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.

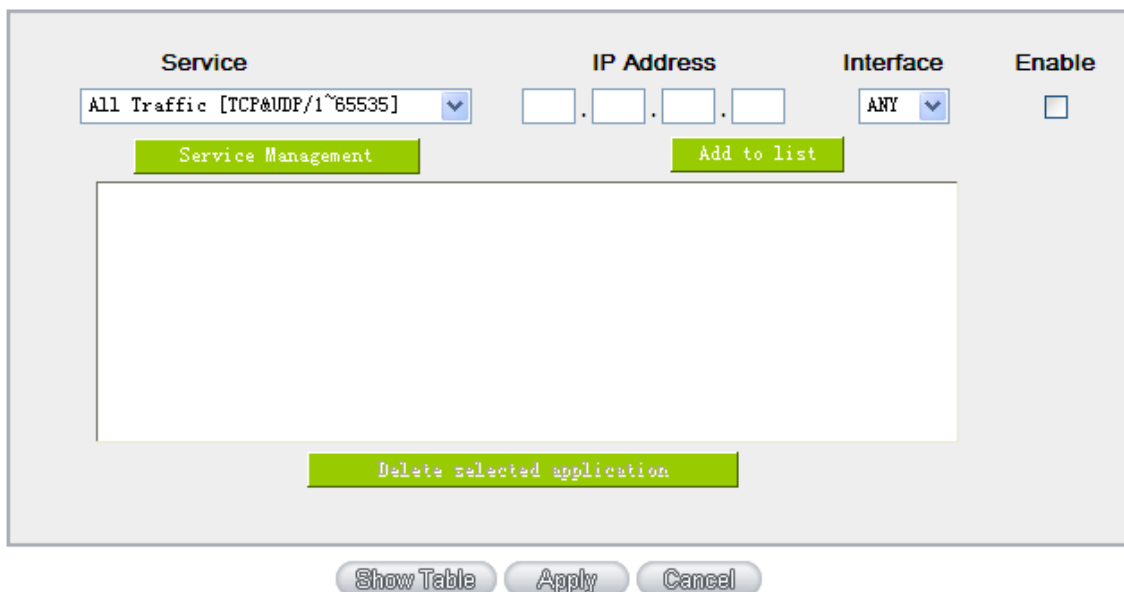
10.1.2 Port Range Forwarding

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	IP Address	Interface	Enable
All Traffic [TCP&UDP/1~65535]	. . .	ANY	<input type="checkbox"/>

Service Management Add to list

Delete selected application

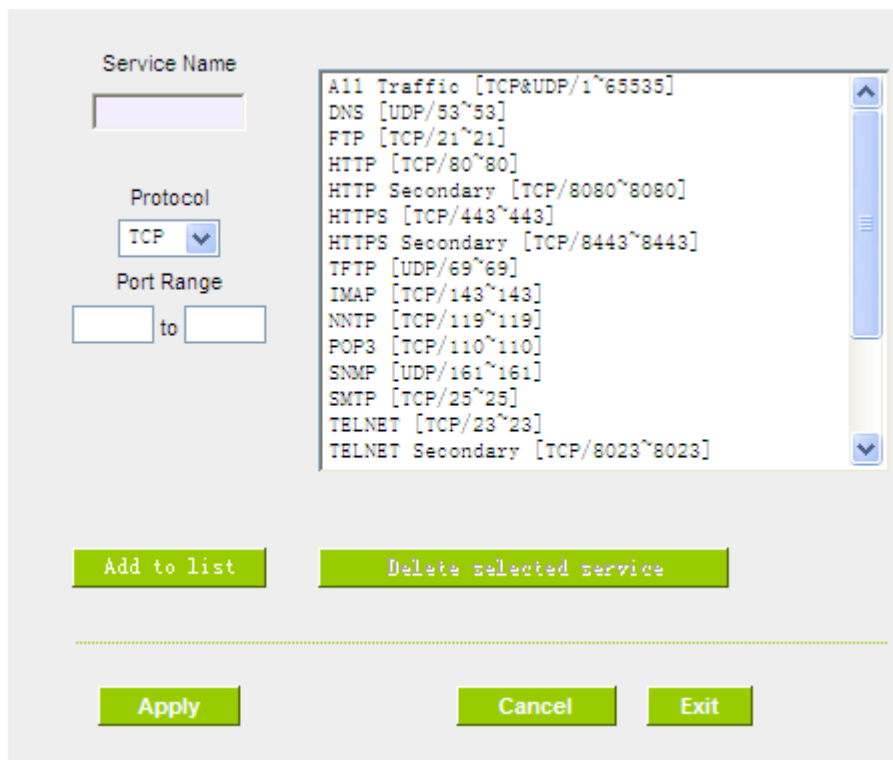
Show Table Apply Cancel

Service Port :	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.
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 :

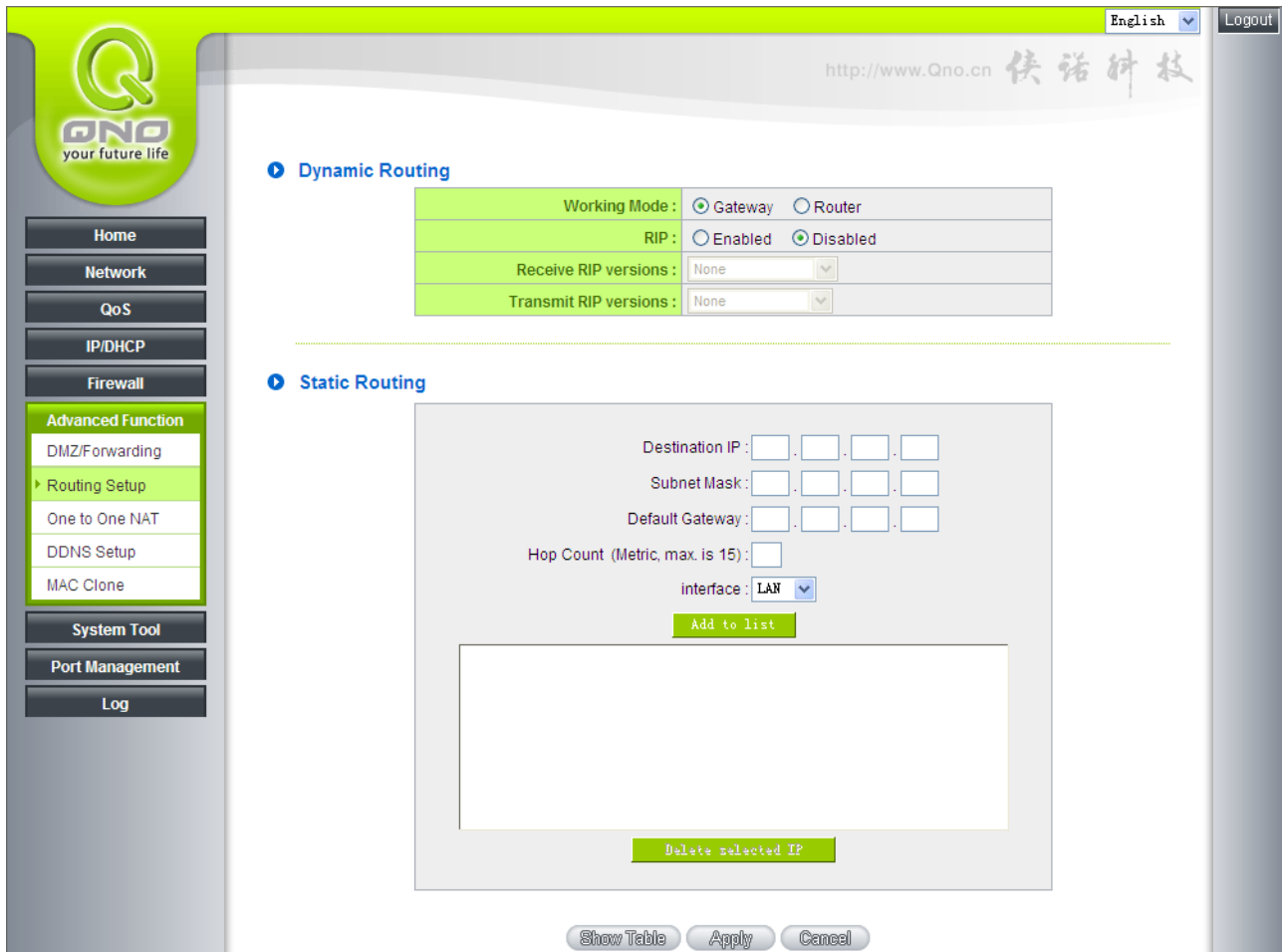


Service Name :	Input the name of the service port users want to activate on the list, such as E-donkey, etc.
Protocol :	To select whether a service port is TCP or UDP.
Port Range :	To activate this function, input the range of the service port locations

	users want to activate such as 500~500 or 2300~2310, etc.
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 Routing

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



The screenshot shows the QNO router's web management interface. The top navigation bar includes 'English' and 'Logout'. The main content area is divided into two sections: 'Dynamic Routing' and 'Static Routing'.

Dynamic Routing Configuration:

- Working Mode: Gateway Router
- RIP: Enabled Disabled
- Receive RIP versions: None (dropdown)
- Transmit RIP versions: None (dropdown)

Static Routing Configuration:

- Destination IP: [] . [] . [] . []
- Subnet Mask: [] . [] . [] . []
- Default Gateway: [] . [] . [] . []
- Hop Count (Metric, max. is 15): []
- interface: LAN (dropdown)
- Buttons: Add to list, Delete selected IP

At the bottom of the interface, there are buttons for 'Show Table', 'Apply', and 'Cancel'.

Dynamic Routing

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

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

Dynamic Routing

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

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.

10.2.2 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

Destination IP : . . .

Subnet Mask : . . .

Default Gateway : . . .

Hop Count (Metric, max. is 15) :

interface : ▼

Dest. IP :	Input the remote network IP locations and subnet that is to be routed. For example, the IP/subnet is 192.168.2.0/255.255.255.0.
Subnet Mask :	
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.

10.3 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

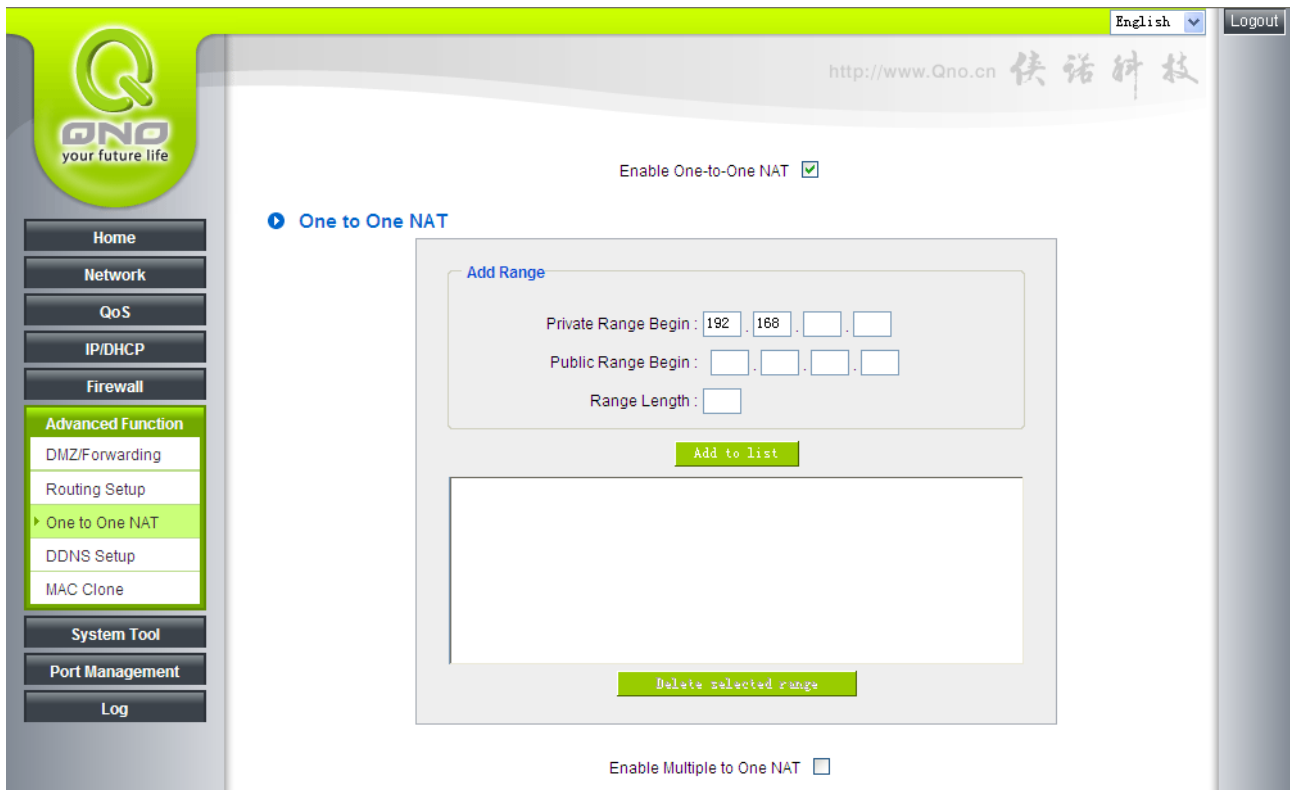
210.11.1.3 → 192.168.1.4

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.



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.

10.4 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.



English Logout

http://www.Qno.cn 快诺科技

DDNS Setup

Interface	Status	Host Name	Config.
WAN1	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns:--- 3322:--- Qno:---	Edit
WAN2	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns:--- 3322:--- Qno:---	Edit
WAN3	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns:--- 3322:--- Qno:---	Edit
WAN4	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns:--- 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 :

DynDNS.org

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

3322.org

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

QnoDDNS.org.cn

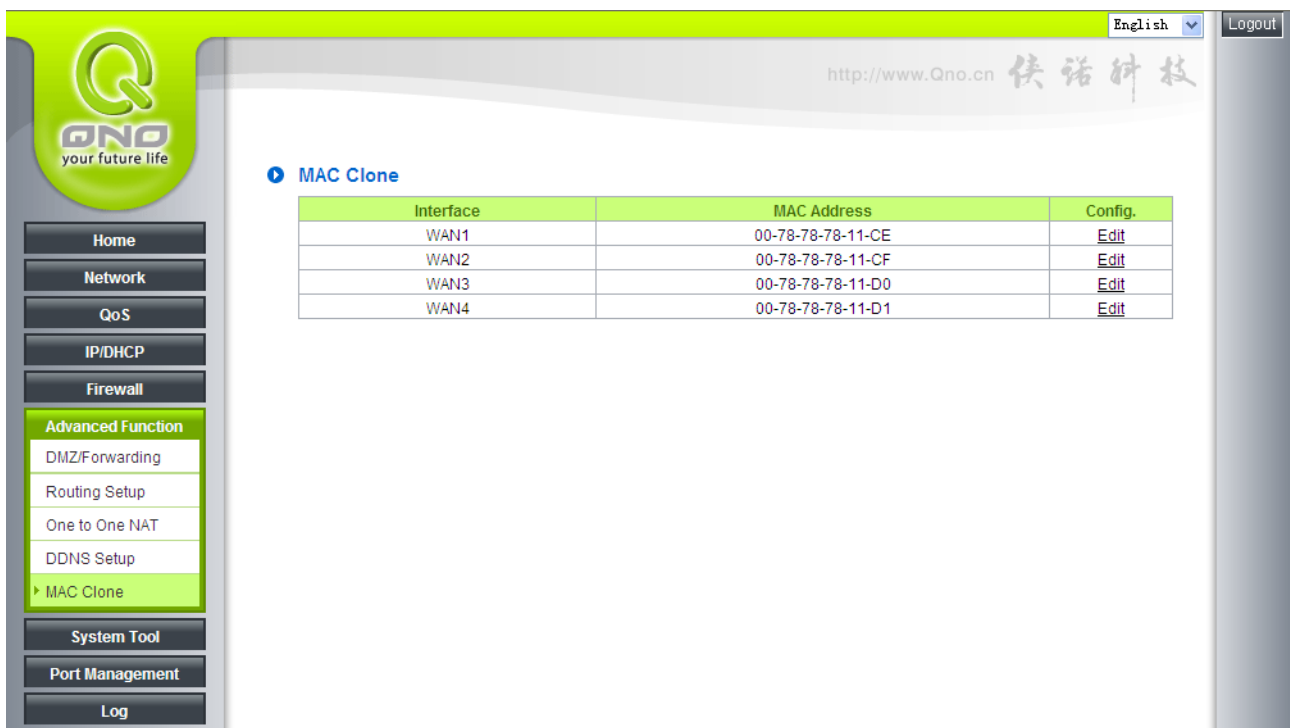
User name:	<input type="text"/> .qnoDDNS.org.cn
Password:	<input type="password"/>
Internet IP Address:	0.0.0.0
Status:	DDNS function is disabled or No Internet connection.

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.
Dynamic Domain Name	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.
WAN 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.

10.5 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.



Interface	MAC Address	Config.
WAN1	00-78-78-78-11-CE	Edit
WAN2	00-78-78-78-11-CF	Edit
WAN3	00-78-78-78-11-D0	Edit
WAN4	00-78-78-78-11-D1	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:

User Defined WAN MAC Address :	<input checked="" type="radio"/> <input type="text" value="00"/> <input type="text" value="0e"/> <input type="text" value="a0"/> <input type="text" value="50"/> <input type="text" value="00"/> <input type="text" value="01"/>
	(Default: 00-0e-a0-50-00-01)
MAC Address from this PC :	<input type="radio"/> <input type="text" value="00-1f-c6-7b-8a-bd"/>

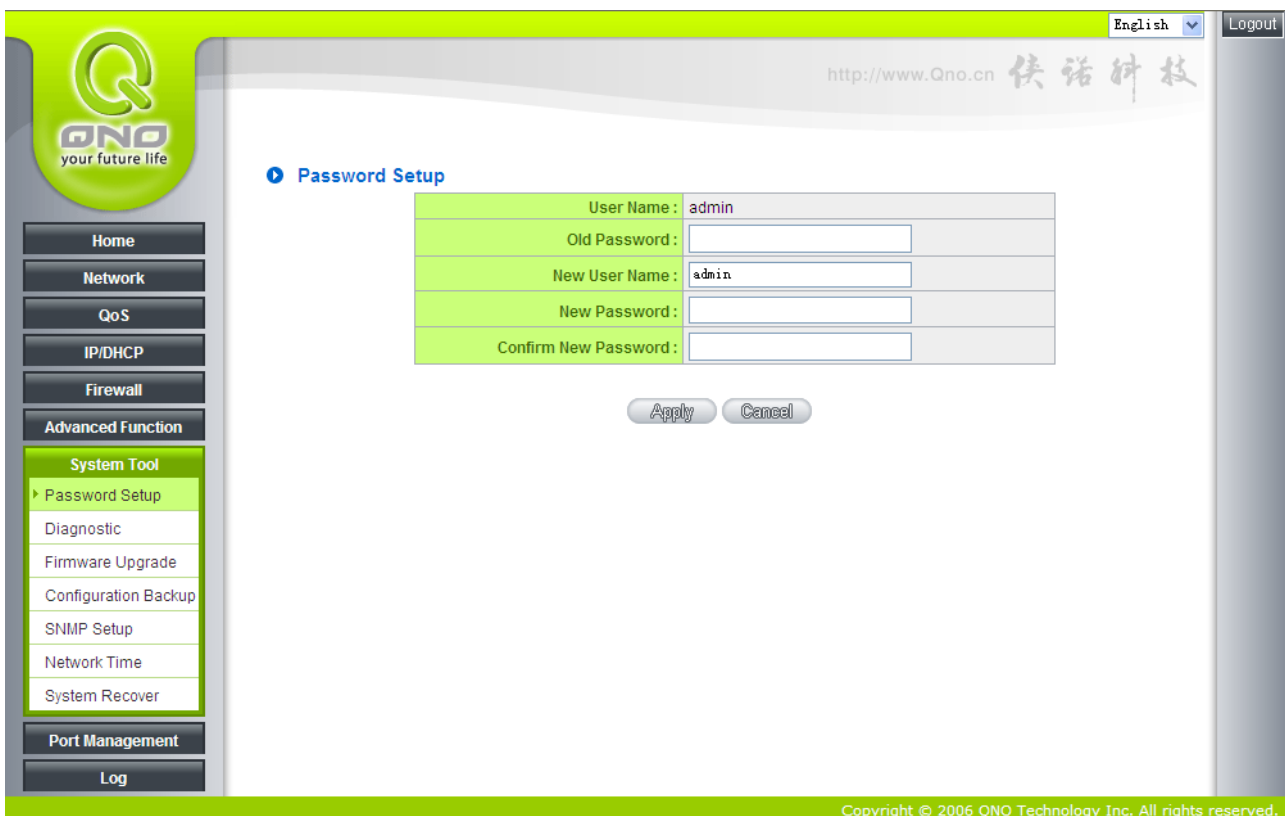
XI 、 System Tool

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

GIGABIT router 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).



The screenshot shows the QNO router's web management interface. The top navigation bar includes the QNO logo, a language dropdown set to 'English', and a 'Logout' button. The main content area is titled 'Password Setup' and contains a form with the following fields:

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

Below the form are 'Apply' and 'Cancel' buttons. The left sidebar menu is expanded to show 'System Tool' options: Password Setup (selected), Diagnostic, Firmware Upgrade, Configuration Backup, SNMP Setup, Network Time, and System Recover. Other sidebar options include Home, Network, QoS, IP/DHCP, Firewall, Advanced Function, Port Management, and Log. The footer contains the copyright notice: 'Copyright © 2006 QNO Technology Inc. All rights reserved.'

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 :
Name: www.google.com
Address: 66.249.89.104

Ping

DNS Name Lookup Ping

Ping host or IP address :
Status: **Test Succeeded**
Packets: 4/4 transmitted, 4/4 received, 0% loss
Minimum = 18 ms
Round Trip Time: Maximum = 99 ms
Average = 48 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 GIGABIT Router 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.



English ▼ Logout

http://www.Qno.cn 侠诺科技

▶ Firmware Upgrade

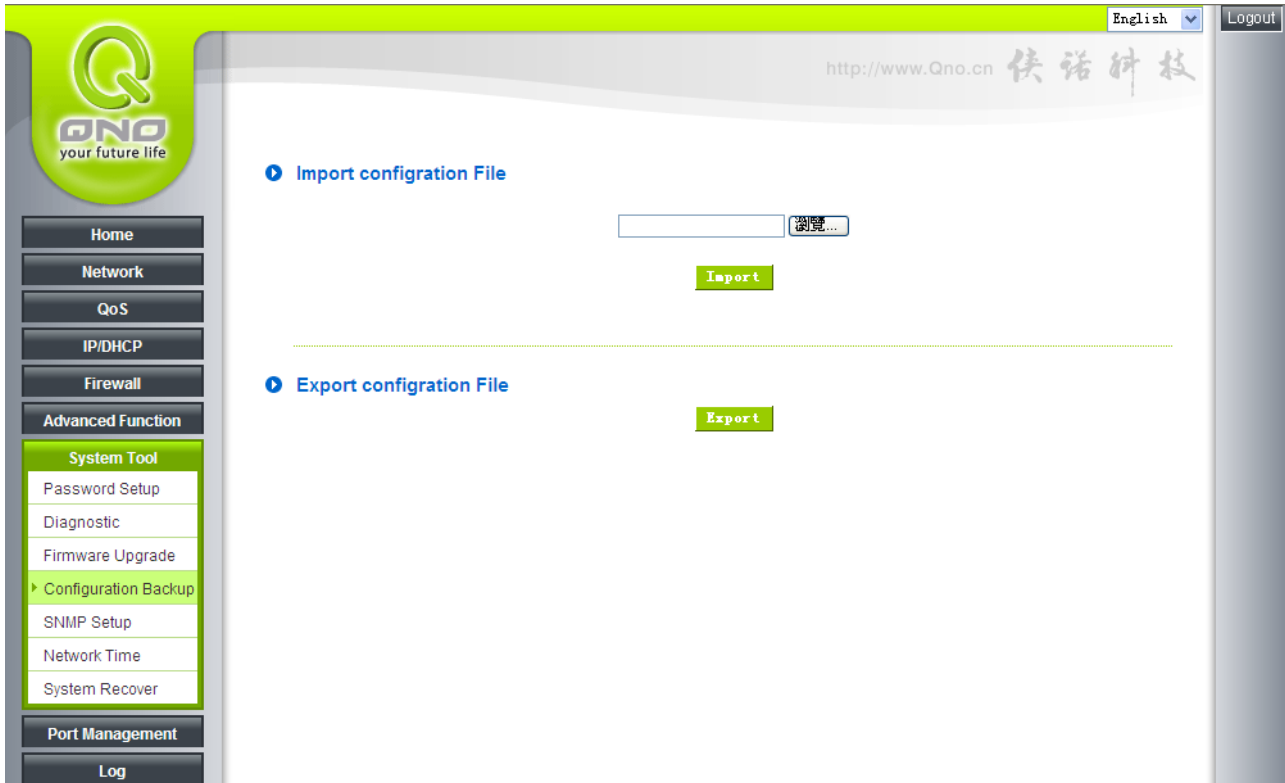
浏览...

Firmware Upgrade Right Now

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 :

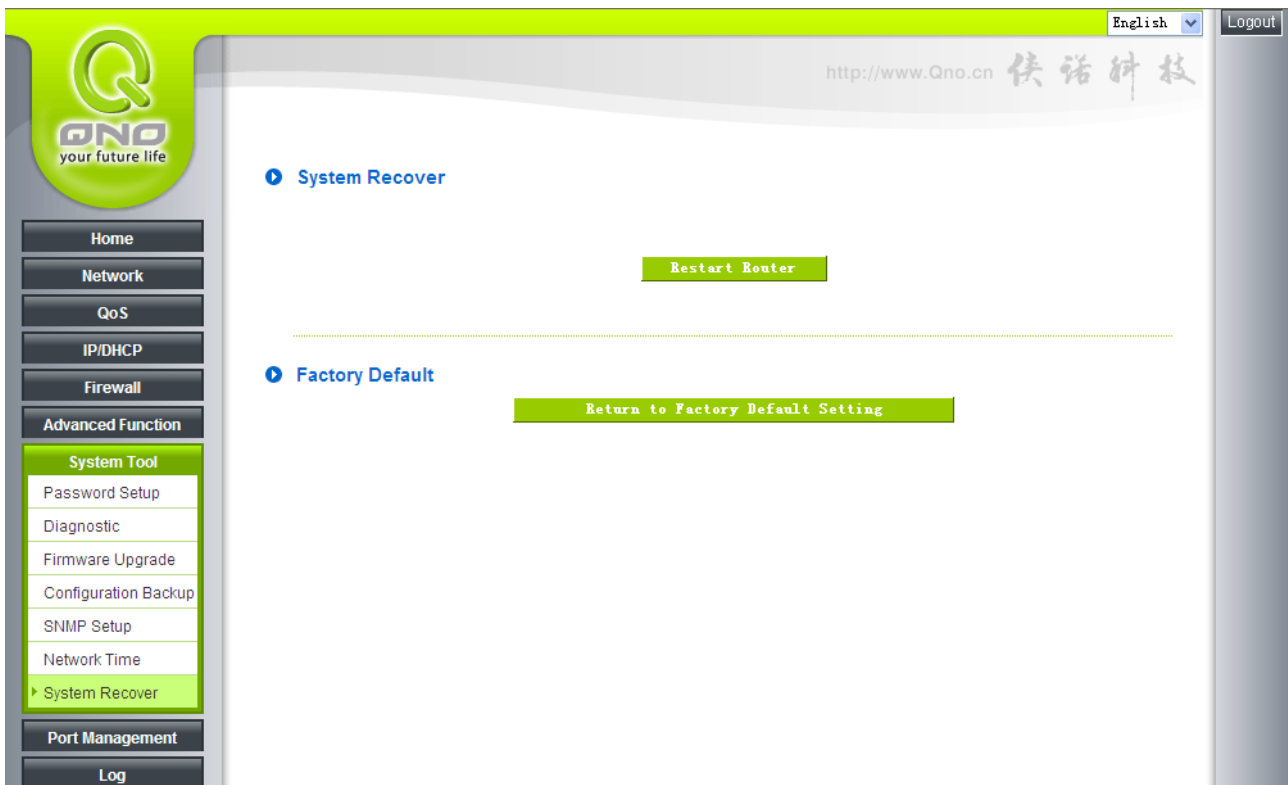
This feature allows users to integrate all backup content of parameter settings into the GIGABIT Router. Before upgrade, confirm all information about the software version. Select and browse the backup parameter file: "config.exp." Select the file and click "**Import**" to import the file.

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 System Recover

Users can restart the GIGABIT Router with System Recover button.



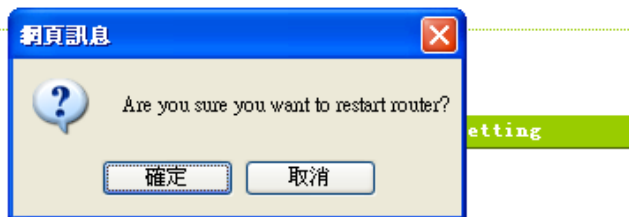
Restart

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

▶ System Recover

Restart Router

▶ Factory Default

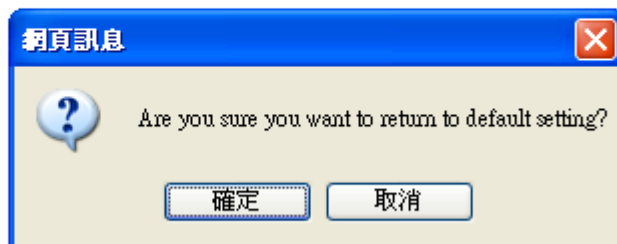


Return to Factory Default Setting

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

▶ Factory Default

Return to Factory Default Setting



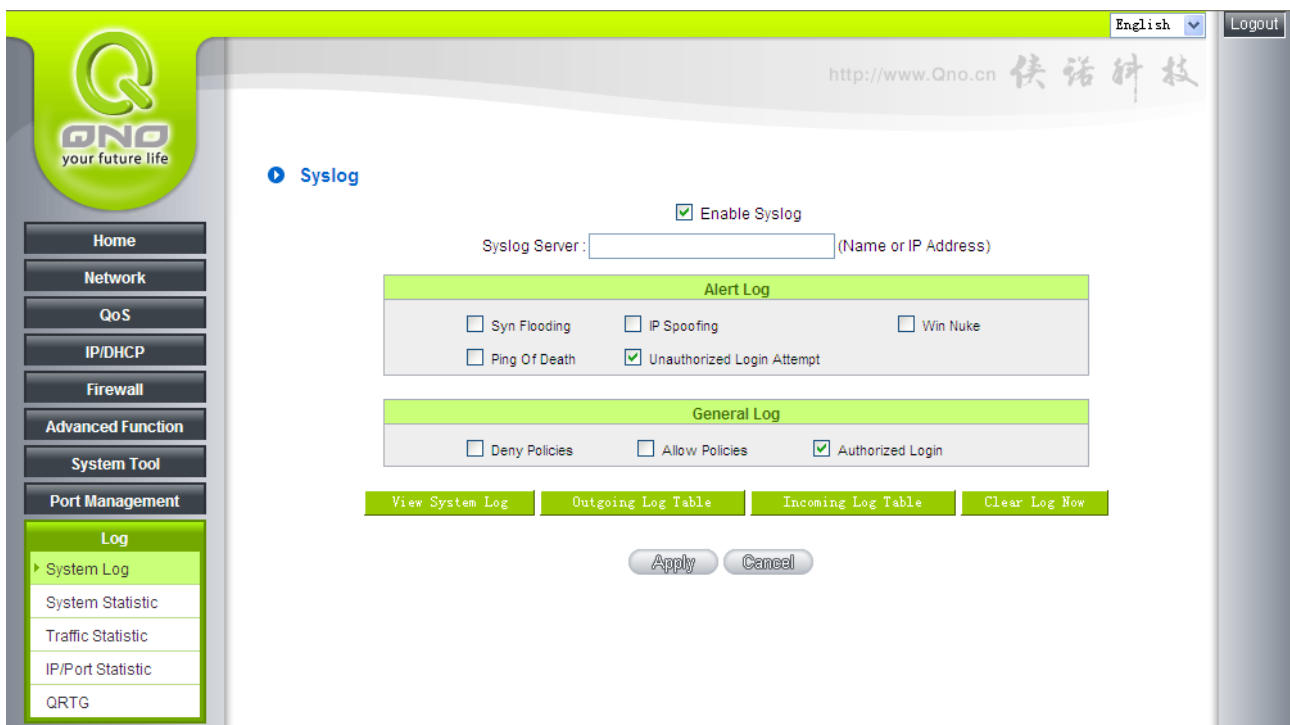
We suggest you backup your router configuration before upgrade firmware, after upgraded firmware, you can reset router configuration to default for check the router stability, and then restore original router configuration. (About backup and restore router configuration, you can refer Chapter 12.3)

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.



System Log

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.

Log Setting

Alert Log

Syn Flooding

IP Spoofing

Win Nuke

Ping Of Death

Unauthorized Login Attempt

General Log

Deny Policies

Allow Policies

Authorized Login

View System Log

Outgoing Log Table

Incoming Log Table

Clear Log Now

Apply

Cancel

The GIGABIT Router 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 GIGABIT Router 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.

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

- Allow Policies :** If remote users enter the system because of compliance with access rules; for instance, message will be recorded in the system log.
- Authorized Login :** Successful entry into the system includes login from the remote end or from the LAN into this device. These messages will be recorded in the system log.

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

View System Log :

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

System Log		
Current Time: Mon Apr 20 16:59:02 2009		<input type="button" value="All"/> <input type="button" value="Refresh"/> <input type="button" value="Close"/>
Time	Event-Type	Message
Jan 1 08:00:07 2000	System Log	SMB : System is up
Jan 1 08:00:17 2000	System Log	WAN4=59.105.115.196 WAN1_MASK=255.255.255.255 WAN4_GATEWAY=59.105.115.1 WAN4_DNS1=139.175.55.244 WAN4_DNS2=139.175.252.16 mtu=1492
Jan 1 08:00:17 2000	System Log	WAN2=59.105.115.248 WAN1_MASK=255.255.255.255 WAN2_GATEWAY=59.105.115.1 WAN2_DNS1=139.175.55.244 WAN2_DNS2=139.175.252.16 mtu=1492
Jan 1 08:00:17 2000	System Log	WAN connection is up : 59.105.115.196/255.255.255.255 gw 59.105.115.1 on ppp4
Jan 1 08:00:18 2000	System Log	dhcpConfig: open/write/close: No such file or directory
Jan 1 08:00:18 2000	System Log	dhcpConfig: fopen: No such file or directory
Apr 20 16:57:38 2009	System Log	WAN connection is up : 59.105.115.248/255.255.255.255 gw 59.105.115.1 on ppp2
Apr 20 16:57:46 2009	System Log	WAN connection is up : 192.168.4.141/255.255.254.0 gw 192.168.4.1 on eth1

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 Log Table

Time ▲	Event-Type	Message
Apr 20 17:05:25 2009	Connection Accepted	IN=eth0 OUT=ppp4 SRC=192.168.1.211 DST=121.6.29.221 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=50341 DF PROTO=TCP SPT=5110 DPT=1268 WINDOW=0 RES=0x00 ACK RST URGP=0
Apr 20 17:05:27 2009	Connection Accepted	IN=eth0 OUT=ppp4 SRC=192.168.1.211 DST=121.6.29.221 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=50343 DF PROTO=TCP SPT=5110 DPT=1268 WINDOW=0 RES=0x00 ACK RST URGP=0
Apr 20 17:05:30 2009	Connection Accepted	IN=eth0 OUT=ppp4 SRC=192.168.1.211 DST=114.138.154.217 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=50344 DF PROTO=TCP SPT=23469 DPT=4832 WINDOW=0 RES=0x00 ACK RST URGP=0

Incoming Packet Log :

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

Incoming Log Table

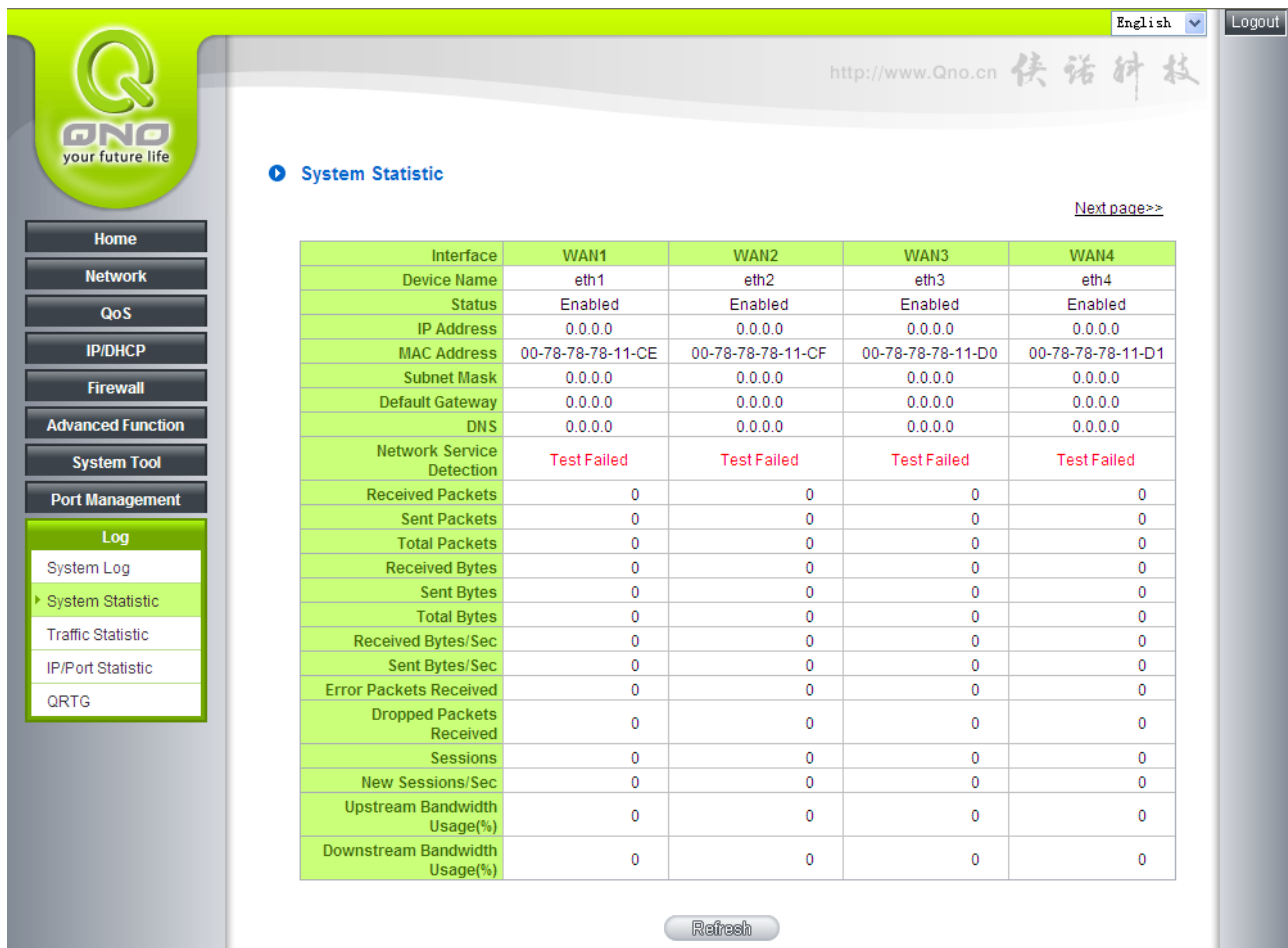
Time ▲	Event-Type	Message
Apr 20 17:05:25 2009	Connection Accepted	IN=ppp4 OUT=eth0 SRC=121.6.29.221 DST=192.168.1.211 LEN=48 TOS=0x00 PREC=0x00 TTL=107 ID=9178 DF PROTO=TCP SPT=1268 DPT=5110 WINDOW=65535 RES=0x00 SYN URGP=0
Apr 20 17:05:27 2009	Connection Accepted	IN=ppp4 OUT=eth0 SRC=121.6.29.221 DST=192.168.1.211 LEN=48 TOS=0x00 PREC=0x00 TTL=107 ID=9231 DF PROTO=TCP SPT=1268 DPT=5110 WINDOW=65535 RES=0x00 SYN URGP=0
Apr 20 17:05:30 2009	Connection Accepted	IN=ppp4 OUT=eth0 SRC=114.138.154.217 DST=192.168.1.211 LEN=52 TOS=0x00 PREC=0x00 TTL=42 ID=58763 DF PROTO=TCP SPT=4832 DPT=23469 WINDOW=59136 RES=0x00 SYN URGP=0

Clear Log Now :

This feature clears all the current information on the log.

12.2 System Statistic

The GIGABIT Router 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 (%).



English Logout

http://www.Qno.cn 快诺科技

System Statistic

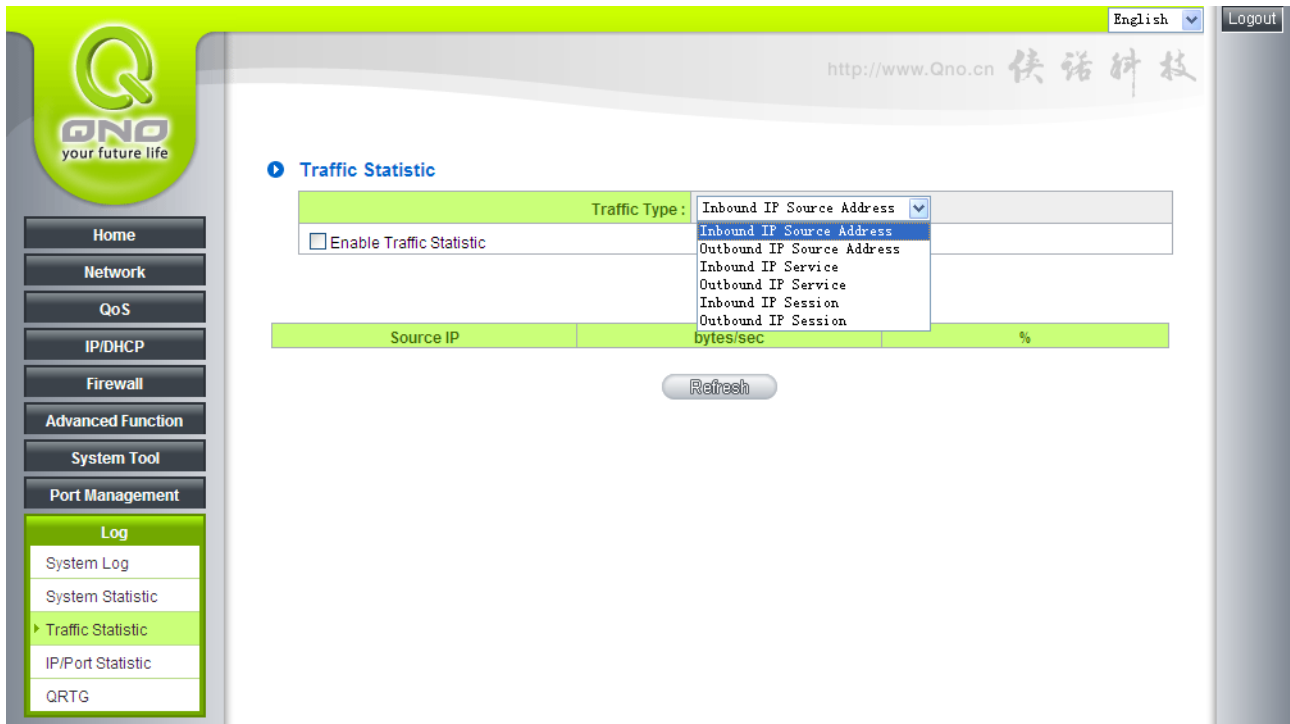
[Next page>>](#)

Interface	WAN1	WAN2	WAN3	WAN4
Device Name	eth1	eth2	eth3	eth4
Status	Enabled	Enabled	Enabled	Enabled
IP Address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
MAC Address	00-78-78-78-11-CE	00-78-78-78-11-CF	00-78-78-78-11-D0	00-78-78-78-11-D1
Subnet Mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Network Service Detection	Test Failed	Test Failed	Test Failed	Test Failed
Received Packets	0	0	0	0
Sent Packets	0	0	0	0
Total Packets	0	0	0	0
Received Bytes	0	0	0	0
Sent Bytes	0	0	0	0
Total Bytes	0	0	0	0
Received Bytes/Sec	0	0	0	0
Sent Bytes/Sec	0	0	0	0
Error Packets Received	0	0	0	0
Dropped Packets Received	0	0	0	0
Sessions	0	0	0	0
New Sessions/Sec	0	0	0	0
Upstream Bandwidth Usage(%)	0	0	0	0
Downstream Bandwidth Usage(%)	0	0	0	0

Refresh

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 Source Address

Enable Traffic Statistic

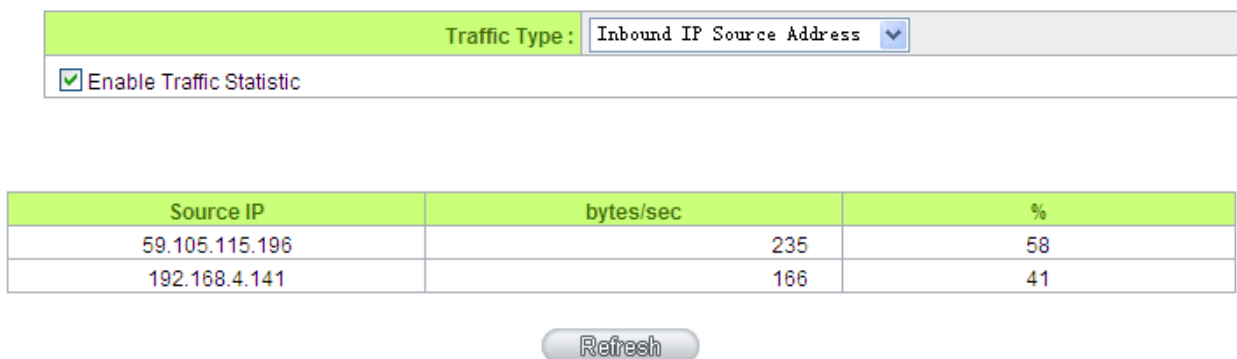
Source IP	bytes/sec	%
-----------	-----------	---

Refresh

By Inbound IP Address :

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

Traffic Statistic



Traffic Type: Inbound IP Source Address

Enable Traffic Statistic

Source IP	bytes/sec	%
59.105.115.196	235	58
192.168.4.141	166	41

Refresh

By outbound IP Address :

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

Traffic Statistic

Traffic Type: Outbound IP Source Address Enable Traffic Statistic

Source IP	bytes/sec	%
59.105.115.196	8	100

Refresh

By Inbound Port :

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

Traffic Statistic

Traffic Type: Inbound IP Service Enable Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	ssh(22)	248	89
UDP	dns(53)	28	10

Refresh

By Outbound Port :

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

Traffic Statistic

Traffic Type : Outbound IP Service Enable Traffic Statistic

Protocol	Dest. Port	bytes/sec	%
TCP	ssh(22)	423	93
TCP	http(80)	22	4
UDP	dns(53)	9	1

Refresh

By Inbound Session :

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

Traffic Statistic

Traffic Type : Inbound IP Session Enable Traffic Statistic

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
59.105.115.196	TCP	80	122.116.174.226	1924	347	53
192.168.1.211	TCP	22	58.215.87.207	35600	135	20
192.168.1.211	TCP	22	58.215.87.207	33049	86	13
192.168.1.211	TCP	22	58.215.87.207	37342	51	7
192.168.1.211	UDP	32789	192.168.5.21	53	28	4

Refresh

By Outbound Session :

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

Traffic Statistic

Traffic Type : Outbound IP Session

Enable Traffic Statistic

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.211	TCP	22	58.215.87.207	50521	121	58
59.105.115.196	TCP	80	122.116.174.226	1924	41	20
192.168.1.211	TCP	22	58.215.87.207	52821	27	13
192.168.1.211	UDP	32789	192.168.5.21	53	16	7

12.4 IP/ Port Statistic

The GIGABIT Router 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.

Log

- System Log
- System Statistic
- Traffic Statistic
- IP/Port Statistic**
- QRTG

IP/Port Statistic

Enable IP/Port Statistic Specific IP/Port status for : Port Port:

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

Enable IP/Port Statistic Specific IP/Port status for: **IP** IP address : 192 . 168 . 4 . 141

Source IP	Protocol	Source Port	Interface (WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.4.141	TCP	80	WAN1	192.168.4.166	3664	0	0
192.168.4.141	TCP	80	WAN1	192.168.4.166	3665	54	42
192.168.4.141	TCP	80	WAN1	192.168.4.166	3670	0	0
192.168.4.141	TCP	80	WAN1	192.168.4.166	3662	0	0
192.168.4.141	TCP	80	WAN1	192.168.4.166	3661	116	2216
192.168.4.141	TCP	80	WAN1	192.168.4.166	3668	0	0
192.168.4.141	TCP	80	WAN1	192.168.4.166	3669	0	0
192.168.4.141	TCP	80	WAN1	192.168.4.166	3671	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

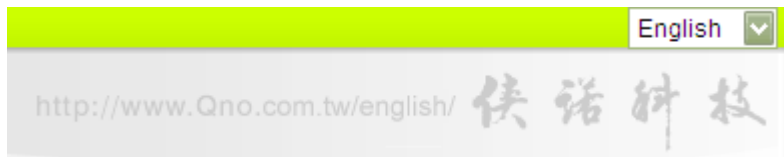
Enabled

Search Type: **Service Port** Service Port : 80

Source IP	Protocol	Source Port	Interface	Dest. IP	Dest. Port	Downstream Bandwidth Bytes/Sec	Upstream Bandwidth Bytes/Sec
192.168.1.100	TCP	1290	WAN2	207.46.111.14	80	217	85
192.168.1.100	TCP	1944	WAN2	203.69.138.19	80	0	0

XIII 、 Log out

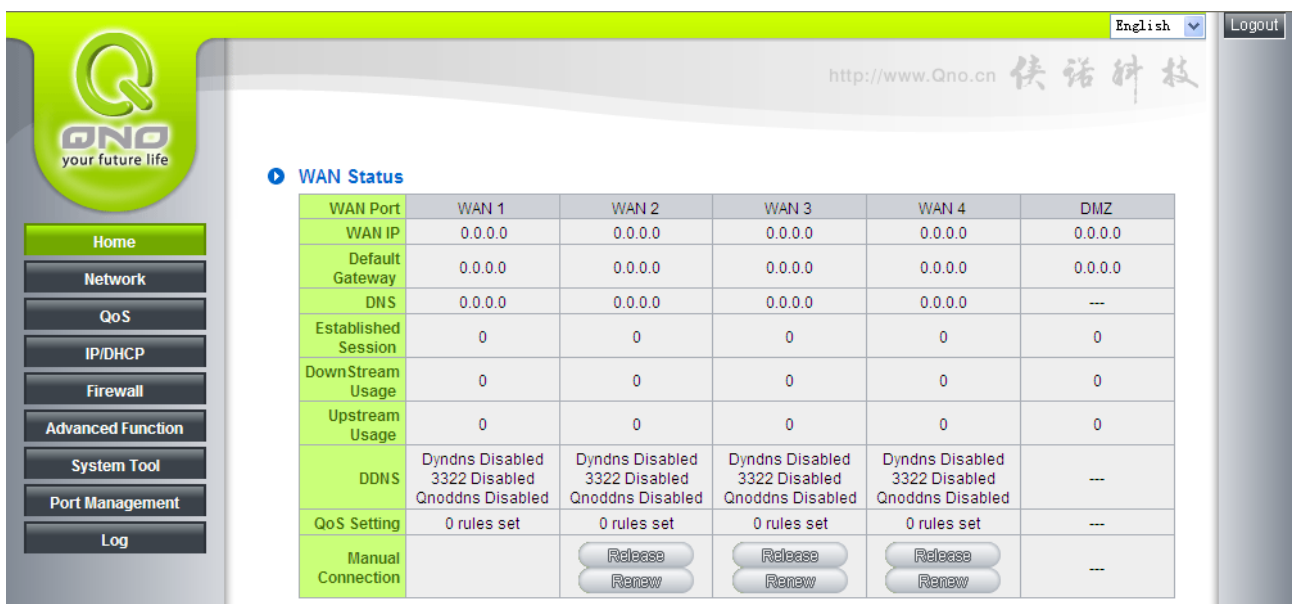
On the top right corner of the web- based UI, there is a Logout button. Click on it to log out of the web- based UI. To enter next time, open the Web browser and enter the IP address, user name and password to log in.



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 VPN Firewall capability at the same time.本章

Router overall interface is as below.



The screenshot shows the WAN Status page in the QNO router's web interface. The page features a navigation menu on the left with options like Home, Network, QoS, IP/DHCP, Firewall, Advanced Function, System Tool, Port Management, and Log. The main content area displays a table for WAN Status with columns for WAN Port, WAN 1, WAN 2, WAN 3, WAN 4, and DMZ. The table lists various parameters such as WAN IP, Default Gateway, DNS, Established Session, DownStream Usage, Upstream Usage, DDNS, QoS Setting, and Manual Connection. The Manual Connection row includes buttons for Release and Renew for each WAN port.

WAN Port	WAN 1	WAN 2	WAN 3	WAN 4	DMZ
WAN IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
DNS	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	---
Established Session	0	0	0	0	0
DownStream Usage	0	0	0	0	0
Upstream Usage	0	0	0	0	0
DDNS	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	Dyndns Disabled 3322 Disabled Qnoddns Disabled	---
QoS Setting	0 rules set	0 rules set	0 rules set	0 rules set	---
Manual Connection		Release Renew	Release Renew	Release Renew	---

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
QoS		VIII. QoS
	Bandwidth Management	8.1 (QoS) 8.3 Bandwidth Management
	Session Control	8.2 Session Limit
IP/DHCP		VII. Port Management
	Setup	7.3 DHCP/ IP

	Status	7.4 DHCP Status
	IP & MAC Binding	7.5 IP & MAC Binding
	IP Grouping	7.6 IP Grouping
Firewall		IX. Firewall
	General Policy	9.1 General Policy 9.2 Restricted Application
	Access Rule	9.3 Access Rule
	Content Filter	9.4 Content Filter
Advanced Function		X. Advanced Setting
	DMZ Host	10.1 DMZ Host
	Routing	10.2 Routing
	One to One NAT	10.3 One to One NAT
	DDNS	10.4 DDNS
	MAC Clone	10.5 MAC Clone
System Tool		XI. 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
	Time	5.2 Change and Set Login Password and Time
	System Recover	11.4 System Recover
Port Management		VII. Port Management
	Setup	7.1 Setup
	Status	7.2 Status
Log		XII. Log
	System Log	12.1 System Log
	System Status	12.2 System Status
	Traffic Statistic	12.3 Traffic Statistic
	IP/Port statistic	1.4 IP/Port statistic

Appendix II: Troubleshooting

(1) Block BT Download

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

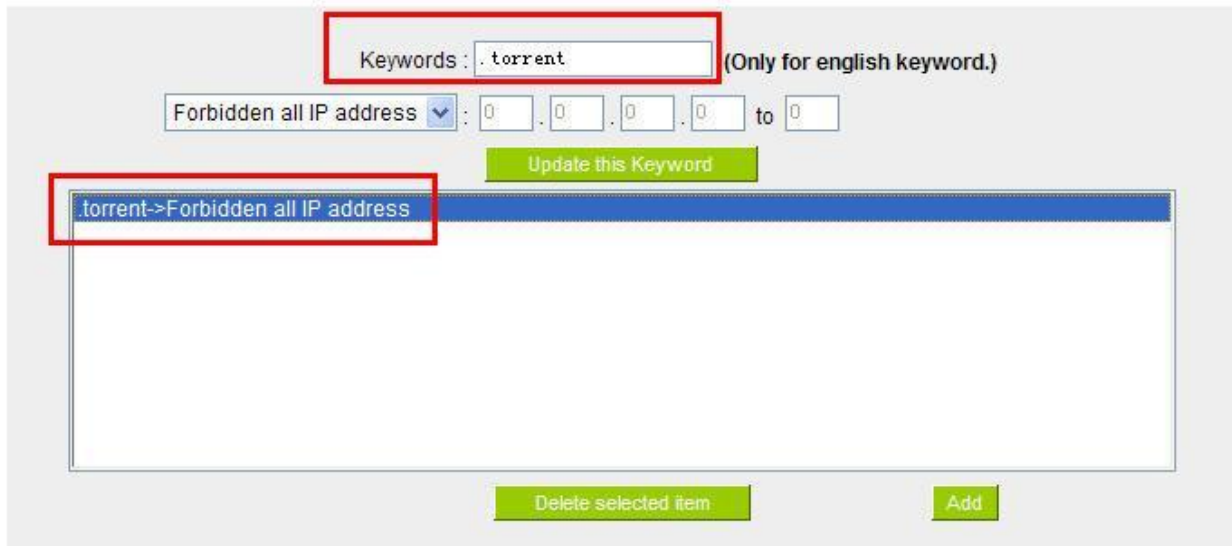
- Accept Allowed Domains
- Block Forbidden Domains

Forbidden Domains

Enabled

Website Blocking by Keywords

Enabled



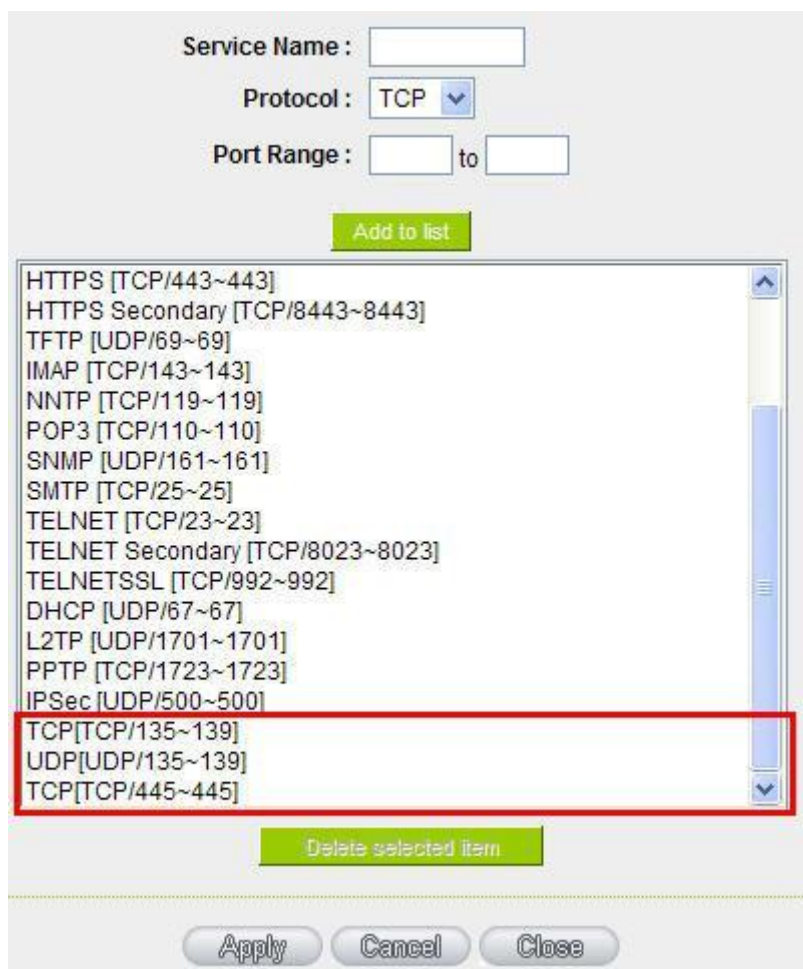
Keywords : (Only for english keyword.)

Forbidden all IP address . . . to

(2) 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

Add to list

- 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]

Delete selected item

Apply Cancel Close

- 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]	Service Port Management
Log:	No log	
Interface:	Any	
Source IP:	Any	
Dest. IP:	Any	

Scheduling

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

Back Apply Cancel

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	<input checked="" type="checkbox"/>	Allow	TCP [445]	*	Any	Any	Always		Edit	
2	<input checked="" type="checkbox"/>	Deny	UDP [135]	*	Any	Any	Always		Edit	
3	<input checked="" type="checkbox"/>	Deny	TCP [135]	*	Any	Any	Always		Edit	
	<input checked="" type="checkbox"/>	Allow	All Traffic [*]	LAN	Any	Any	Always			
	<input checked="" type="checkbox"/>	Deny	All Traffic [*]	WAN1	Any	Any	Always			

Add New Rule Return to Default Rules

(3) Block QQLive Video Broadcast Setting

QQLive Video broadcast software is a stream media broadcast software. Many clients are bothered by the same problem: When several users apply QQLive Video broadcast software, a greater share of the bandwidth is occupied, thus overloading the device. 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]	Service Port Management
Log :	No log	
Interface :	Any	
Source IP :	Any	
Dest. IP :	Single	121 . 14 . 75 . 115

▶ Scheduling

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

Back Apply Cancel

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** with repeat operation.

cache.tv.qq.com	loginqqlivedx.qq.com	qqlive.qq.com
58.60.11.145	219.133.49.159	219.133.62.70
58.60.11.146	loginqqlivewt.qq.com	tv1-3t.qq.com
58.60.11.147	58.251.63.13	221.236.11.40
59.36.97.5	loginqqlivexy.qq.com	tv2.qq.com
59.36.97.7	202.205.3.218	218.17.209.17
59.36.97.37		
219.133.63.48		

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

(4) ARP Virus Attack Prevention

1. ARP Issue and Information

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

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

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

IP	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, pinging the LAN IP to see the packet loss. Enter the ping 192.168.1.1 (Gateway IP address) as illustrated.

```

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

```

If there are cases of packet loss of the ping LAN IP and if 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 :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SPI (Stateful Packet Inspection) :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DoS (Denial of Service) :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Advanced
Block WAN Request :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Remote Management :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Port : <input type="text" value="80"/>
Multicast Pass Through :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Prevent ARP Virus Attack :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Router sends ARP <input type="text" value="20"/> times per-second.

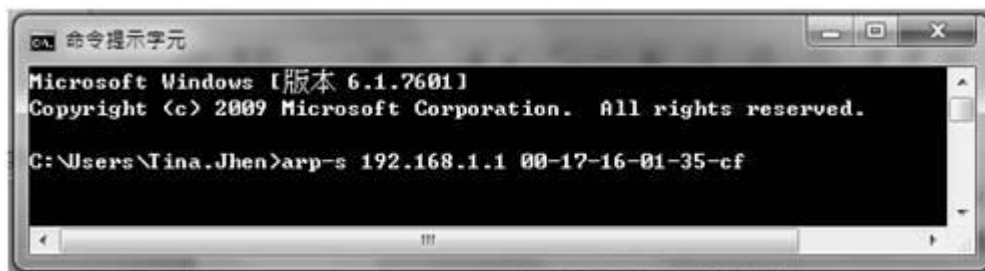
b) Bind the Gateway IP and MAC address for each PC

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 :	<input type="text" value="30"/> <input type="text" value="7e"/> <input type="text" value="95"/> <input type="text" value="99"/> <input type="text" value="94"/> <input type="text" value="be"/> (Default: 30-7e-95-99-94-be)
Device IP Address :	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="1"/>
Subnet Mask :	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="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.



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.

IP & MAC Binding

[Show new IP user](#)

Static IP : . . .

MAC Address : - - - - -

Name :

Enabled :

[Update this Entry](#)

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

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

Block MAC address on the list with wrong IP address

Block MAC address not on the list

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

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

Show new IP user

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	<input type="text"/>	<input type="checkbox"/>
192.168.1.100	00:20:ed:41:cb:9d	<input type="text"/>	<input type="checkbox"/>

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

Show new IP user

Static IP : . . .

MAC Address : - - - - -

Name :

Enabled :

Update this Entry

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

Delete selected item
Add

Block MAC address on the list with wrong IP address

Block MAC address not on the list

Show Table
Apply
Cancel

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](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](http://www.qno.com.tw/web/where_buy.asp)

Taiwan Support Center :

E- mail : QnoFAE@qno.com.tw