your future life

3WAN 1LAN Small Scale Multi-WAN QoS Router

Load Balance, Bandwidth Management, and Network Security

English User's Manual

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.

Content

1、Introduction

3WAN/1LAN Small Scale Multi-WAN QoS Router (The device) is designed for small internet café, enterprise, communities, and schools, which is economical and effective. The device has three WAN ports with load blance function. The WAN capatabilities can meet most bandwidth market spec. The device also has one 10/100 Base-T/TX Ethernets (RJ45) embedded for LAN use. LAN port can be linked to additional swithes in order to connect more network equipments.

Built- in Firewall can fulfill most enterprise requirements for preventing external network attacks. Firewall utilizes Prevent Arp Attack, Denial of Service, and SPI (Stateful Packet Inspection). Access rule setting can allow or forbid network access services, limit intranet user network usage.

Unique bandwidth management ensures administrators to have reasonable and effective allocation for limited network resources. Users don' t have to spend extra money on getting more bandwidth. Also, if downloading oppupies the bandwidth, administrator can choose rate control or priority for managing the bandwdith.

Except private and pulic IP translation, Network Address Translation (NAT) can allow many users have Internet access with only one public IP. DHCP support Class C IPs. Users can plan and manage the network environment by applying IP & MAC binding.

In addtion, the device includes One- to- One NAT to meet the demand for intranet server setup. Through management tools, network administrators can manage the device through Web browsers. At the same time, from various online system logs, administrators can have a clear understanding about network activities, have a definite strategy for Internet access rule management.

This manual describs the settings and details for each feature. If you are not sure about connecting the device with Internet, please read Quick Installation Guide first so that you can connect the device with Internet quickly.

You can visit www.Qno.com.tw for online information, as well as refer to Appendix 2：Qno Tehcnical Support Information to contact FAE support.

2、Hardware Installation

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

2.1 Firewall LED Signal

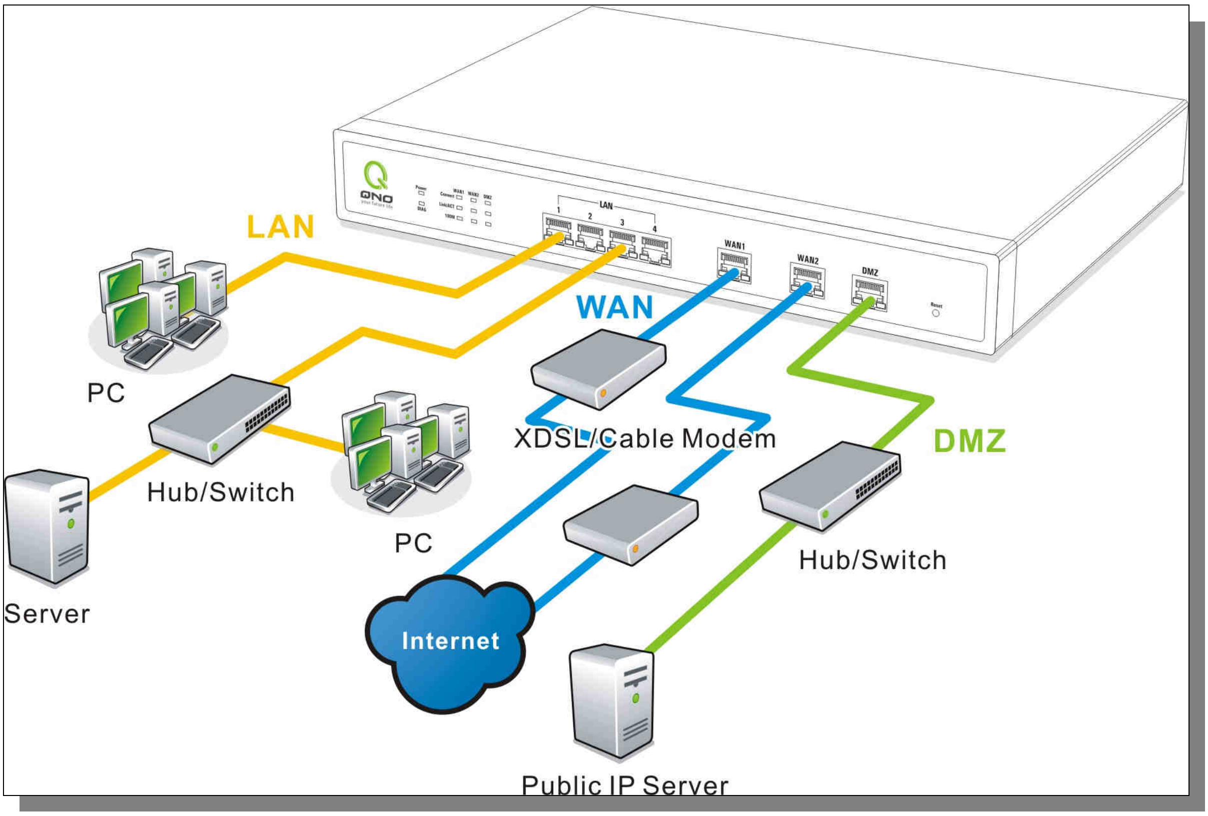
LED Status

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.
100Mbps / 10Mbps	Amber	Amber LED on: Ethernet is running at 100Mbps. Amber LED off: Ethernet is running at 10Mbps.
Connect	Green	Green LED on: WAN port is connected and got an IP address. Green LED off: WAN port does not get an IP address.

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.

2.2 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.

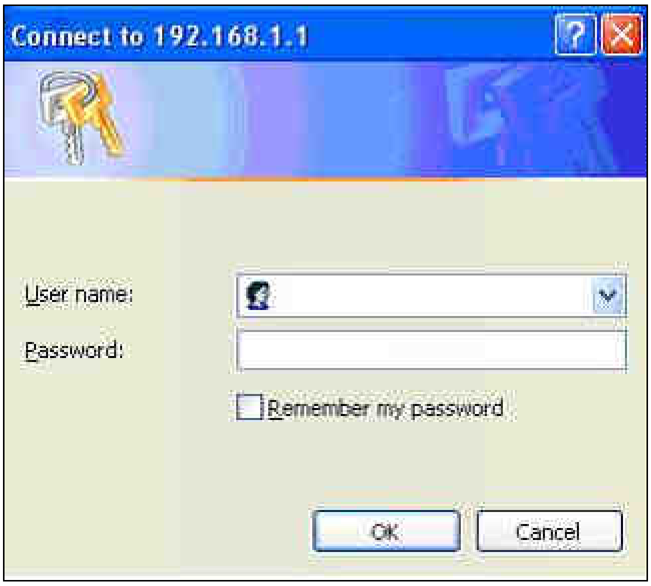
LAN Connection: The LAN port can be connected to a Switching Hub or directly to a PC. Users can use servers for monitoring or filtering through the port after "Physical Port Mangement" configuration is done.

3、Quick Connection Settings

This chapter introduces setting screens, Homepage messages, and basic connection.

3.1 Login

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



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

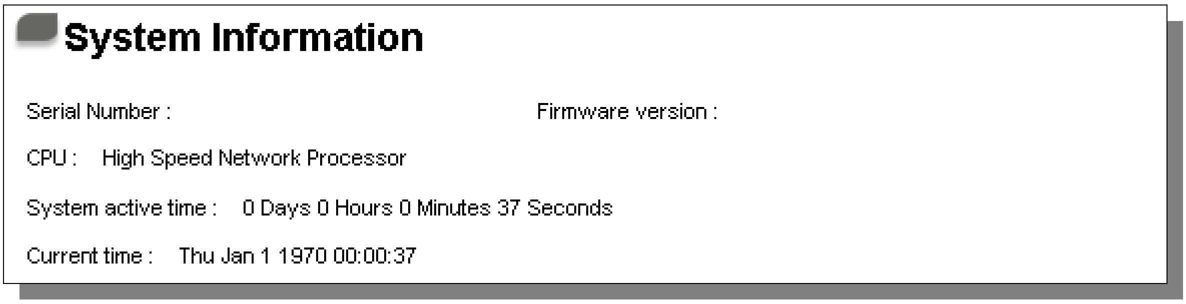
Attention!

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.

3.2 **Home Page**

In the Home page, all firewall router parameters and status are listed for users’ reference.

3.2.1 System Information



System Information

Serial Number : Firmware version :

CPU : High Speed Network Processor

System active time : 0 Days 0 Hours 0 Minutes 37 Seconds

Current time : Thu Jan 1 1970 00:00:37

Serial Number : This number is the device serial number.

Firmware version : Information about the device current software version.

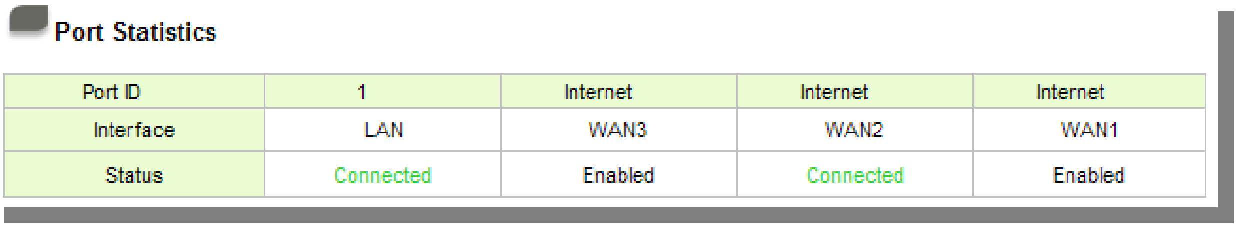
CPU : Information abou the device current CPU.

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

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.

3.2.2 Port Statistics

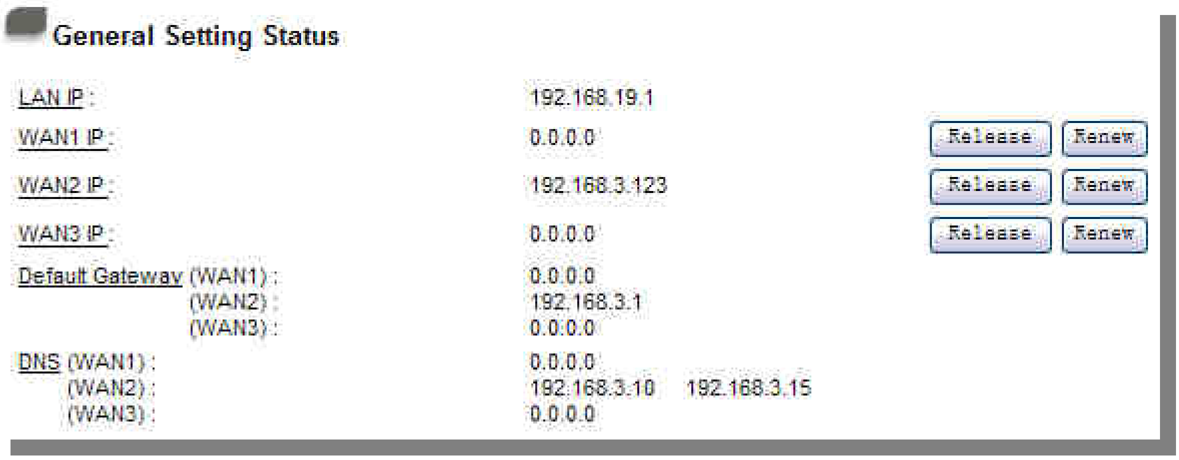


Port Statistics

Port ID	1	Internet	Internet	Internet
Interface	LAN	WAN3	WAN2	WAN1
Status	Connected	Enabled	Connected	Enabled

The status of all system ports, including Connected, Enabled, and Closed, will be shown.

3.2.3 General Setting Status



General Setting Status

LAN IP : 192.168.19.1

WAN1 IP : 0.0.0.0

WAN2 IP : 192.168.3.123

WAN3 IP : 0.0.0.0

Default Gateway (WAN1) : 0.0.0.0
(WAN2) : 192.168.3.1
(WAN3) : 0.0.0.0

DNS (WAN1) : 0.0.0.0
(WAN2) : 192.168.3.10 192.168.3.15
(WAN3) : 0.0.0.0

LAN IP:

Indicates the LAN port current IP configuration. The default IP is 192.168.1.1. Click the hyperlink to enter and manage the configuration.

WAN 1, WAN2, WAN3 IP:

Indicates the WAN1, WAN2, and WAN3 current IP configuration. Click each hyperlink to enter and manage the configuration. When "Obtain an IP automatically" is selected, two buttons (Release and Renew) will appear on the right of the page. Click "Release" to release the IP that is issued by the ISP, and click "Renew" to refresh the IP that is issued by the ISP. If a WAN connection, such as PPPoE or PPTP, is selected, "Disconnect" and "Connect" will appear on the page.

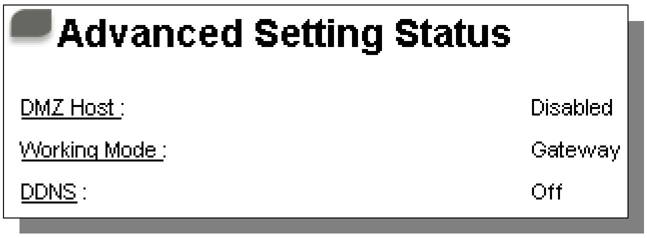
Default Gateway:

Indicates the current Gateway IP configuration. Click the hyperlink to enter and manage the configuration.

DNS:

Indicates the current DNS IP configuration. Click the hyperlink to enter and manage the configuration.

3.2.4 Advanced Setting Status



Advanced Setting Status

DMZ Host : Disabled

Working Mode : Gateway

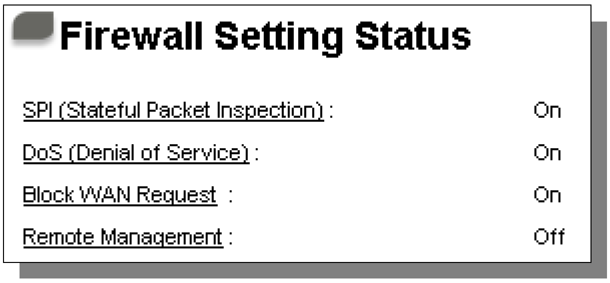
DDNS : Off

DMZ Host： Identifie if DMZ function is enabled. Users can click the hyper link to enter the setting directly. System default is "Disabled".

Working Mode：Identifies the current working mode (could be either NAT Gateway or Router mode). Users can click the hyper link to enter the setting directly. System default is NAT Gateway mode.

DDNS： Show if the DDNS function is enabled. Users can click the hyper link to enter the setting directly. System default is "Disabled".

3.2.5 Firewall Setting Status



Firewall Setting Status

SPI (Stateful Packet Inspection) :	On
DoS (Denial of Service) :	On
Block WAN Request :	On
Remote Management :	Off

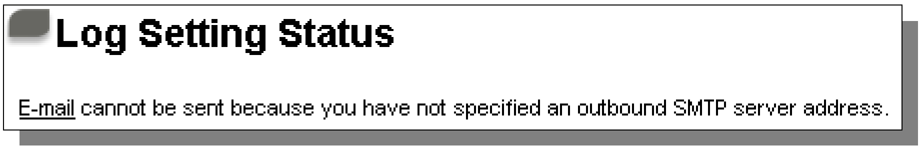
SPI (Stateful Packet Inspection)： Indicates whether SPI (Stateful Packet Inspection) is on or off. The default configuration is "On".

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".

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".

3.2.6 Log Setting Status



Log Setting Status

E-mail cannot be sent because you have not specified an outbound SMTP server address.

The E-Mail hyperlink will be connected to Syslog page.

1. If the e-mail server has not been configured in the log setting, the information will appear as "**E-MAIL can not be sent because you have not specified an outbound SMTP server address**."

2. If the e-mail server has been configured in the log setting but e-mail transmission conditions are not reached the threshold, the information will appear as "**E-MAIL settings have been configured**."

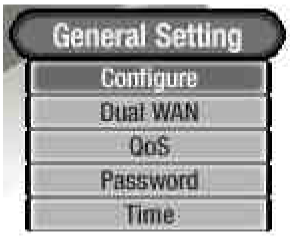
3. If the e-mail server has been configured in the log setting and the log has been transmitted to the e-mail server, the information will appear as "**E-MAIL settings have been configured and sent out**."

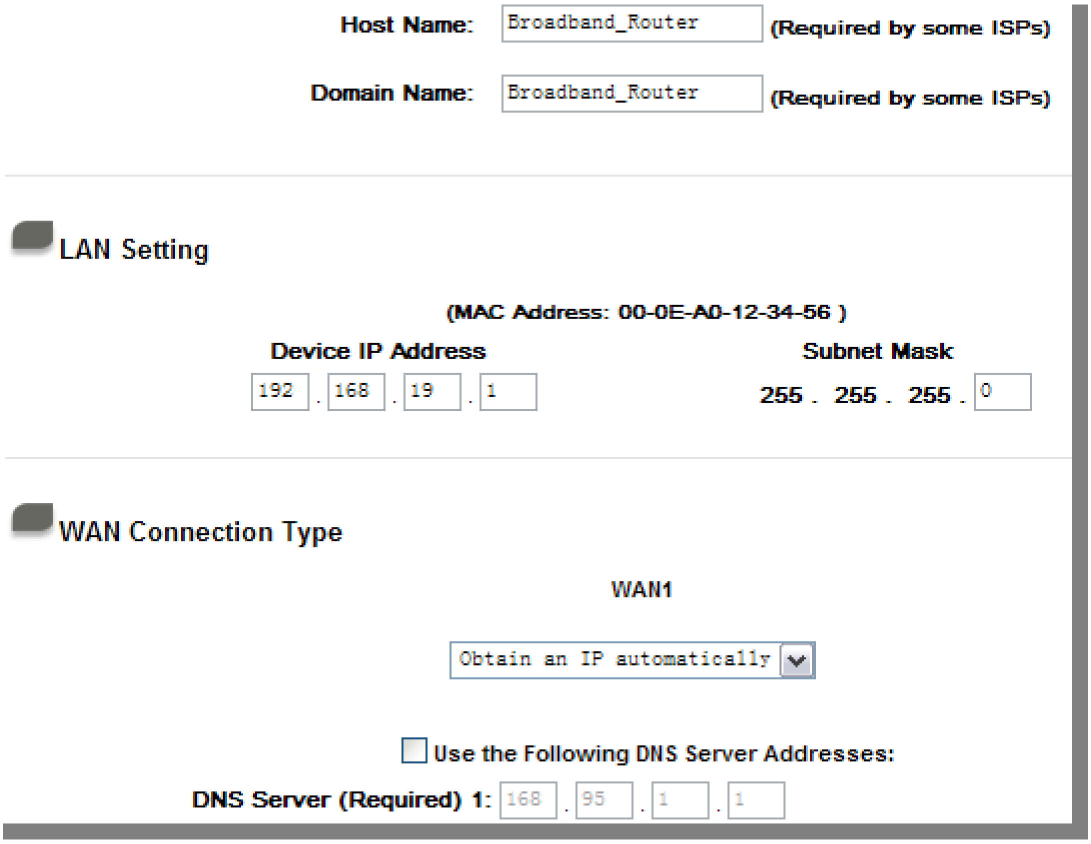
4. If the e-mail server has been configured in the log setting but the log is not able to be sent to the e-mail server, the information will appear as "**E-MAIL cannot be sent out, probably use incorrect settings.**"

3.3 Basic Connection Settings

This General Setting 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.

3.3.1 General Setting





Host Name: Broadband_Router (Required by some ISPs)

Domain Name: Broadband_Router (Required by some ISPs)

LAN Setting

(MAC Address: 00-0E-A0-12-34-56)

Device IP Address: 192 . 168 . 19 . 1

Subnet Mask: 255 . 255 . 255 . 0

WAN Connection Type

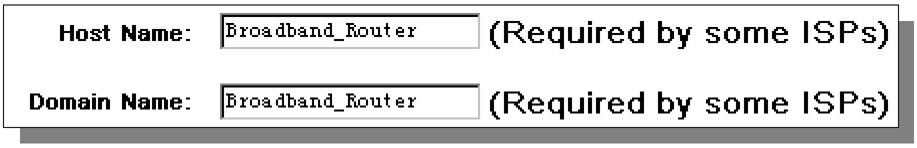
WAN1

Obtain an IP automatically

□ Use the Following DNS Server Addresses:

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

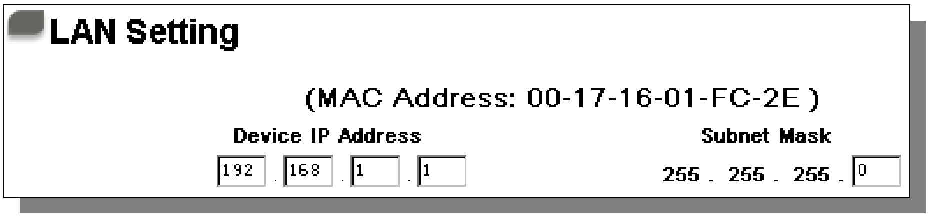
Host Name and Domain Name : Device name and domain name can be input in the two boxes. Though this configuration is not necessary in most environments, some ISPs in some countries may require it.



Host Name: Broadband_Router (Required by some ISPs)

Domain Name: Broadband_Router (Required by some ISPs)

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



LAN Setting

(MAC Address: 00-17-16-01-FC-2E)

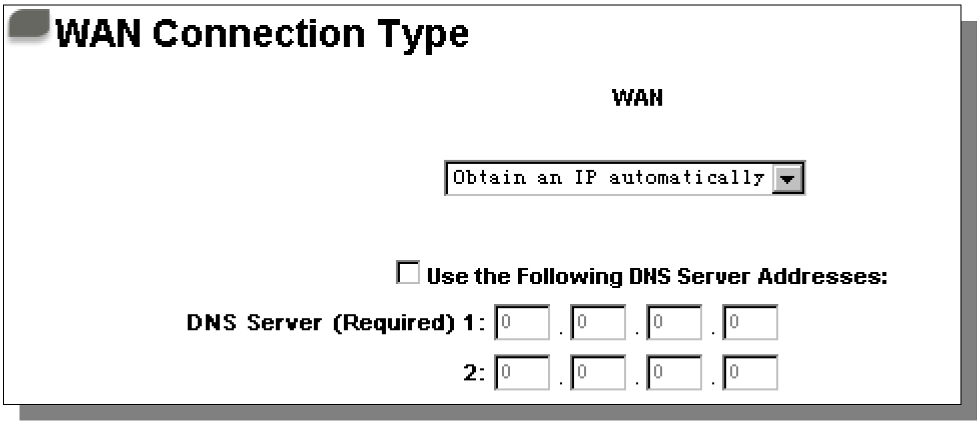
Device IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255 . 255 . 255 . 0

WAN and the Internet Connection Configuration

Obtain an IP automatically：

This is the device system default connection mode. This mode is often used in the connection mode to obtain an automatic DHCP IP, such as cable modem or DHCP client connection. 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.



WAN Connection Type

WAN

Obtain an IP automatically

□ Use the Following DNS Server Addresses:

DNS Server (Required) 1: 0 . 0 . 0 . 0

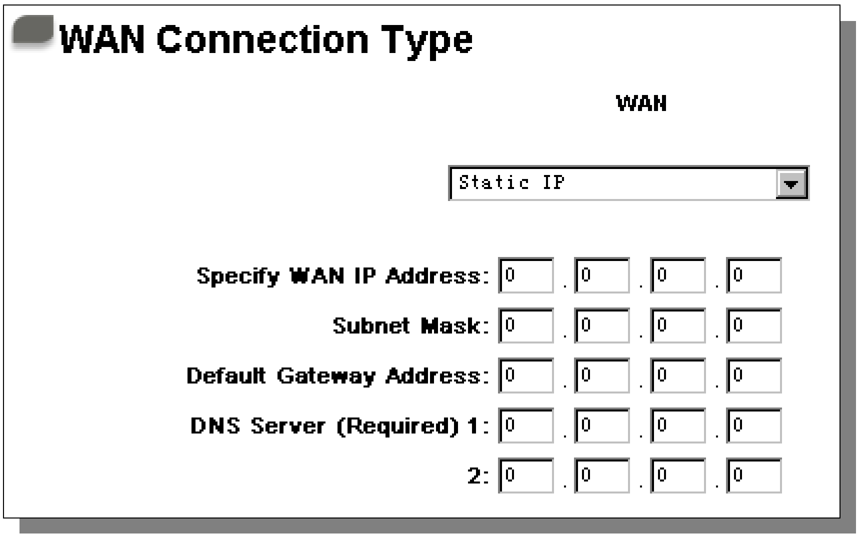
2: 0 . 0 . 0 . 0

Use the Following DNS Server Address：	Select a user-defined DNS server IP address.
DNS Server：	Input the DNS IP address set by ISP. At least one IP group should be input. The maximum acceptable is two IP groups.

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

Static IP：

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



WAN Connection Type

WAN

Static IP

Specify WAN IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway Address: 0 . 0 . 0 . 0

DNS Server (Required) 1: 0 . 0 . 0 . 0

2: 0 . 0 . 0 . 0

Specify 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

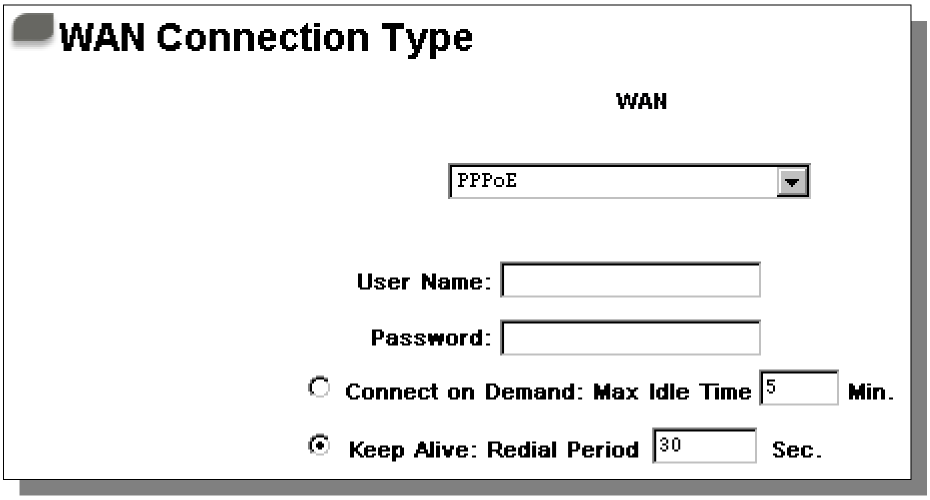
Defaule Gateway Address： Input the default gateway issued by ISP. For ADSL users, it is usually an ATU-R IP address. As for optical fiber users, please input the optical fiber switching IP.

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. Input the user connection name and password issued by ISP. Then use the built- in PPP Over-Ethernet software to connect with the Internet. If the PC has been installed with the PPPoE dialing software provided by ISP, please remove it. This software will no longer be used for network connection.



WAN Connection Type

WAN

PPPoE

User Name:

Password:

○ Connect on Demand: Max Idle Time 5 Min.

● Keep Alive: Redial Period 30 Sec.

User Name： Input the user name issued by ISP.

Password： Input the password issued by ISP.

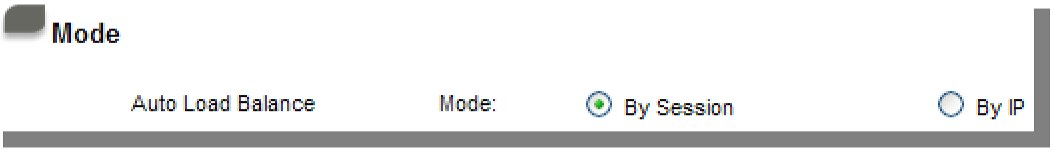
Connect on Demand：Max Idle Time___Min.： This function enables the auto-dialing PPPoE connection. When the client port attempts to connect with the Internet, the device will automatically make a dial connection. If the line has been idle for a period of time, the system will disconnect the link automatically. The default time for automatic disconnection when there is no packet transmissions is five minutes. Users can enter the time frame by themselves.

Keep Alive：Redial Period___Sec.： This function enables the PPPoE dial connection to keep connected, and to automatically redial if the line is interrupted. It also enables a user to set up a time for redialing. The default is 30 seconds.

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

3.3.2 Multi- WAN Setting

Users must choose Dual WAN from Dual WAN/ DMZ mode in the general setting before proceeding the setting.



Mode

Auto Load Balance Mode: ● By Session ○ By IP

This device provides two load balance: by sessions or by IP. 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!

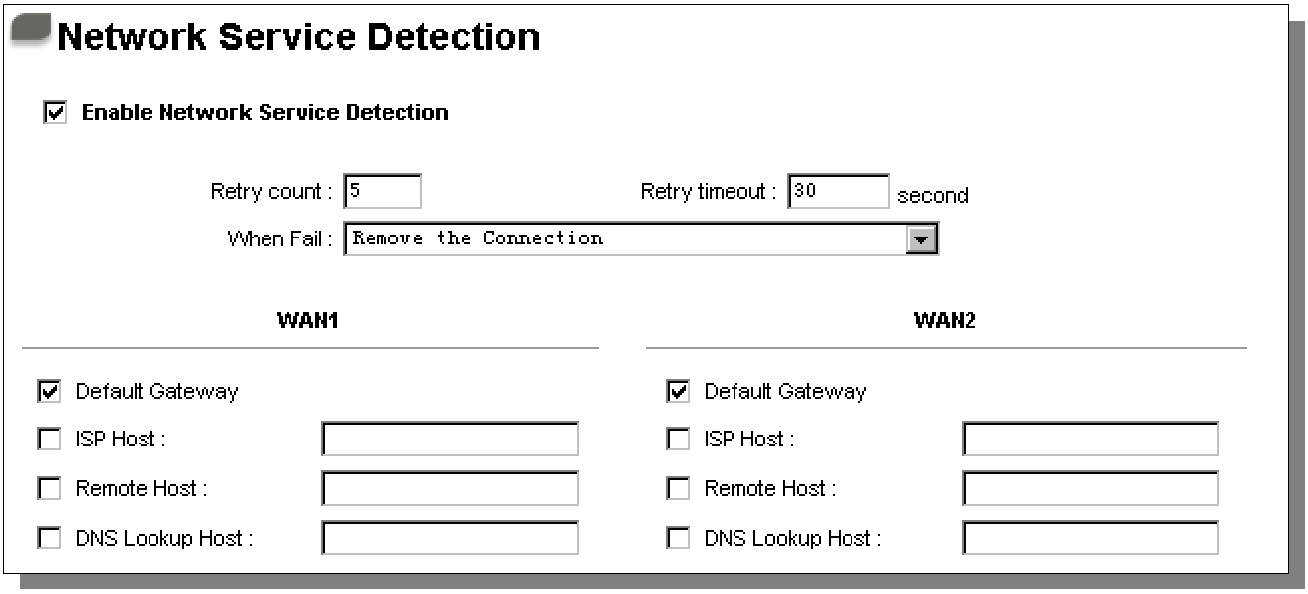
For either session balancing or IP connection balancing, collocation with Protocol Binding will provide a more flexible application for bandwidth. Users can assign a specific Intranet IP to go through a specific service provider for connection, or assign an IP for a specific destination to go through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

Network Service Detection



Network Service Detection

☑ Enable Network Service Detection

Retry count : 5   Retry timeout : 30 second

When Fail : Remove the Connection

WAN1		WAN2	
☑ Default Gateway		☑ Default Gateway	
□ ISP Host :		□ ISP Host :	
□ Remote Host :		□ Remote Host :	
□ DNS Lookup Host :		□ DNS Lookup Host :	

Enable Network Service Detection： If this option is selected, information such “**Retry Count**” or “**Retry Timeout**” will be displayed. If two WANs are used for external connection, be sure to activate the NSD system, so as to avoid any unwanted break caused by the device misjudgment of the overload traffic for the WAN.

Retry count： This selects the retry times for network service detection. The default is five times. If there is no feedback from the Internet in the configured “Retry Times", it will be judged as “External Connection Interrupted”.

Retry timeout： Delay time for external connection detection latency. The default is 30 seconds. After the retry timeout, external service detection will restart.

When Fail： (1) Generate the Error Condition in the System Log: If an ISP connection failure is detected, an error message will be recorded in the System Log. This line will not be removed; therefore, the some of the users on this line will not have normal connections.

This option is suitable under the condition that one of the WAN connections has failed; the traffic going through this WAN to the destination IP cannot shift to another WAN to reach the destination. For example, if users want the traffic to 10.0.0.1 ~ 10.254.254.254 to go only through WAN1, while WAN2 is not to support these destinations, users should select this option. When the WAN1 connection is interrupted, packets for 10.0.0.1~10.254.254.254 cannot be transmitted through WAN 2, and there is no need to remove the connection when WAN 1 is interrupted.

(2) Remove the Connection: If an ISP connection failure is detected, no error message will be recorded in the System Log. The packet transmitted through this WAN will be shifted to the other WAN automatically, and be shifted back again when the connection for the original WAN is repaired and reconnected.

This option is suitable when one of the WAN connections fails and the traffic going through this WAN to the destination IP should go through the other WAN to reach the destination. In this way, when any of the WAN connections is broken, other WANs can serve as a backup; traffic can be shifted to a WAN that is still connected.

Detecting Feedback Servers:

Defaule Gateway： The local default communication gateway location, such as the IP address of an ADSL router, will be input automatically by the device. Therefore, users just need to check the option if this function is needed.

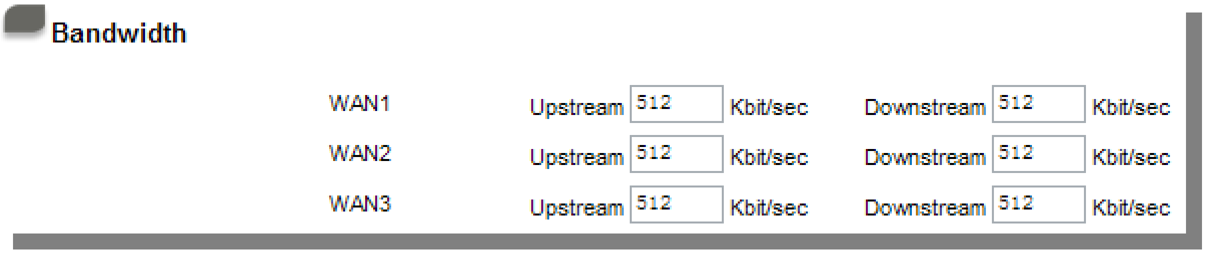
ISP Host： This is the detected location for the ISP port, such as the DNS IP address of ISP. When configuring an IP address for this function, make sure this IP is capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port)

Remote Host： This is the detected location for the remote Network Segment. This Remote Host IP should better be capable of receiving feedback stably and speedily. (Please input the DNS IP of the ISP port).

DNS Lookup Host： This is the detect location for DNS. (Only a web address such as www.hinet.net is acceptable here. Do not input an IP address.) In addition, do not input the same web address in this box for two different WANs.

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

Bandwidth



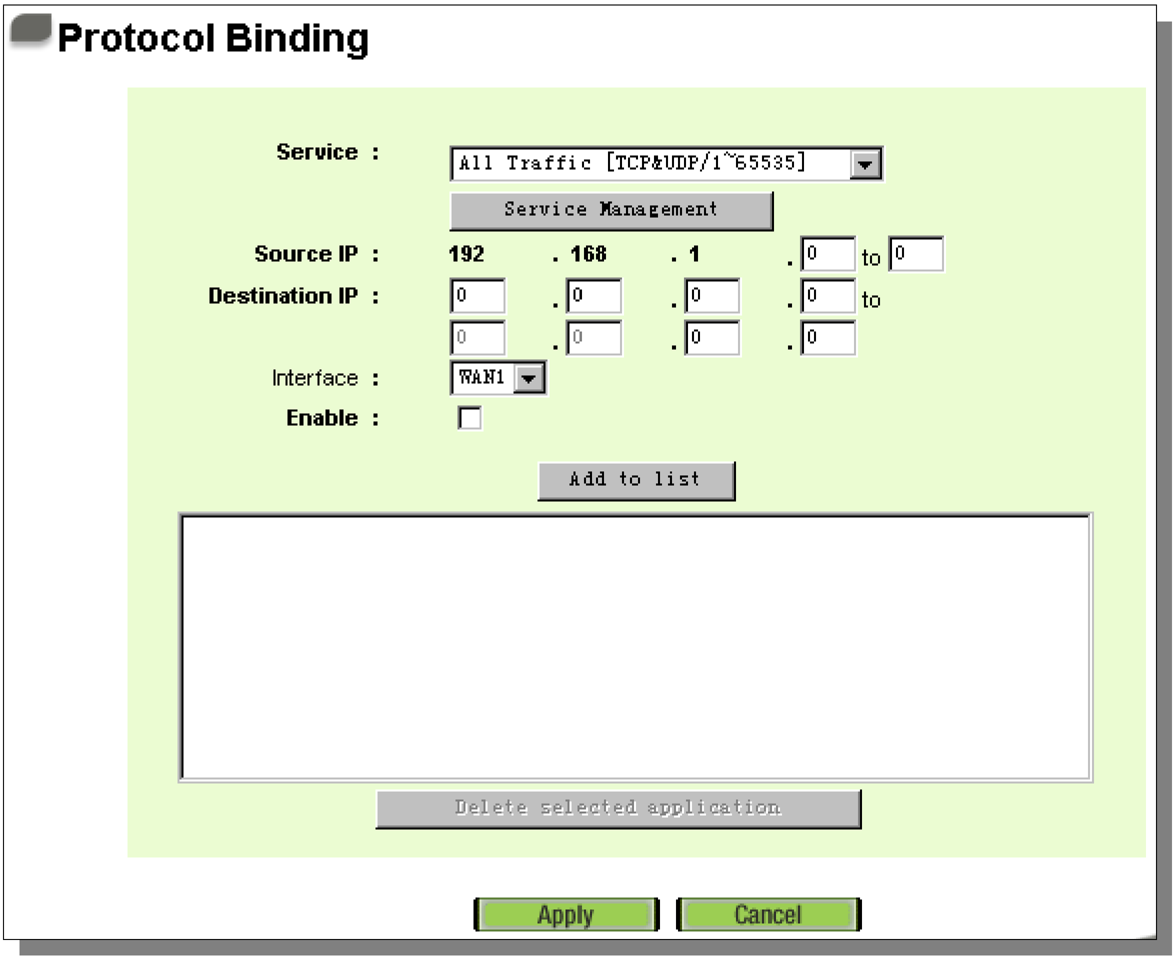
Bandwidth

WAN1	Upstream	512	Kbit/sec	Downstream	512	Kbit/sec
WAN2	Upstream	512	Kbit/sec	Downstream	512	Kbit/sec
WAN3	Upstream	512	Kbit/sec	Downstream	512	Kbit/sec

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

3.3.3 Protocol Binding

Users can assign traffic for specific IPs or services go out from the assigned WAN ports. The remaingin IPs or service will follow the original load balance mechanism.



Protocol Binding

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

Service Management

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

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

Interface : WAN1

Enable : □

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. 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： Activate the rule.

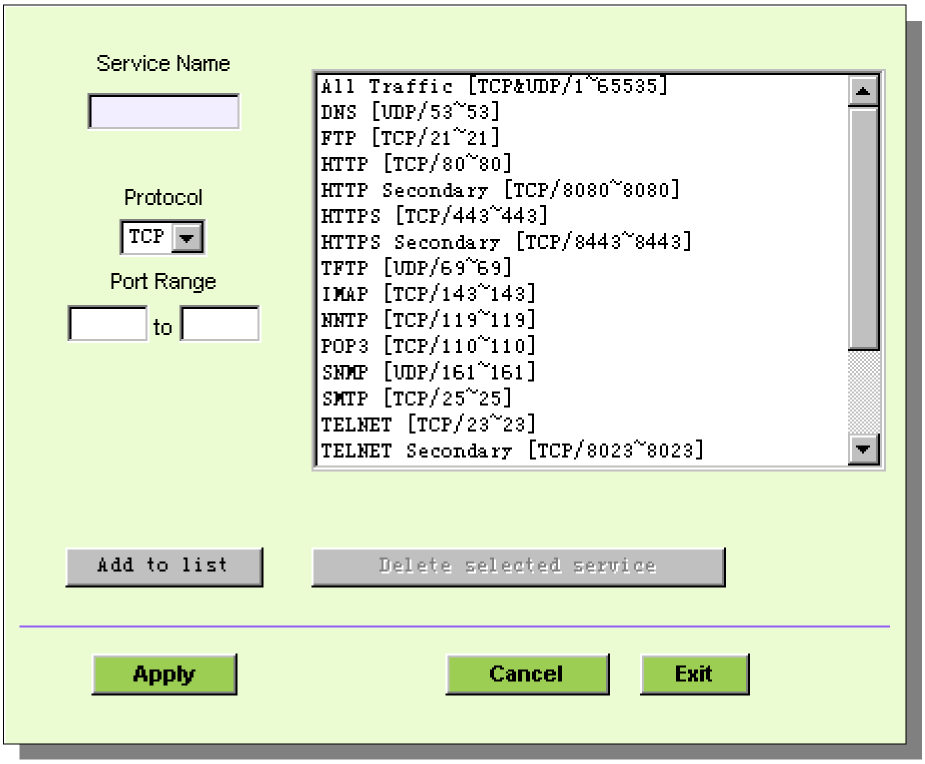
Add to list： Add this rule to the list.

Delete selected application： Remove the rules selected from the Service List.

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

Service Management

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



Protocol: TCP

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

Service Name : 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 : Remove the selected activated Services.

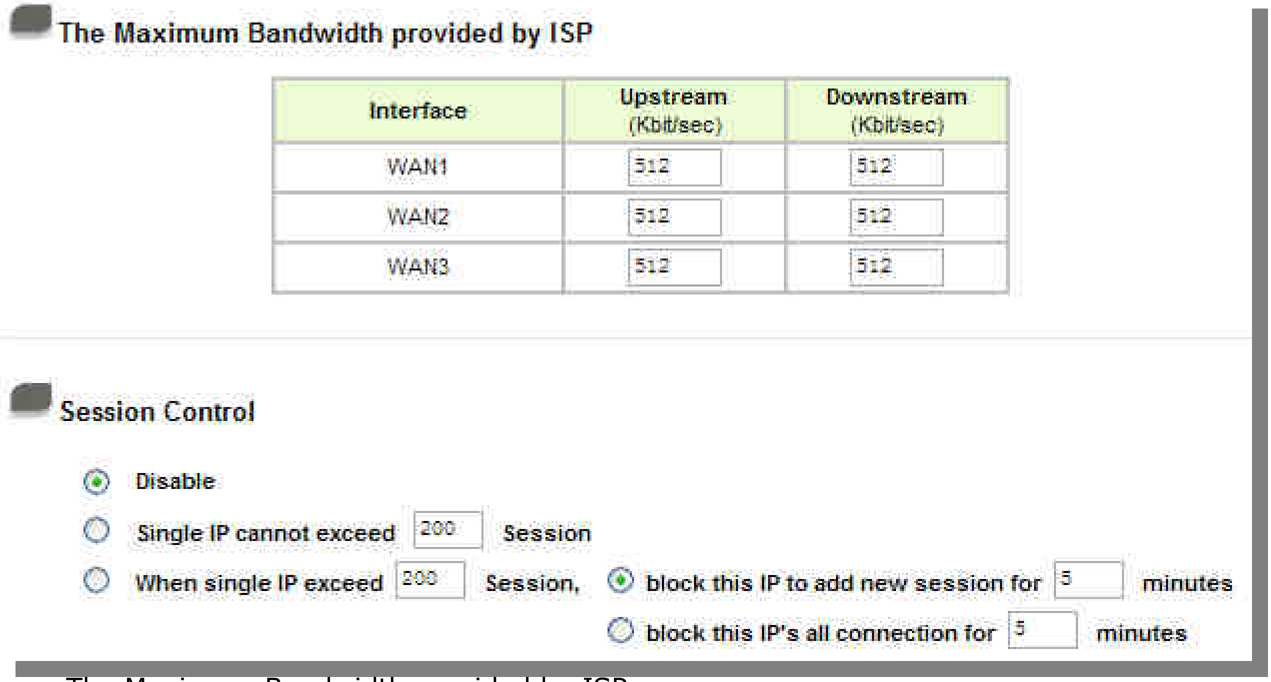
Apply : Click the "**Apply**" button to save the modification.

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

Exit : To quit this configuration window.

3.3.4 Quality of Service (QoS)

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



The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN1	512	512
WAN2	512	512
WAN3	512	512

Session Control

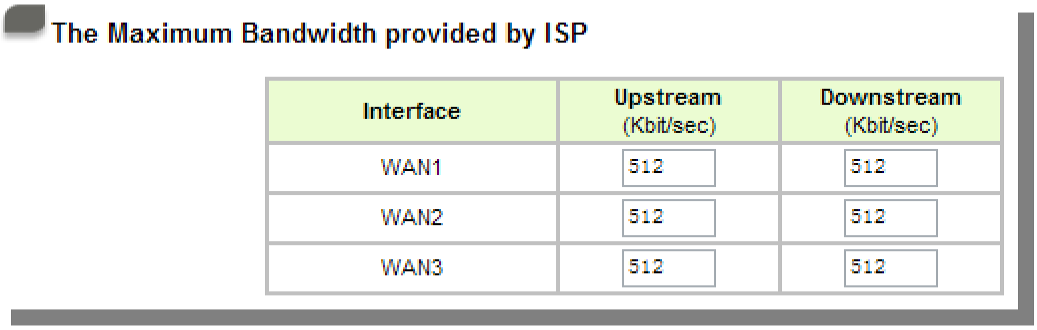
● Disable

○ Single IP cannot exceed 200 Session

○ When single IP exceed 200 Session, ● block this IP to add new session for 5 minutes

○ block this IP's all connection for 5 minutes

The Maximum Bandwidth provided by ISP



The Maximum Bandwidth provided by ISP

Interface	Upstream (Kbit/sec)	Downstream (Kbit/sec)
WAN1	512	512
WAN2	512	512
WAN3	512	512

In the boxes for WAN1, WAN2, WAN3 bandwidth, input the upstream and downstream bandwidth which users applied for from bandwidth supplier. The bandwidth QoS will make calculations according to the data users input. In other words, it will guarantee a minimum rate of upstream and downstream for each IP and Service Port based on the total actual bandwidth of WAN1 and WAN2. For example, if the upstream bandwidths of both WAN1 and WAN2 are 512Kbit/Sec, the total upstream bandwidth will be: WAN1 + WAN2 = 1024Kbit/Sec. Therefore, if there are 50 IPs in the Intranet, the minimum guaranteed upstream bandwidth for each IP would be 1024Kbit/50=20Kbit/Sec. Thus, 20Kbit/Sec can be input for "Mini. Rate" Downstream bandwidth can be calculated in the same way.

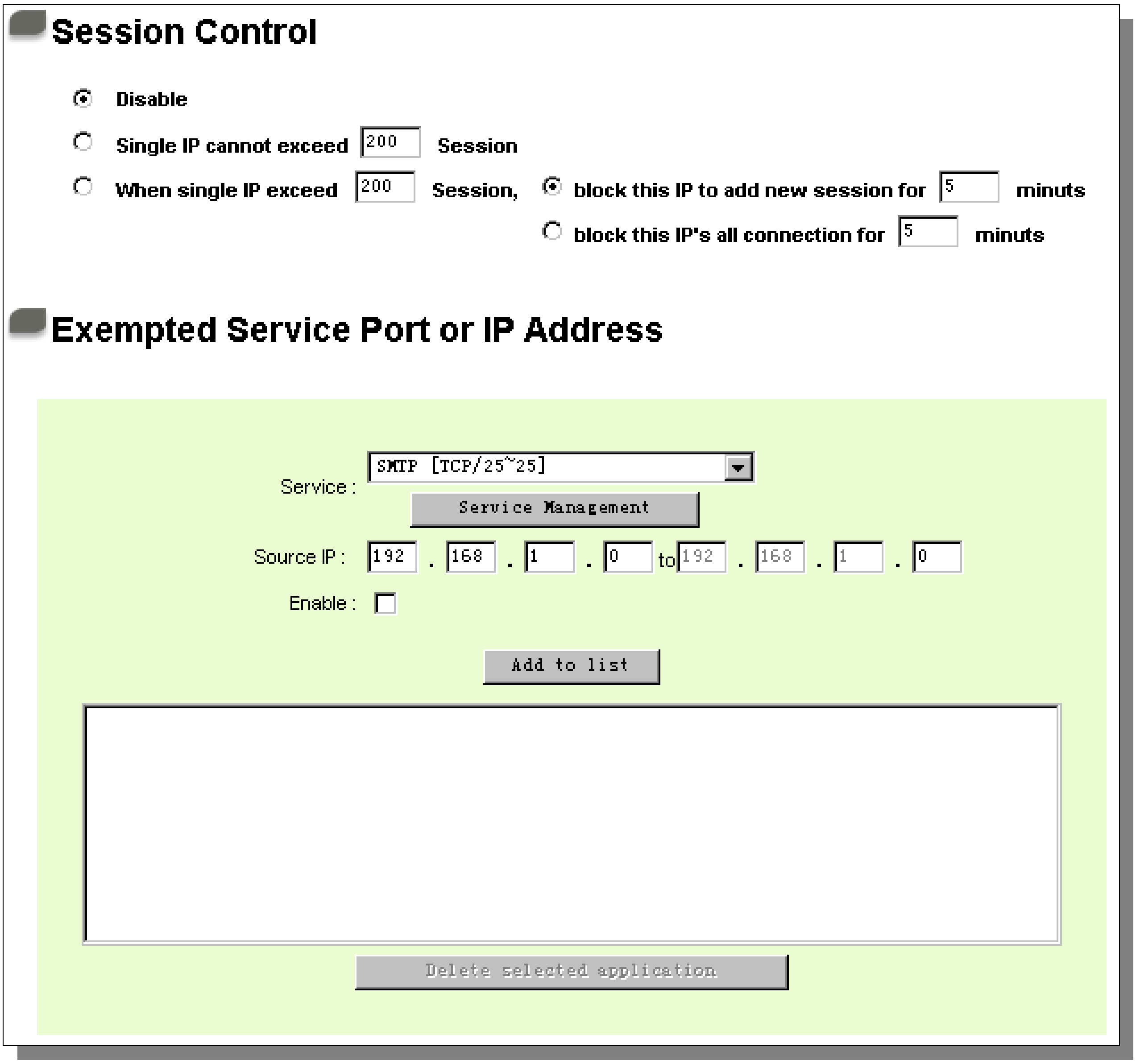
Attention！

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

Session Limit

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

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



Session Control

● Disable

○ Single IP cannot exceed 200 Session

○ When single IP exceed 200 Session, ● block this IP to add new session for 5 minuts

○ block this IP's all connection for 5 minuts

Exempted Service Port or IP Address

Service : SMTP [TCP/25~25]

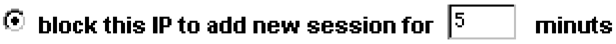
Source IP : 192 . 168 . 1 . 0 to 192 . 168 . 1 . 0

Enable : □

Disable : Disable Session Control function. ◦

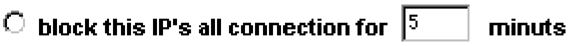
Single IP cannot exceed___session : This option enables the restriction of maximum external connections to each Intranet PC. When the number of external connections reaches the limit, to allow new connections to be built, some of the existing connections must be closed. For example, when BT or P2P is being used to download information and the connections exceed the limit, the user will be unable to connect with other services until either BT or P2P is closed.

When Single IP exceed___session：



● block this IP to add new session for 5 minuts

If this function is selected, when the user's port connection reach the limit, this user will not be able to make a new connection for five minutes. Even if the previous connection has been closed, new connections cannot be made until the setting time ends.



○ block this IP's all connection for 5 minuts

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.

Exempted Service Port or IP Address：

The important services or IPs in a company or business can be configured to be free of the Connection Restriction Rule.

Service：

Select a Service Port to be free of the connection rule.

Source IP：

Add IP addresses/Groups that are free from restriction.

Enable：

Activate the added rule.

Add to list：

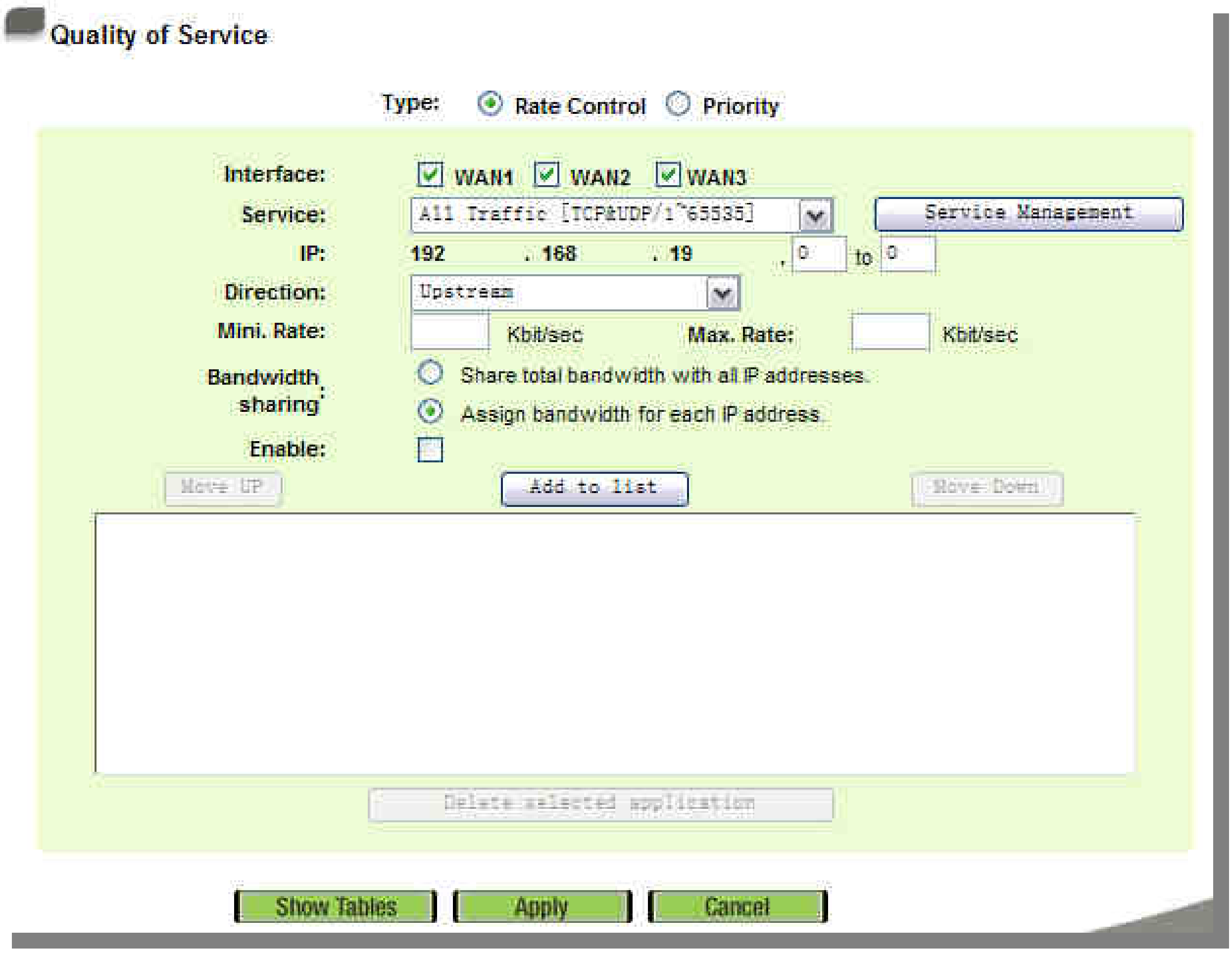
Add the rule into the list.

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

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

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 ○ Priority

Interface: ☑ WAN1 ☑ WAN2 ☑ WAN3

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

IP: 192 . 168 . 19 . 0 to 0

Direction: Upstream

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

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

Enable: □

Interface : Select on which WAN the QoS rule should be executed. It can be a single selection or multiple selections.

Service : Select what bandwidth control is to be configured in the QoS rule. If the bandwidth for all services of each IP is to be controlled, select “All (TCP&UDP) 1~65535”. If only FTP uploads or downloads need to be controlled, select “FTP Port 21~21”. Refer to the Default Service Port

Number List.

IP：

This is to select which user is to be controlled. If only a single IP is to be restricted, input this IP address, such as "192.168.1.100 to 100". The rule will control only the IP 192.168.1.100. If an IP range is to be controlled, input the range, such as "192.168.1.100 ~ 150". The rule will control IPs from 192.168.1.100 to 150. If all Intranet users that connect with the device are to be controlled, input "0" in the boxes of IP address. This means all Intranet IPs will be restricted. QoS can also control the range of Class B.

Direction：

Upstream: Means the upload bandwidth for Intranet IP.

Downstream: Means the download bandwidth for Intranet IP.

Server in LAN, Upstream: If a Server for external connection has been built in the device, this option is to control the bandwidth for the traffic coming from outside to this Server.

Server in LAN, Downstream: If there are web sites built in the Intranet, this option is to control the upload bandwidth for the connections from outside to this Server. For example, game servers have been built in many Internet cafés. This rule can be used to control the bandwidth for connections from outside to the game server of a café to update data. In this way, game players inside the café will not be affected.

Mini.Rate &
Max.Rate：
(Kbit/Sec)

Mini. Rate: The rule is to guarantee minimum available bandwidth.

Max. Rate: This rule is to restrict maximum available bandwidth. The maximum bandwidth will not exceed the limit set up under this rule.

Bandwidth
sharing：

Sharing total bandwidth with all IP addresses: If this option is selected, all IPs or Service Ports will share the bandwidth range (from minimum to maximum bandwidth).

Assign bandwidth for each IP address: If this option is selected, every IP or Service Port in this range can have this bandwidth (minimum to maximum.). For example: If the rule is set for the IP of each PC, the IP of each PC will have the same bandwidth.

Enable： Activate the rule.

Add to list： Add this rule to the list.

Move Up & Move Down： The QoS rules will be executed from the bottom of the list to the top of the list. In other words, the lower down the list, the higher the priority of execution. Users can arrange the sequence according to their priorities. Usually the service ports which need to be restricted, such as BT, e-mule etc., will be moved to the bottom of the list. The rules for certain IPs would then be moved upward.

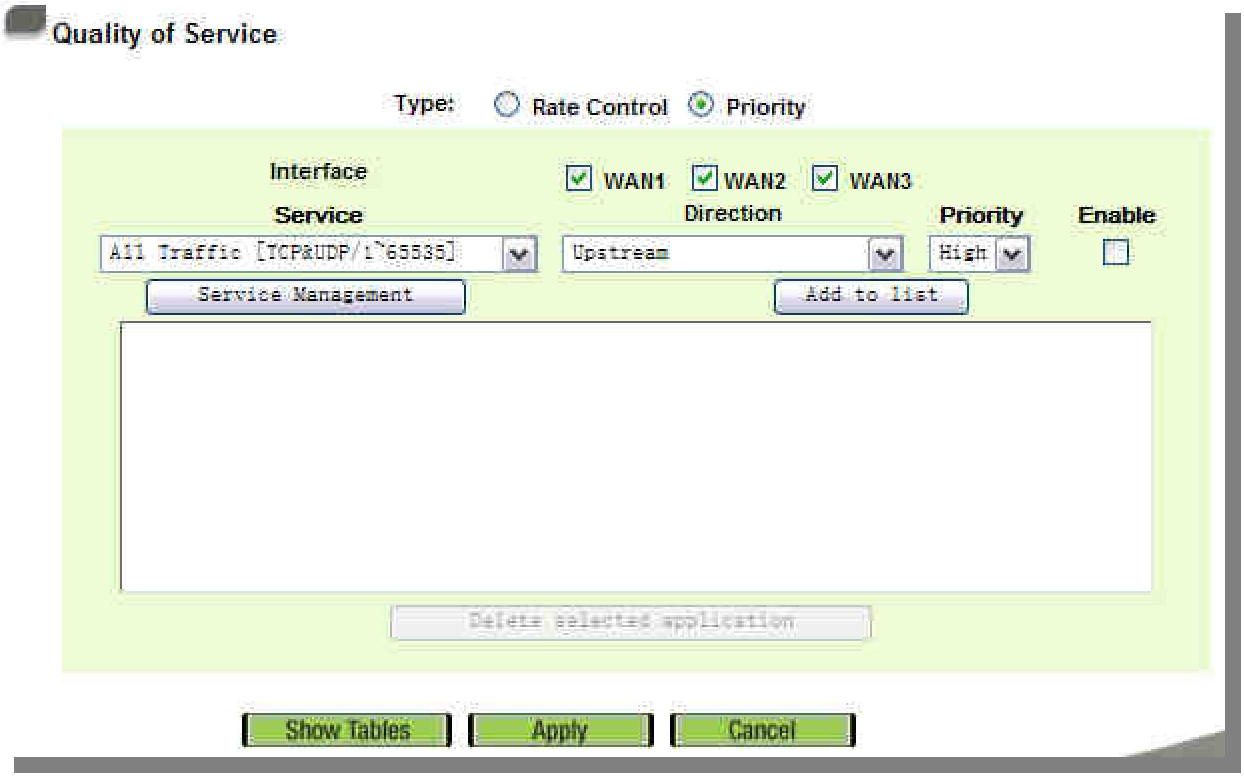
Delete selected Application： Remove the rules selected from the Service List.

Show Tables： This will display all the rules users made for the bandwidth. Click “Edit” to modify.

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

Priority：

Users can choose the service priority as planned. The device will allocate the bandwidth for High(60%) and Low(10%). If user set Port 8 for High, the device will allow 60% of the total bandwidth for Port 80 packets. If users set FTP Port 21 for Low, the device will allow 10 % of the total bandwidth for FTP service. Un- identified services will share 30% of the total bandwidth.



Quality of Service

Type: ○ Rate Control ● Priority

Interface ☑ WAN1 ☑ WAN2 ☑ WAN3

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

Direction: Upstream

Priority: High

Enable □

Interface： Choose which WAN will be applied for the priority setting

Service： Choose the service port for the priority rule. For example, if the service is FTP, choose FTP Port21~21.

Direction： Upstream：Control the service for upstream traffic.
Downstream：Control the service for downstream traffic.

Priority： High：This grarantees the service port with 60% bandwidth.
Low：This limits the service port with 10% bandwidth.

Enable： Activate the rule.

Add to list： Add the rule to the list.

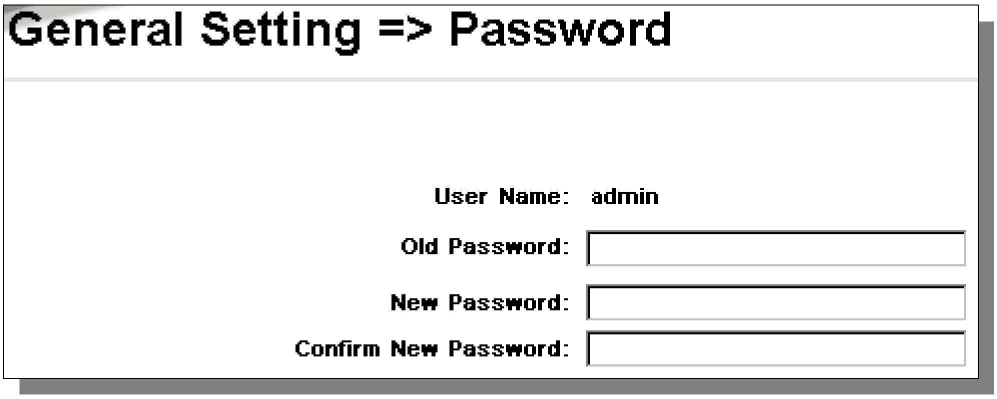
Delete selected Application： Remove the rules selected from the Service List.

Show Tables： This will display all the rules users made for the bandwidth. Click “Edit” to modify.

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

3.3.5 Password

This is an advanced management tool for the device. The default password of the host is "admin". For safety concern, we strongly recommend that changing the password after the first- time login is required. Please keep the password, or you might not login the firewall router. You will have to retrun the factory default if the password is lost.



General Setting => Password

User Name: admin

Old Password:

New Password:

Confirm New Password:

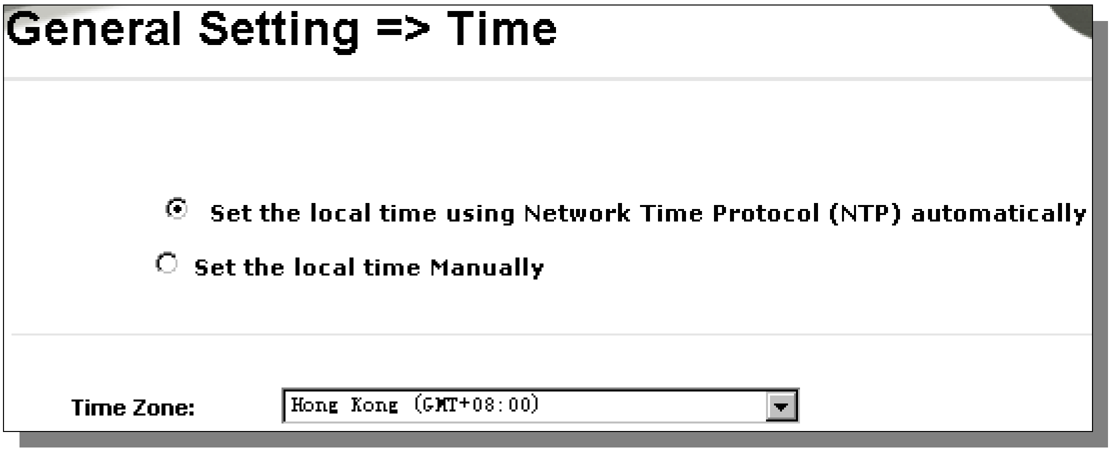
User Name：	The default is "admin".
Old Password：	Input the original password.
New Password：	Input the new user name.
Confirm New Password：	Input the new password again for verification.

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

3.3.6 Time

A function to calculate the correct time is available with the device. Users can either select the embedded NTP Server synchronization function or set up a time reference. This function enables users to know the exact time of event occurrences that are recorded in the System Log, and the time of closing or opening access for Internet resources.

Set the local time using Network Time Protocol (NTP) automatically：Firewall router has built-in NTP server which will update time automatically.



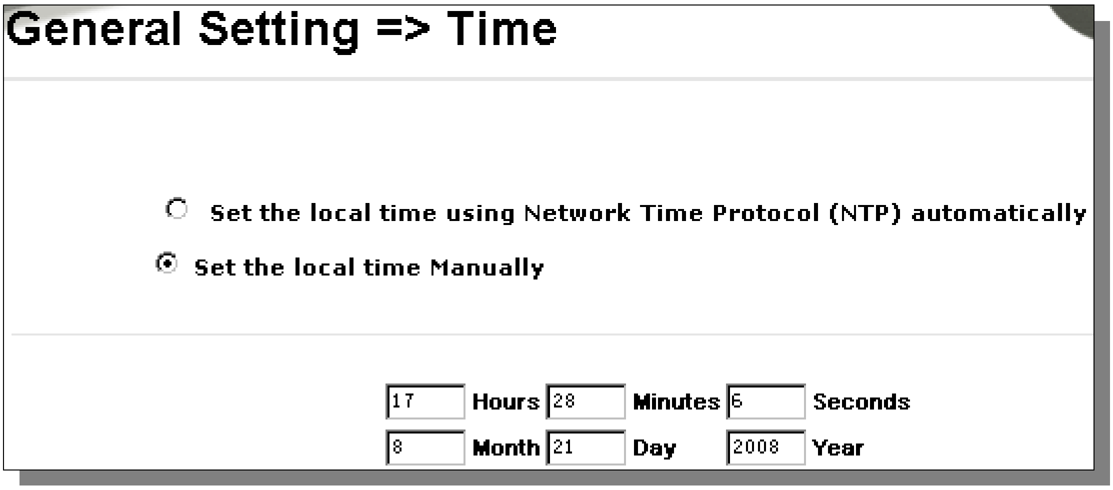
General Setting => Time

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

○ Set the local time Manually

Time Zone: Hong Kong (GMT+08:00)

Set the local time Manually：Enter the correct time.



General Setting => Time

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

● Set the local time Manually

17 Hours 28 Minutes 6 Seconds

8 Month 21 Day 2008 Year

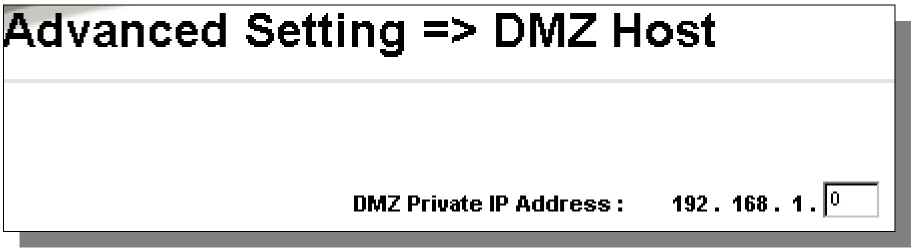
After the changes are completed, click **"Apply"** to save the configuration, or click **"Cancel"** to leave without making any changes.

4、Advanced Setting

This chaptor introduces advanced settings, including virtual server, routing, IP mapping and DDNS.

4.1 DMZ Host

When you keyin the private IP into this DMZ ption, public IPs for WAN1 and WAN2 will be applied for this computer only. That is, packets for WAN will be sent to this computer.



Advanced Setting => DMZ Host

DMZ Private IP Address : 192 . 168 . 1 . 0

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 disabled.

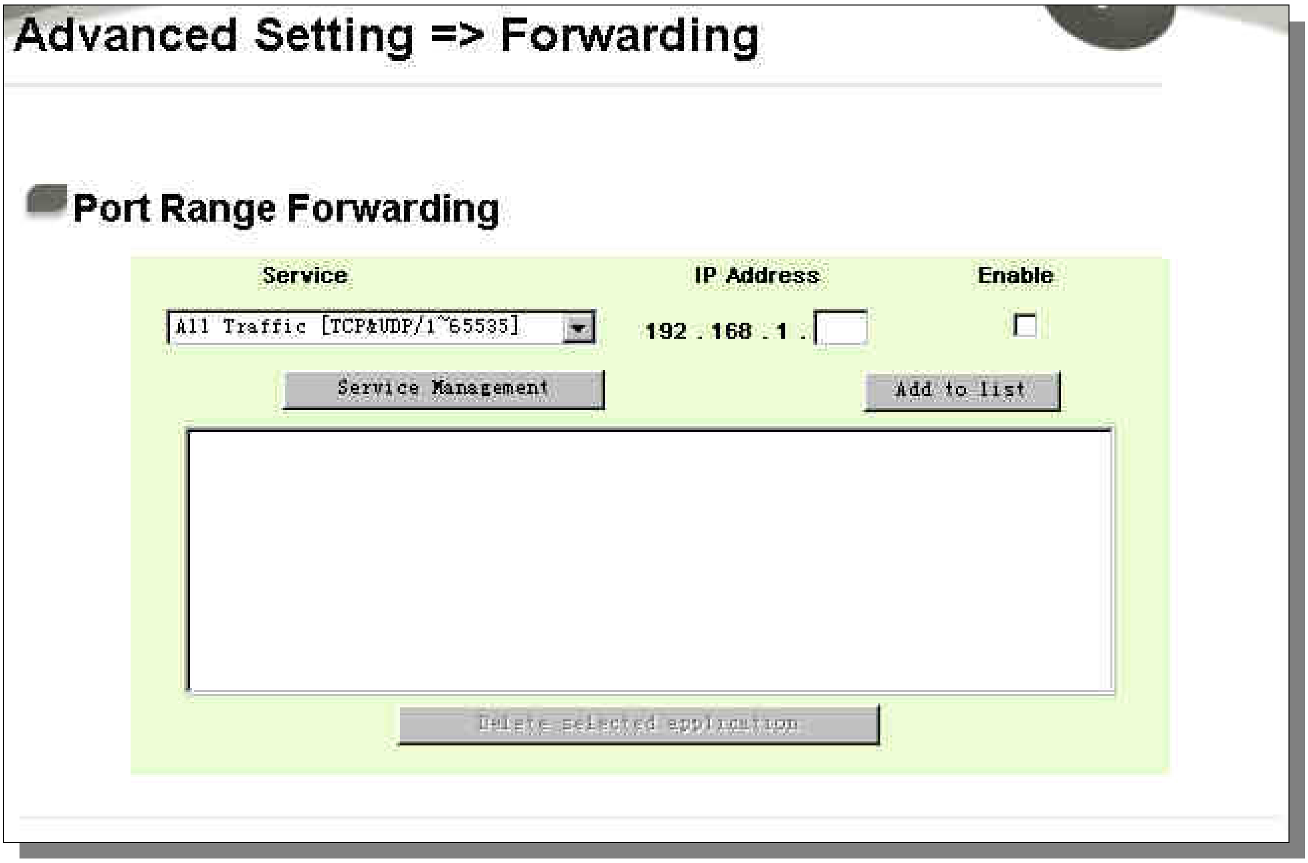
After the changes are completed, click **“Apply”** to save the network configuration modification, or click **“Cancel"** to leave without making any changes.

4.2 Forwarding

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

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

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



Service： Select from this option the default list of service ports of the virtual host that users want to activate.

Such as: All (TCP&UDP) 0~65535, 80 (80~80) for WWW, and 21~21 for FTP. Please refer to the list of default service ports.

IP Address： Input the virtual host IP addresses. For example, 192.168.1.100

Enable： Activate this function

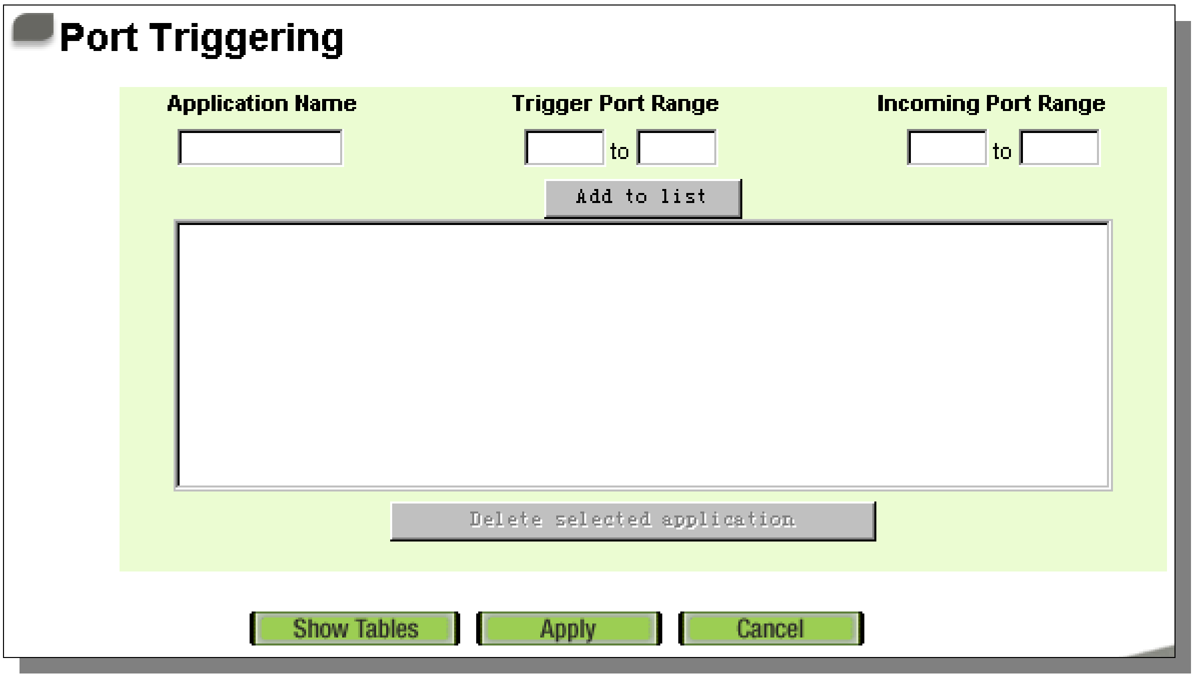
Service Management： Add or remove service ports from the list of service ports.

Add to list： Add to the active service content.

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

Port Triggering :

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



Application Name : Users can define names for special application software. This is to make management simple.

Trigger Port Range : Input the port numbers for data going from the device to the Internet. For example, 9000~10000

Incoming Port Range : Input the port numbers for data coming in from the Internet to the device. For example, 2004~2005

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

Delete selected application : Remove selected services.

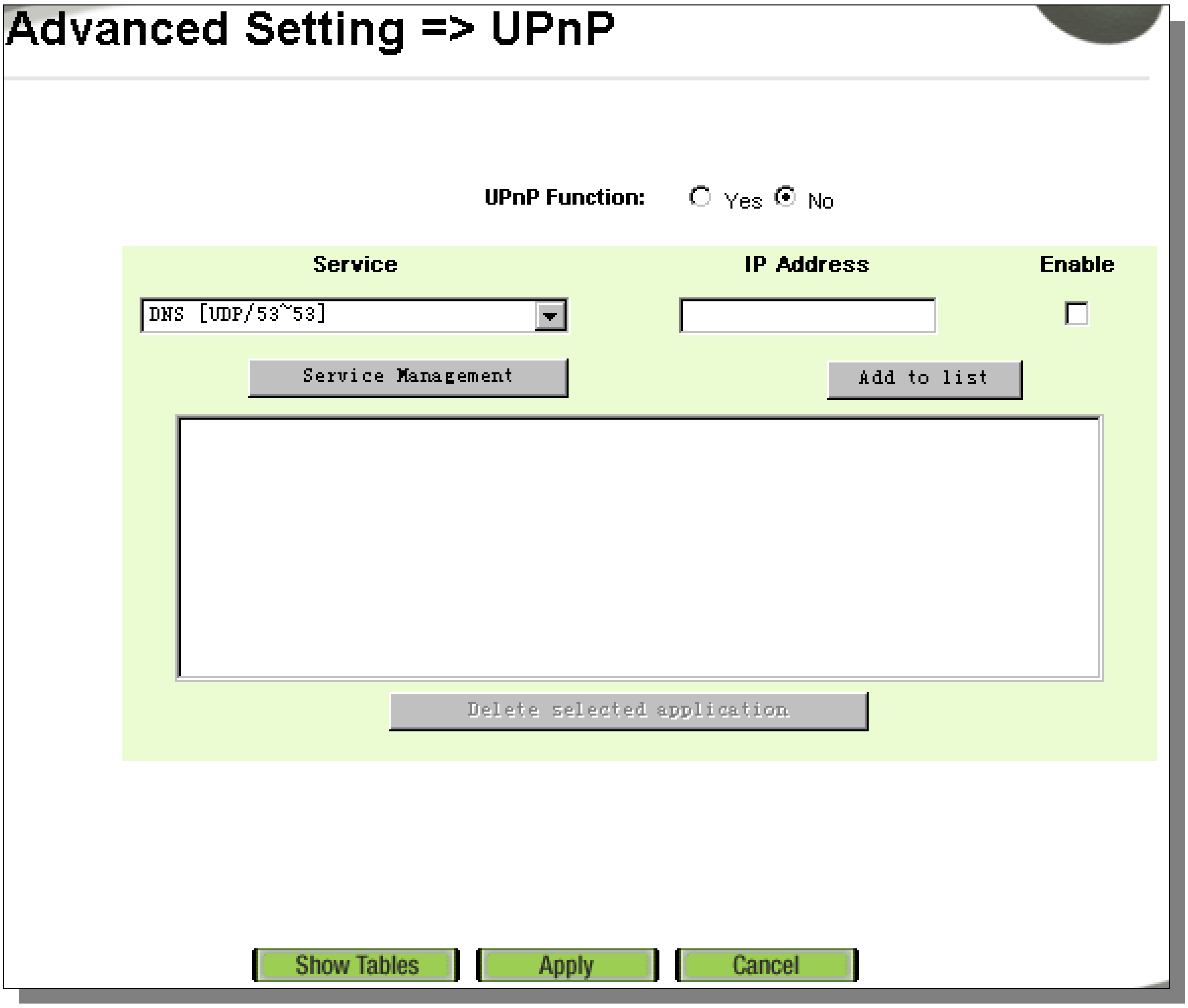
Show Tables : Show all the setting paratemters by pressing the button

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

4.3 UPnP- Universal Plug and Play

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

UPnP function includes UPnP Forwarding. If you would like to setup virtual servers in intranet, you could foolow the Forwarding setting in the previous chaptor, or confige the setting in UPnP Forwarding. However, please not not enter the setting repeatedly to avoid conflicts.



Advanced Setting => UPnP

UPnP Function: ○ Yes ● No

Service: DNS [UDP/53~53]

IP Address:

Enable: □

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

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

Enable： Activate this function.

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

Add to list： Add to active service content.

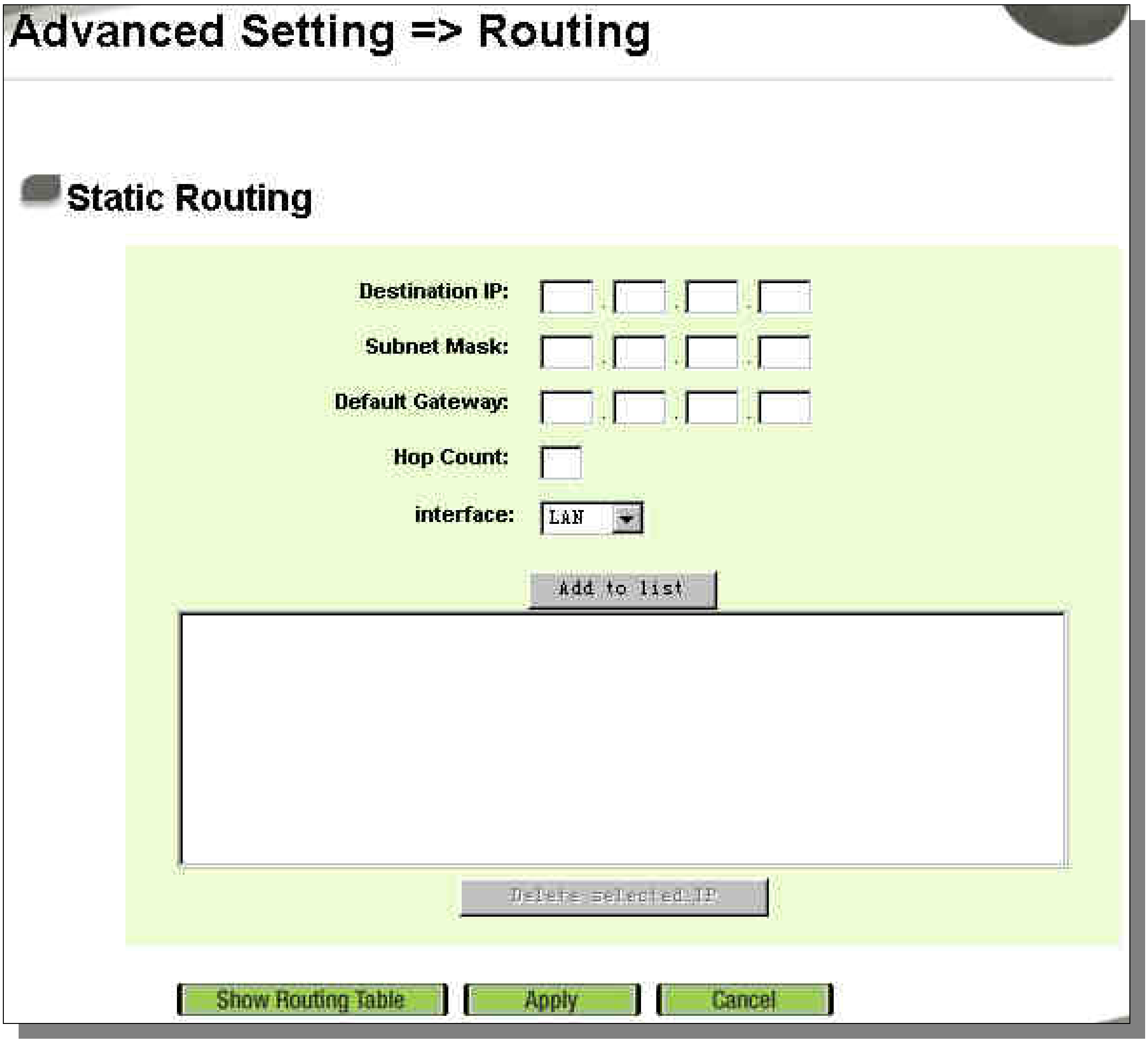
Delete selected application ： Remove selected services.

Show Tables： displays the list ofr current active UPnP functions.

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

4.4 Routing

Static routing enables the packet route by manual routing table. There is two applications: one is connecting different network or routers in intranet, and the other is identifying the route for specific destination IP address. For example, there might be different ISP lines for different WANs in one router. To avoid the connection issue such as mail servers or game servers are in different ISP lines and ISP can not connect eash other, mail servers or game servers should go with different WANs.



interface: LAN

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

Defarult 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 rule into the list.

Delete selected IP： Delete the selected IP in the list.

Show Rounting Table：	Display the current routing list.
Apply：	Save the parameter changes by pressing "Apply".
Cancel：	Clear the parameter changes by pressing "Cancel". Will be effective before pressing "Apply".

4.5 Ont To One NAT

If ISP provides several IP addresses, you can map the other available IPs with intranet computers. Except the device WAN and fiber switch or ATU-R (Gateway) have its own public IP each, these intranet computers have private IP in intranet, and after One- to One NAT mapping, these computer have public IPs when visiting Internet.

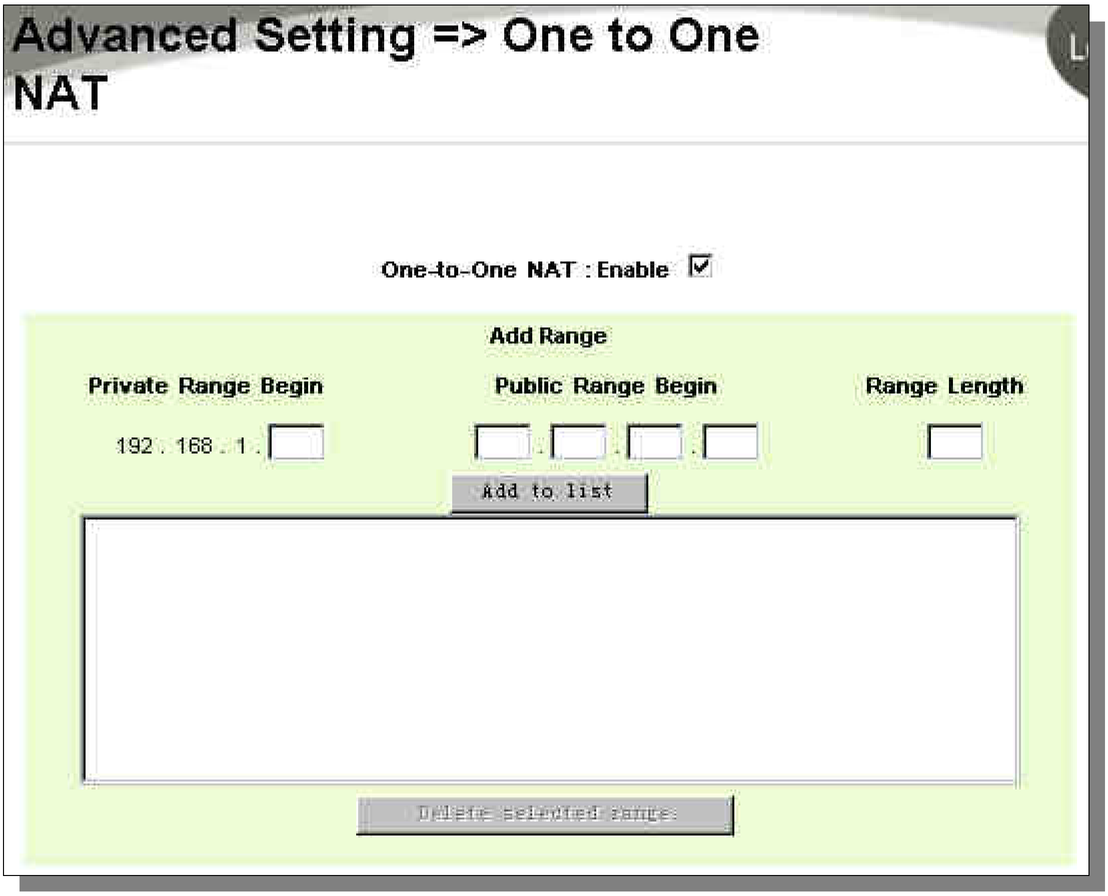
If there are more than two WEB servers in the intranet, you can use the function for mapping external IPs with internal server IPs.

Example： If you have 5 available IPs, which are 210.11.1.1~6, and 210.11.1.1 has been configured as WAN1. Users can respectively configure the other four real IPs for One to One NAT, 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.



Advanced Setting => One to One NAT

One-to-One NAT : Enable ☑

Add Range

Private Range Begin	Public Range Begin	Range Length
192 . 168 . 1 .	. . .	

One-to-One NAT Enable: Activate or close the One-to-One NAT function.

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

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

Range Lengeh: The numbers of final IPs of actual Internet IPs.

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

Delete selected range: Remove a selected One-to-One NAT list.

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

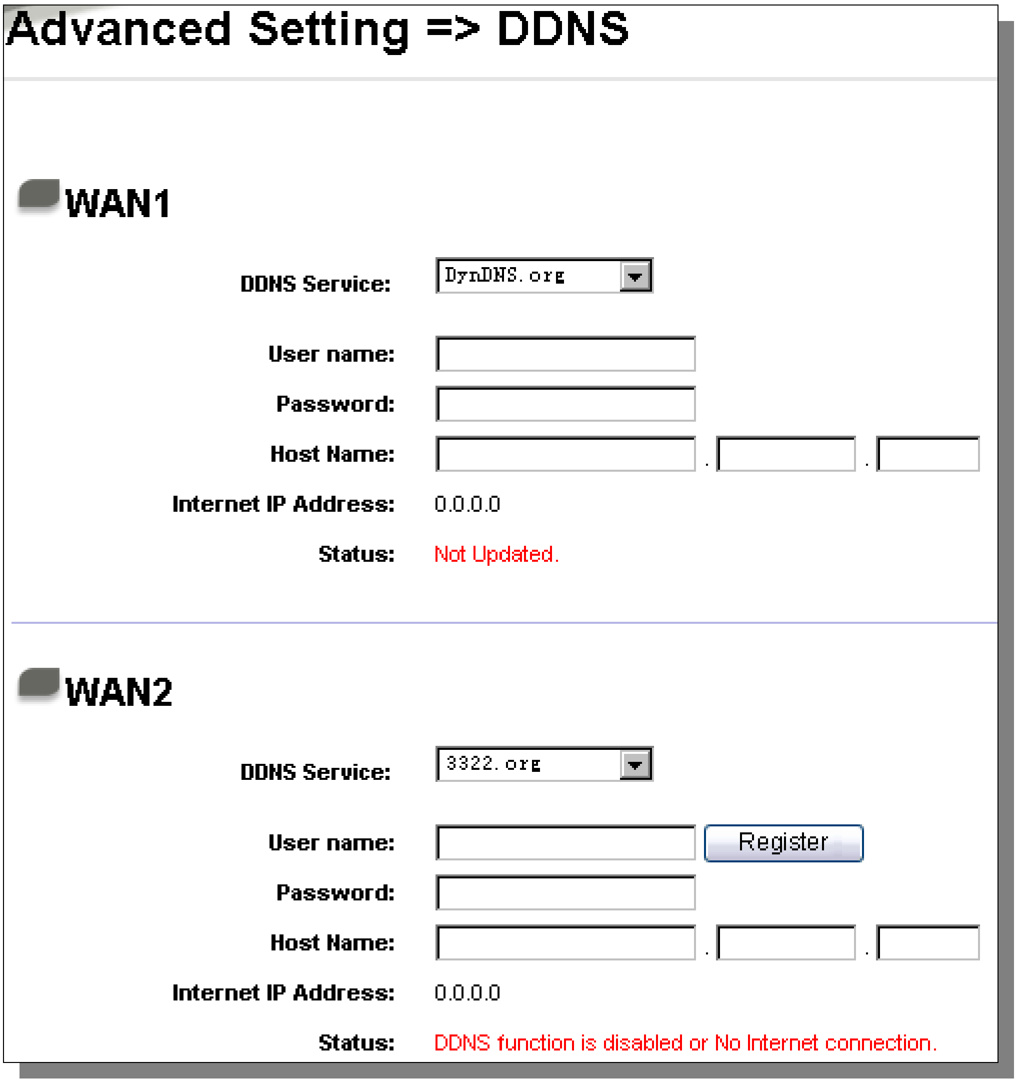
Attention！

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

4.6 DDNS

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

Also, to solve the unstable situation in DDnS server, each WAN will have dynamic IP update for DDNS services.



Advanced Setting => DDNS

WAN1

DDNS Service: DynDNS.org

User name:

Password:

Host Name: . .

Internet IP Address: 0.0.0.0

Status: Not Updated.

WAN2

DDNS Service: 3322.org

User name:

Password:

Host Name: . .

Internet IP Address: 0.0.0.0

Status: DDNS function is disabled or No Internet connection.

DDNS Service :	Check either of the boxes before DynDNS.org, 3322.org, and QnoDDNS.org.cn. (Can be applied at the same time)
User Name :	The name which is set up for DDNS. ●Input a complete website address such as abc.qnoddns.org.cn as a user name for QnoDDNS.
Password :	The password which is set up for DDNS.
Host Name :	Input the website address which has been applied from DDNS. Examples are abc.dyndns.org or xyz.3322.org.

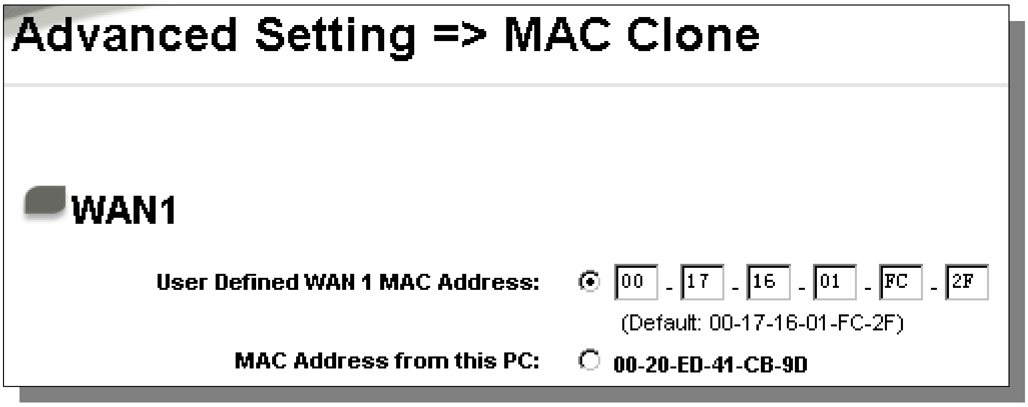
Internet IP Address： Input the actual dynamic IP address issued by the ISP.

Status： An indication of the status of the current IP function refreshed by DDNS.

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

4.7 MAC Clone

Some ISPs require a fixed MAC address (network card address) for ISP verification, which is mostly used in cable modem users. If required, input the network card address (MAC Address：00-xx-xx-xx-xx-xx) here, and the router will use this specific MAC address for verification. Please note: Only WAN1 can use this setting.



Advanced Setting => MAC Clone

WAN1

User Defined WAN 1 MAC Address: ● 00 - 17 - 16 - 01 - FC - 2F
(Default: 00-17-16-01-FC-2F)

MAC Address from this PC: ○ 00-20-ED-41-CB-9D

User Defined WAN 1 MAC Address： Users can enter the network card address manually. The default MAC is the WAN MAC.

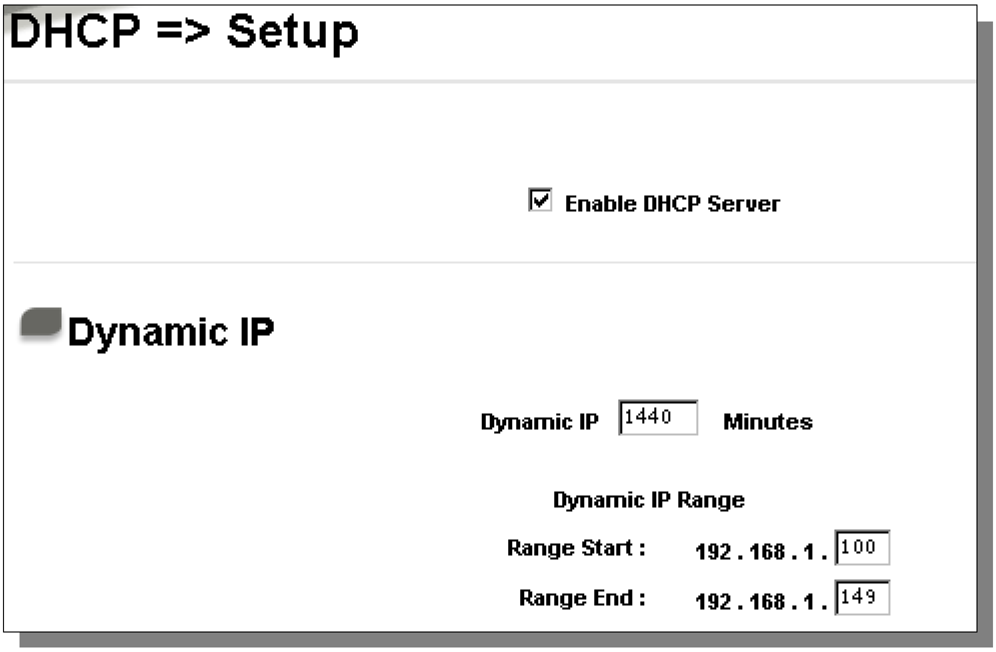
MAC Address from this PC： Current address of MAC that is connected with this PC.

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

4.8 DHCP

The device have one DHCP server with Class C IPs. The default is Enabled. Computers can get IPs automatically.

4.8.1 DHCP Setup



DHCP => Setup

☑ Enable DHCP Server

Dynamic IP

Dynamic IP 1440 Minutes

Dynamic IP Range

Range Start : 192 . 168 . 1 . 100

Range End : 192 . 168 . 1 . 149

Dynamic IP ___Minutes : This setting is the lease time for the IP address. The default is 1,440 minutes, which is one day. When the lease time arrives, PC will ask for IP again. Users can also setup the time based on requirement.

Range Start : The default initial IP is 192.168.1.100. Users can change the IP based on requirements.

Range End : The default final IP is 192.168.1.149. That is, there are total 50 IPs from the default. Users can change the setting with the actual requirement.

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

4.8.2 IP & MAC Binding

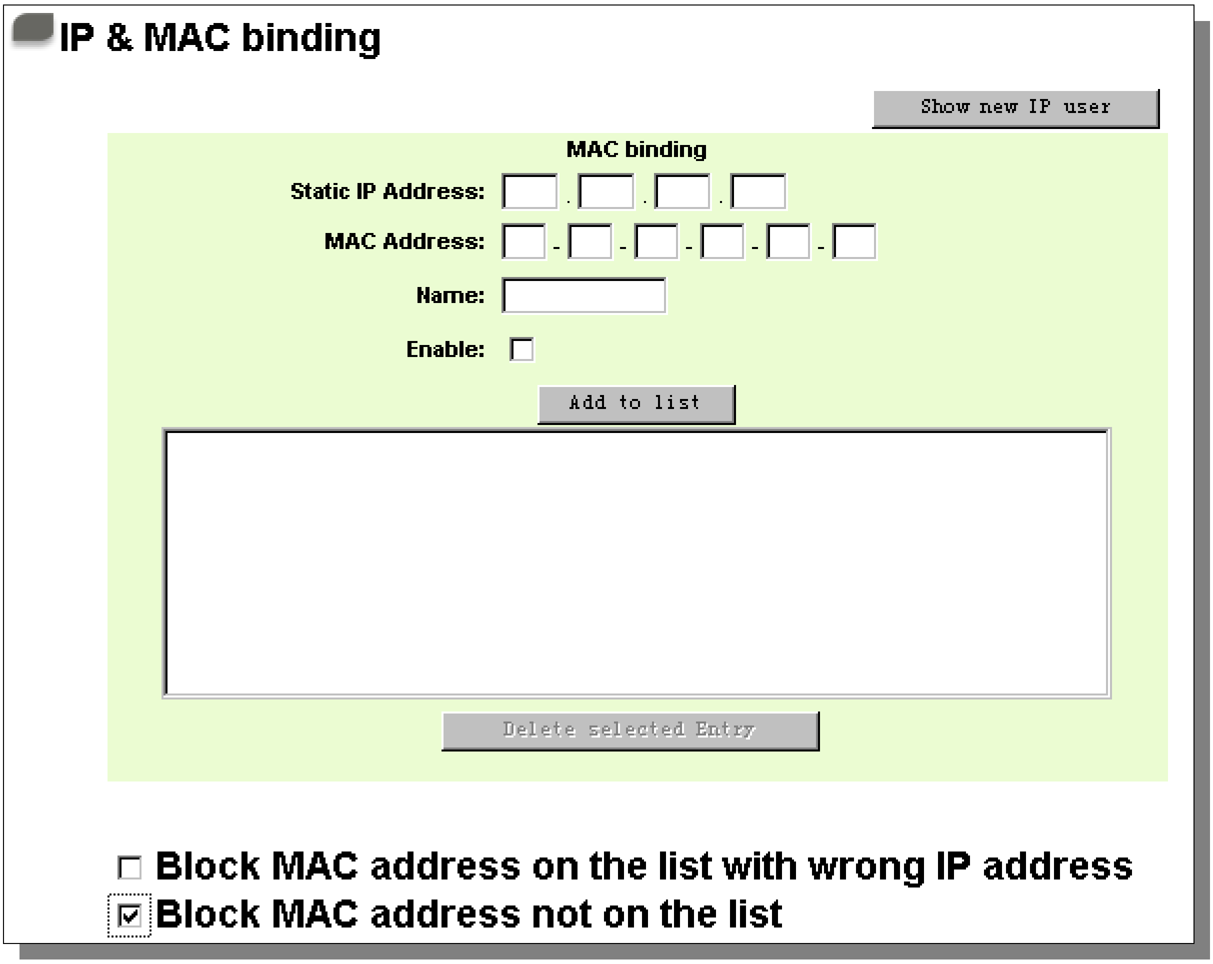
In many enterprise and community networks, administrator can setup the IP & MAC binding feature to ensure that users can not add additional computer or change IPs. Through this feature, computers will have the same IP addresses every time.

User have two options for the setting：

Block MAC address not on the list

The main purpose for this feature is that only the computers which MAC addresses are on the list have the access to Internet. Computers which MAC addresses are not shown can not get IPs.

When the feature is enabled, please fill out the IP column in 0.0.0.0, as well as enable Block MAC address, as shown in the following fig.

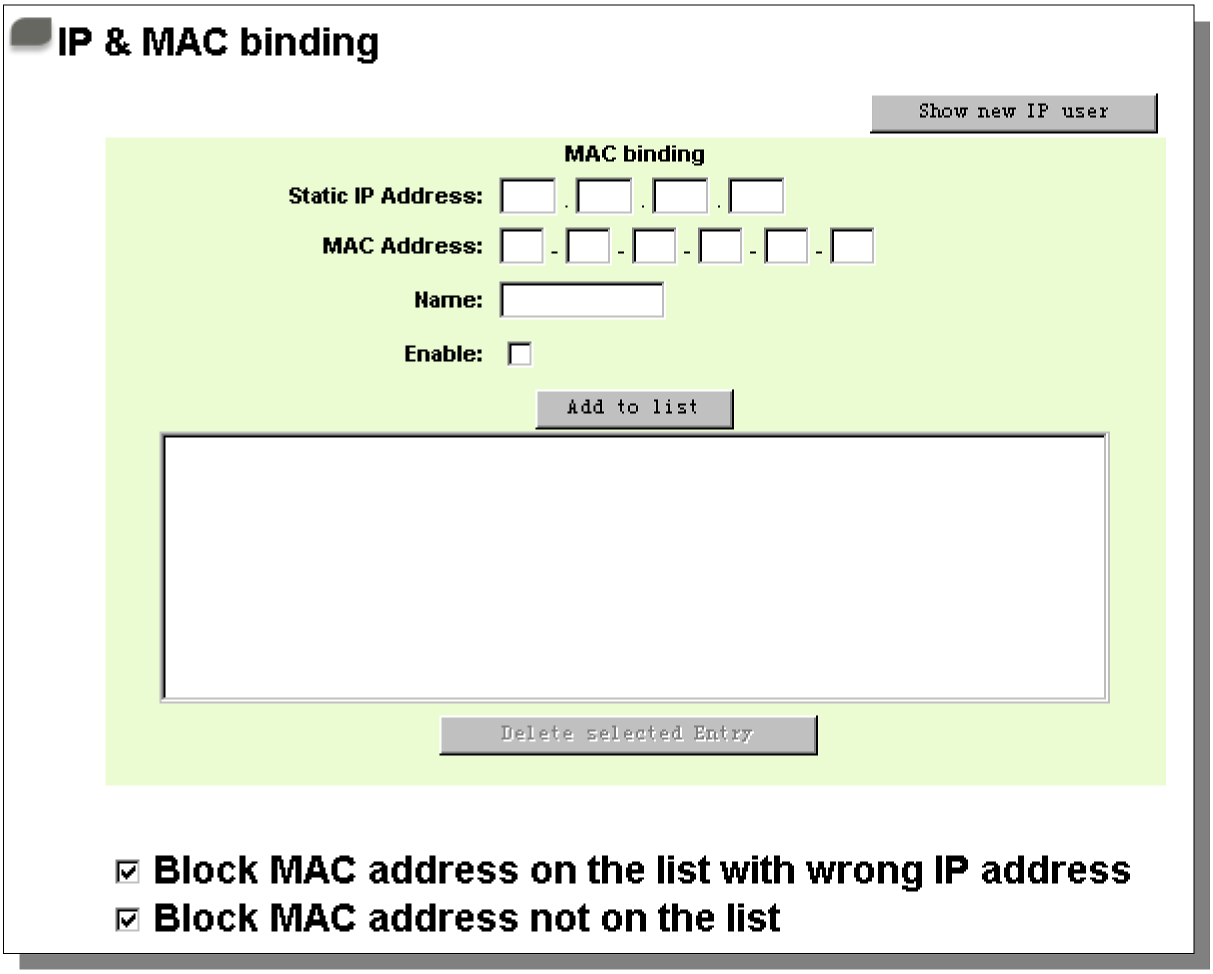


□ Block MAC address on the list with wrong IP address

☑ Block MAC address not on the list

IP & MAC Binding

The main purpose for this feature is that the computer with the assigned MAC will alwayshave the same IP. Also, if Block MAC address on the list with wrong IP address is enabled, the computer with assigned IP won't have access to Internet.



IP & MAC binding

Static IP Address: . . .

MAC Address: - - - - -

Name:

Enable: □

☑ Block MAC address on the list with wrong IP address

☑ Block MAC address not on the list

Static IP Address： There are two ways to input static IP:

1. If users want to set up a MAC address to acquire IP from DHCP, but the IP need not be a static IP, input 0.0.0.0 in the boxes. The boxes cannot be left empty.

2. If users want DHCP to assign a static IP for a PC every single time, users should input the IP address users want to assign to this computer in the boxes. The server or PC which is to be bound will then acquire a static virtual IP whenever it restarts.

MAC Address: Input the static real MAC (the address on the network card) for the server or PC.

Name: Input the name or address of the client for identification. The maximum acceptable characters are 12. Either

Chinese or English can be accepted.

Enable: Activate this configuration

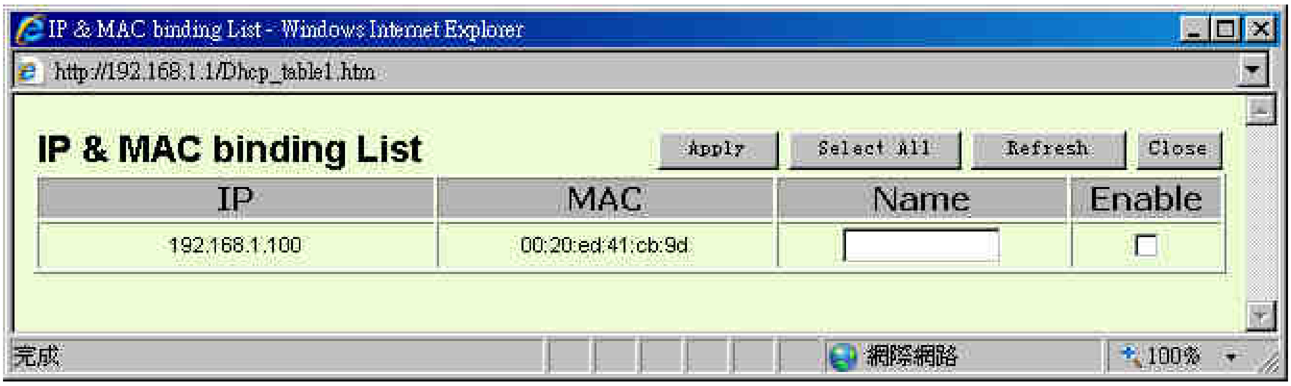
Block MAC address on the list with wrong IP address: When this option is activated, MAC addresses which are not included in the list will not be able to connect with the Internet.

Block MAC address not on the list: When this option is checked, user-modified IP or IP which is not configured in the list will not be able to connect with the Internet.

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

Show New IP User：

The main purpose for this feature is to reduce the effort for network administrators. It is time- consuming to check every computer MAC address and bind the IP and MAC address. Moreover, manual MAC address keyin also causes errors. By looking up the table, administrators can see all the MAC addresses which are not binded, and apply the binding directly on the table. In addition, if administrators find that the same MAC address which is already binded is shown on the list, it represents that the user is trying to change the IP for Internet access.



IP & MAC binding List - Windows Internet Explorer

http://192.168.1.1/Dhcp_table1.htm

IP & MAC binding List

IP	MAC	Name	Enable
192.168.1.100	00:20:ed:41:cb:9d		□

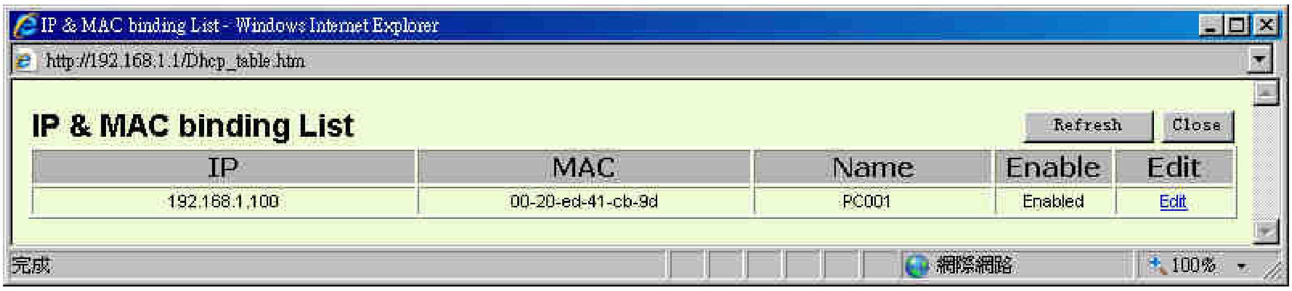
Name: Input the name or address of the client for identification. The maximum acceptable characters are 12.

Enable： Activate this configuration

Apply:	Bind the chosen IP into the binding list
Select All：	All the IP shown on the list will be binded
Refresh：	Update the list
Close:	Close the list

Show Tables

The list will show all the IP/MAC binding and cureent status. Users can click “Edit” for revision.


IP & MAC binding List - Windows Internet Explorer
http://192.168.1.1/Dhcp_table.htm
Refresh
Close
完成
網際網路
100%

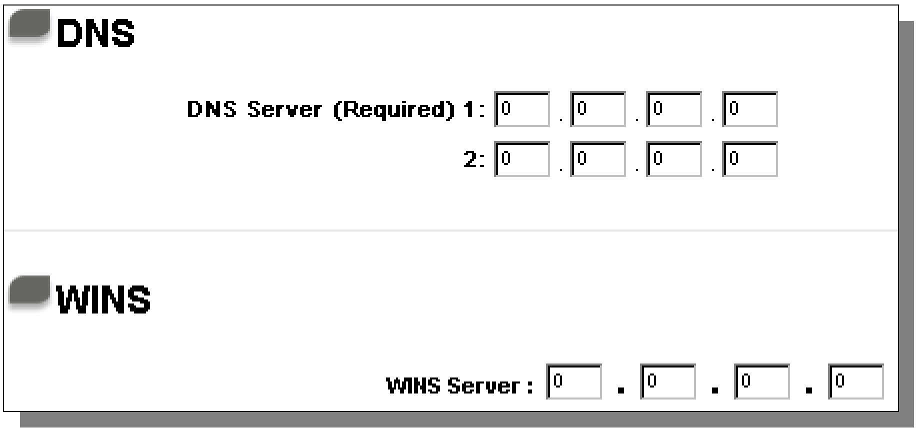
IP & MAC binding List

IP	MAC	Name	Enable	Edit
192.168.1.100	00-20-ed-41-cb-9d	PC001	Enabled	Edit

4.8.3 DNS & WINS Server Setting

DNS Server IP：

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

DNS Server (Required) 1: 0 . 0 . 0 . 0

2: 0 . 0 . 0 . 0

WINS

WINS Server : 0 . 0 . 0 . 0

DNS Server 1 : Input the IP address of the DNS server. The default is "0".

DNS Server 2 : Input the IP address of the DNS server. The default is "0".

WINS Server :

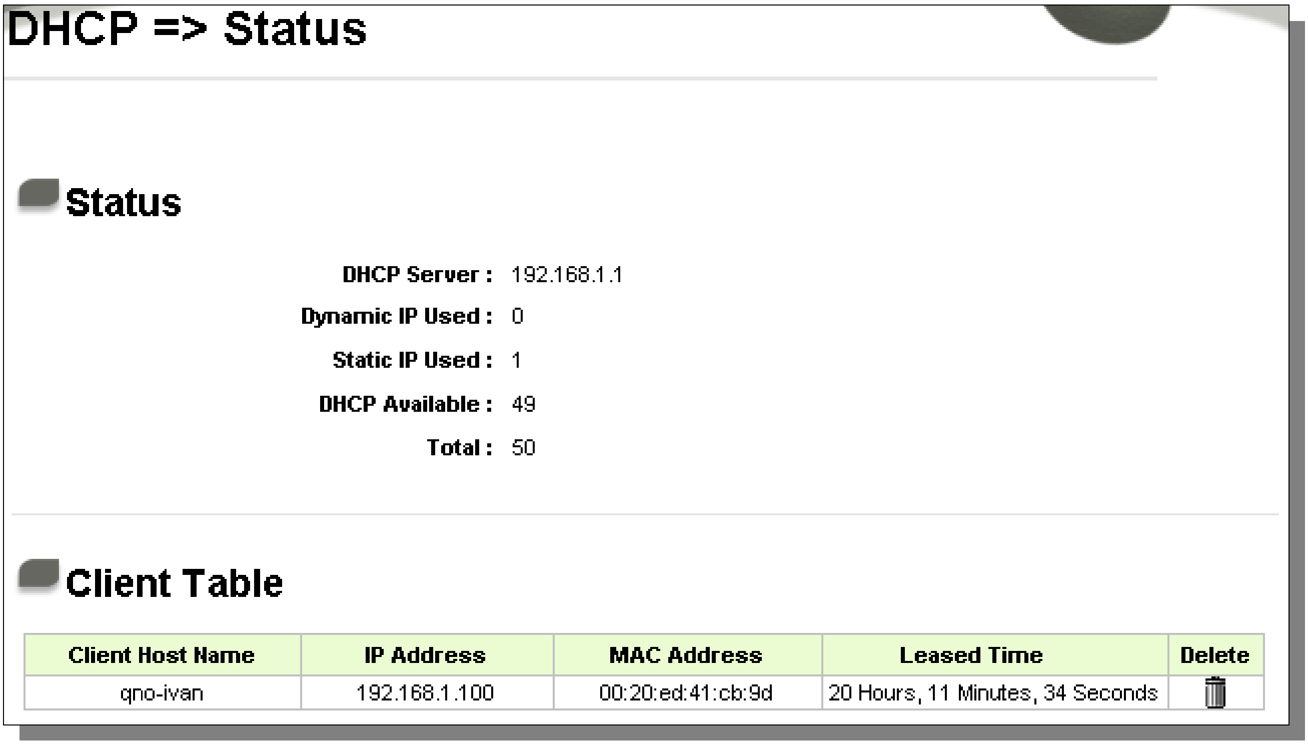
If there is a WIN server in the network, users can input the IP address of that server directly.

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

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

4.8.4 DHCP Status

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



DHCP => Status

Status

DHCP Server : 192.168.1.1
Dynamic IP Used : 0
Static IP Used : 1
DHCP Available : 49
Total : 50

Client Table

Client Host Name	IP Address	MAC Address	Leased Time	Delete
qno-ivan	192.168.1.100	00:20:ed:41:cb:9d	20 Hours, 11 Minutes, 34 Seconds	🗑

DHCP Server: DHCP IP address

Dynamic IP Used： The amount of dynamic IP leased by DHCP.

Static IP Used: The amount of static IP assigned by DHCP.

DHCP Available: The amount of IP still available in the DHCP server.

Total: The total IP which the DHCP server is configured to lease.

Client-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.

Leased Time: The lease time of the IP released by DHCP.

Delete: Remove a record of an IP lease.

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

5、Tool Setting

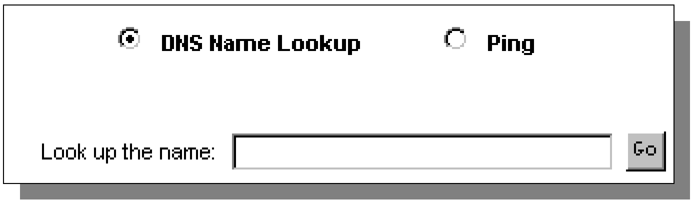
This chapter introduces tools for managing the router and testing network connection.

5.1 Diagnostic

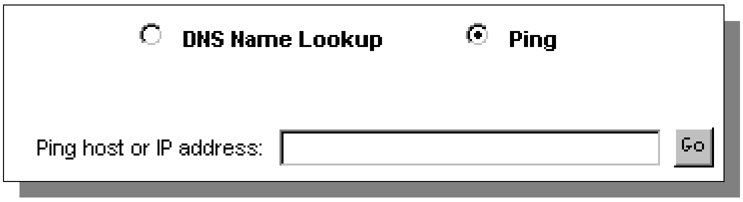
The device provides a simple online network diagnostic tool to help users troubleshoot network-related problems. This tool includes **DNS Name Lookup** (Domain Name Inquiry Test) and **Ping (Packet Delivery/Reception Test)**.

DNS Name Lookup

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



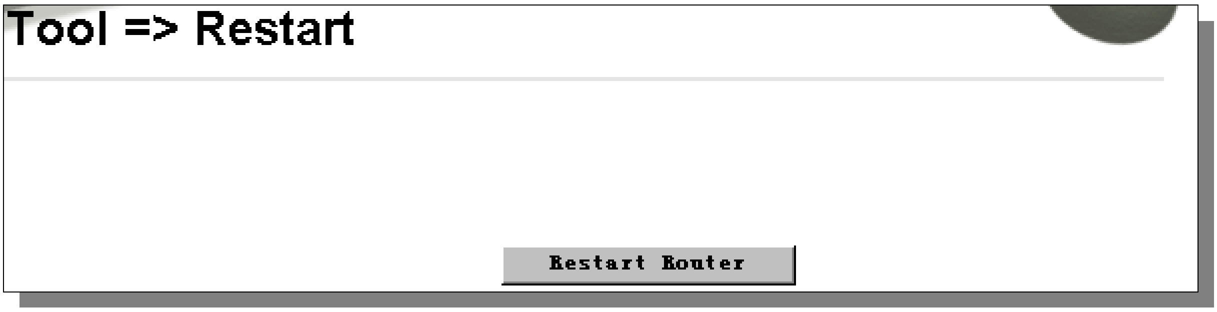
Ping - Packet Delivery/Reception Test



This item informs users of the status quo of the outbound session and allows the user to know the existence of computers online. On this test screen, please enter the host IP that users want to test such as 192.168.5.20. Press "Go" to start the test. The result will be displayed on this screen.

5.2 Restart

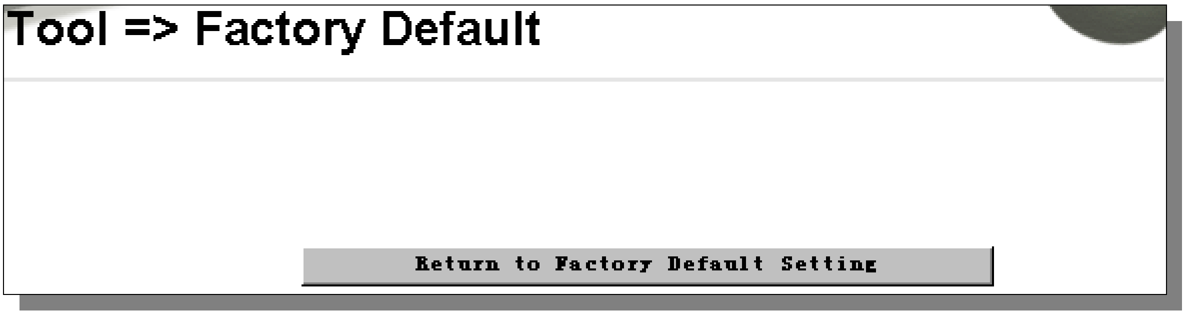
Click "**Restart Router**" to start it again. This operation message will then be recorded in system log. Press "**Reset**" on the device panel to reset manually. **Press Reset and hold for 5 seconds** and the device will restart after the yellow light flickers 5 times.



Tool => Restart

5.3 Factory Default

Select “**Return to Factory Default Setting**” to reset all the settings and restart the device. We recommend that users should back up the current configuration first before returning to default. After the firmware upgrade, users can return to factory default to make sure the stability. Then, import the backup configuration to the device. Please refer to ‘Setting Backup” for exporting and importing device configuration.



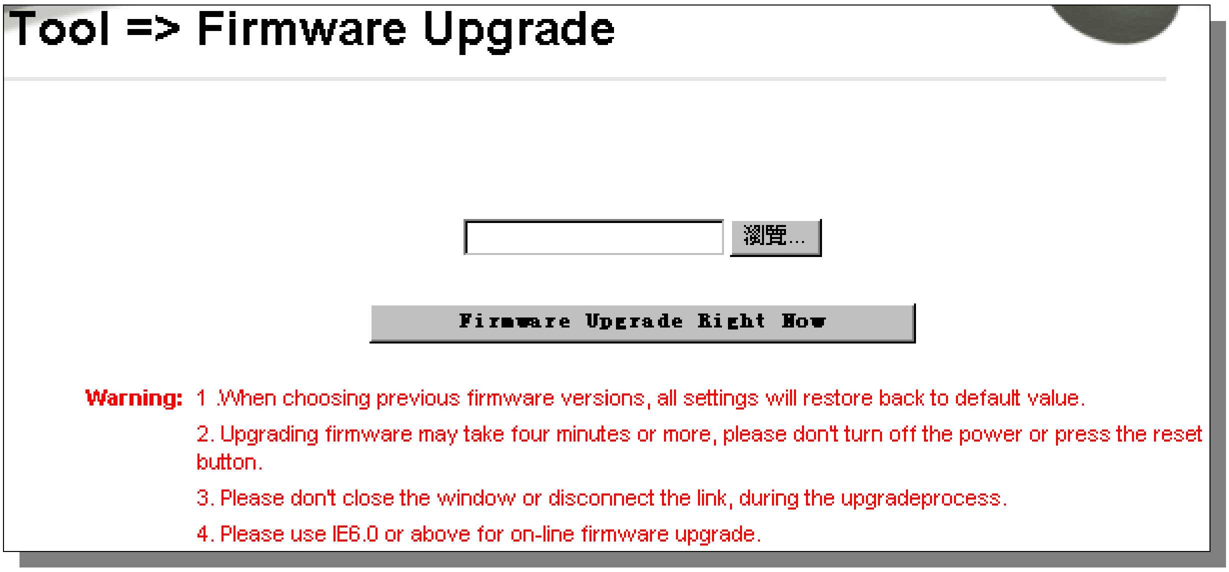
Tool => Factory Default

5.4 Firmware Upgrade

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

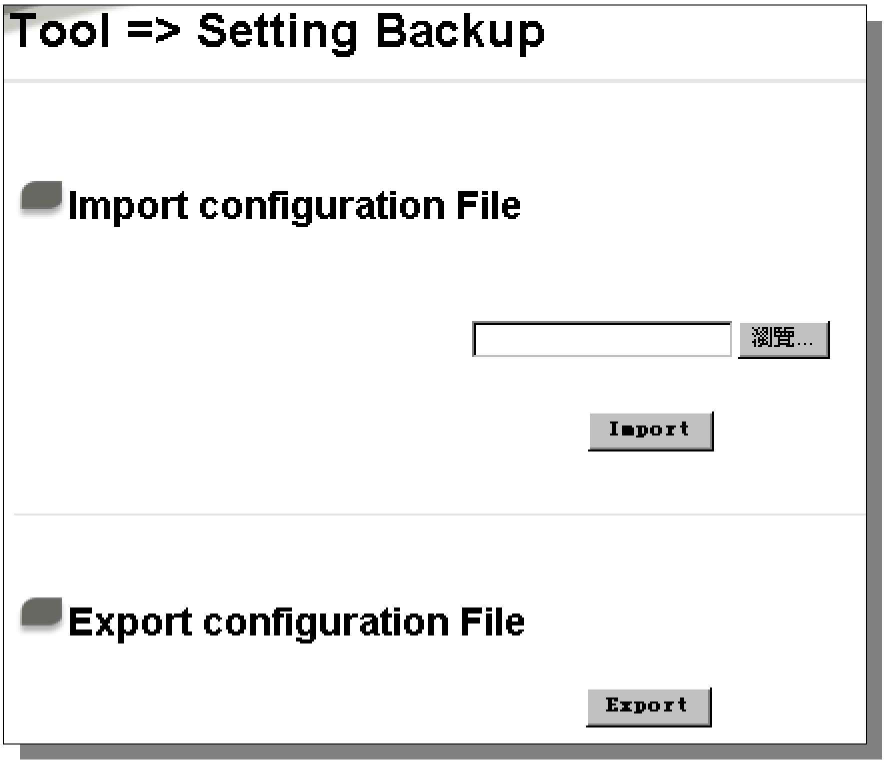
Attention！

Before firmware upgrade, please read the notes in the screen carefully. During the firmware upgrade, please do not exit the upgrade screen, or it might cause router upgrade failure.


Tool => Firmware Upgrade

Warning: 1 .When choosing previous firmware versions, all settings will restore back to default value.
2. Upgrading firmware may take four minutes or more, 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 upgradeprocess.
4. Please use IE6.0 or above for on-line firmware upgrade.

5.5 Setting Backup



Tool => Setting Backup

Import configuration File

Export configuration File

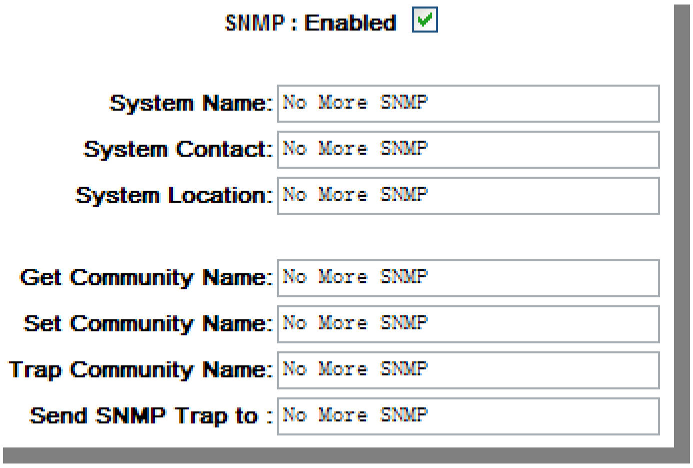
Import configuration File：

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

Export configuration File：

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

5.6 SNMP



SNMP : Enabled ☑

System Name: No More SNMP

System Contact: No More SNMP

System Location: No More SNMP

Get Community Name: No More SNMP

Set Community Name: No More SNMP

Trap Community Name: No More SNMP

Send SNMP Trap to : No More SNMP

Enabled : Activate SNMP feature. The default is activated.

System Name : Set the name of the device such as QVM1000.

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

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

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

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

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

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

Apply : Press **"Apply"** to save the settings.

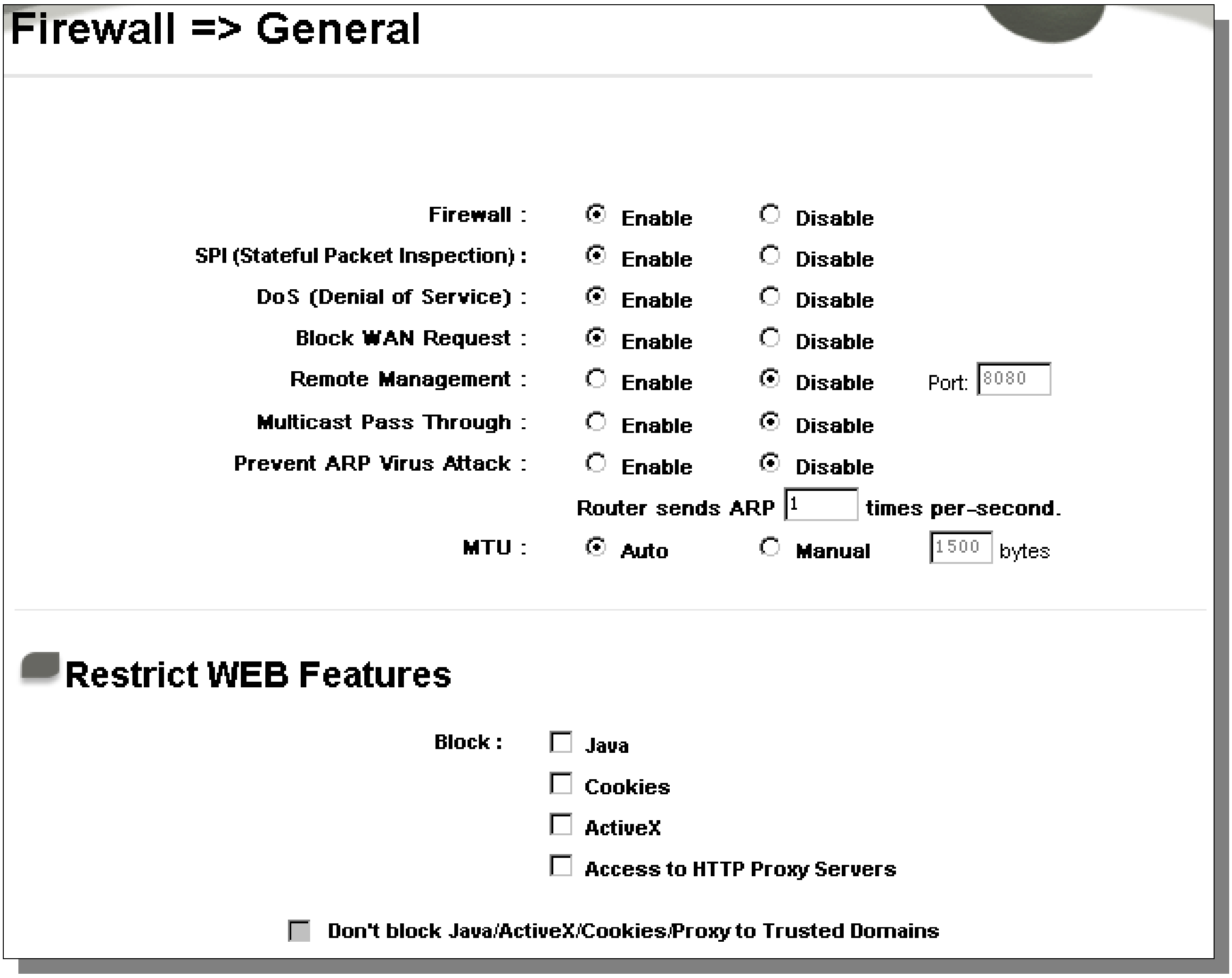
Cancel : Press **"Cancel"** to keep the settings unchanged.

6、Firewall

This chaptor introduces firewall setting uptions, as well as network control settings.

6.1 Firewall General Setting

From Firewall => General, users can enable or disable the functions.   Default is Firewall enabled, and disable other unnecessary responses.



Firewall => General

Firewall : ● Enable ○ Disable

SPI (Stateful Packet Inspection) : ● Enable ○ Disable

DoS (Denial of Service) : ● Enable ○ Disable

Block WAN Request : ● Enable ○ Disable

Remote Management : ○ Enable ● Disable Port: 8080

Multicast Pass Through : ○ Enable ● Disable

Prevent ARP Virus Attack : ○ Enable ● Disable

Router sends ARP 1 times per-second.

MTU : ● Auto ○ Manual 1500 bytes

Restrict WEB Features

Block : □ Java
□ Cookies
□ ActiveX
□ Access to HTTP Proxy Servers

□ Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains

Firewall：	Enable or disable the function.
SPI (Stateful Packet Inspection):	This enables the packet to actively detect the authentication technology. The Firewall operates mainly on a network level. By executing the dynamic

authentication of each connection, the program will perform an alarming function. Meanwhile, firewalls of the packet authentication type may decline the connection to non-standard communications protocol.

DoS (Denial of Service): This averts DoS attacks such as SYN Flooding, Smurf, LAND, Ping of Death, and IP Spoofing.

Block WAN Request: If set as **Enabled**, then device will shut down outbound ICMP to connect to machines with abnormal packet responses. If you try to ping the device 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. 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.

MTU: MTU is an acronym for Maximum Transmission Unit. The default value is 1500.But in different network environments, different values can be applied. ADSL PPPoE is the most common condition. (ADSL PPPoE MTU Size: 1492). Generally, the default value of Auto is good enough and further settings are not necessary.

Restrict WEB Features： It supports the block that is connected through: Java, Cookies, Active X, and HTTP Proxy access.

Don't block Java/ActiveX/Cookies/Proxy to Trusted Domains:	If this option is activated, users can add trusted network or IP address into the trust domain, and it will not block items such as Java/ActiveX/Cookies contained in the web pages from the trust domains.

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

6.2 Access Rule

The device has a user-friendly network access regulatory tool. Administratorrs may define network access rules for different users and conditions. 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.

They can select to enable/ disable the network so as to protect all internet access.

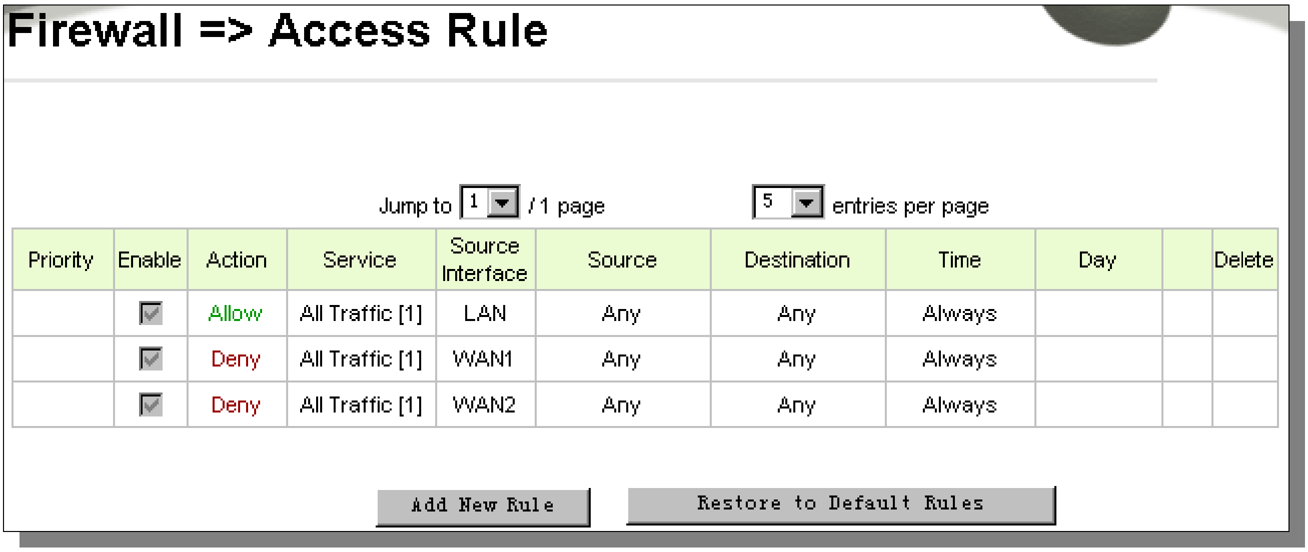
The following describes the internet access rules

- 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)



Firewall => Access Rule

Jump to 1 / 1 page   5 entries per page

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

In addition to the default rules, all the network access rules will be displayed as illustrated above. Users may follow or self- define the priority of each network access rule.

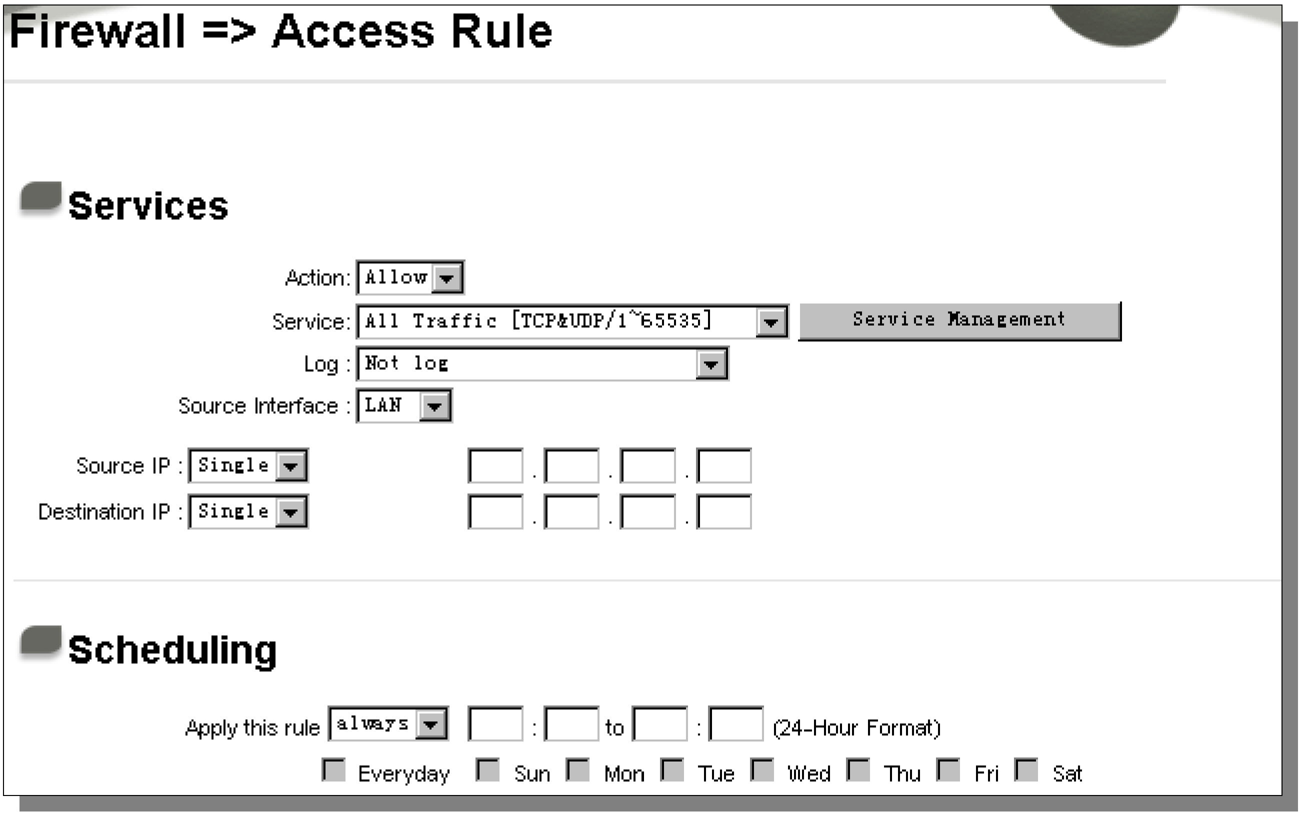
Edit : define the network access rule item

Trash Can Icon : remove the item

Add New Rule : create a new network access rule

Restore to Default Rules : restore all settings to the default values and delete all the self-defined settings.

Add New Access Rules



Firewall => Access Rule

Services

Action: Allow

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

Log : Not log

Source Interface : LAN

Source IP : Single . . .

Destination IP : Single . . .

Scheduling

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

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

Action: This allows setting the rule under control.

Allow：Permits the pass of packets compliant with this control rule

Deny：Prevents the pass of packets not compliant with this control rule

Service: From the drop-down menu, select the service that users grant or do not give permission.

Service Management: If the service that users wish to manage does not exist in the drop-down menu, press Service Management to add the new service.

From the pop-up window, enter a service name and communications protocol and port, and then click the "Add to list" button to add the new service.

Source Interface: Select the source port whether users are permitted or not (for example: LAN, WAN1, WAN2, WAN3 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.

Destination: 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 **"___to__",** and the operation will run according to the defined time

Apply this rule: Shows the rules is activated for 24 hours.(Default)

Users might also choose time and day control

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

Day Control: "**Everyday**" means this period of time will be under control everyday. If users only certain days of a week should be under control, users may select the desired days directly.

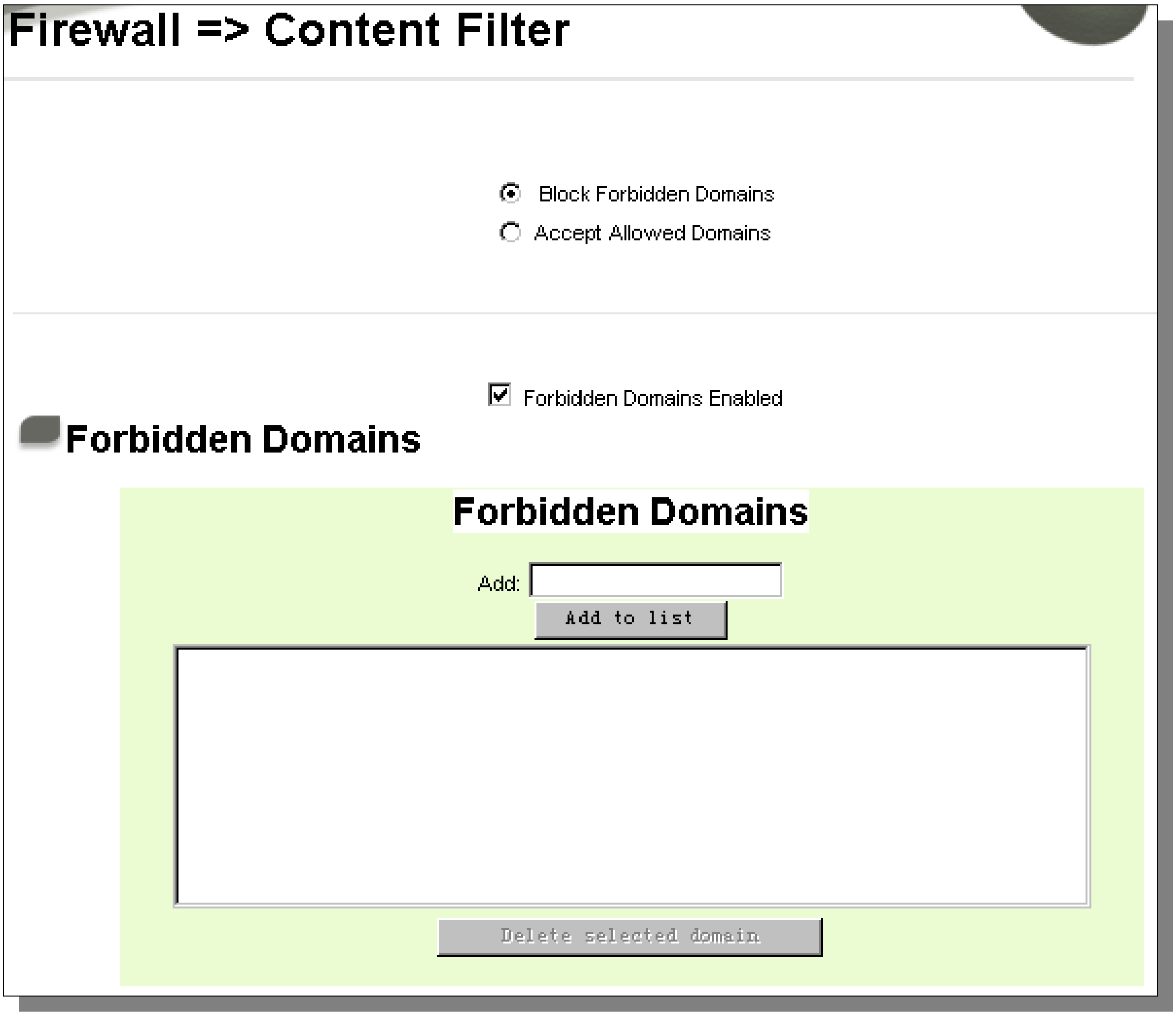
After modification, press **"Apply"** to save the network settings or press **"Cancel"** to keep the settings unchanged.

6.3 Content Filter

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

Block Forbidden Domains

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



Firewall => Content Filter

● Block Forbidden Domains
○ Accept Allowed Domains

☑ Forbidden Domains Enabled

Forbidden Domains

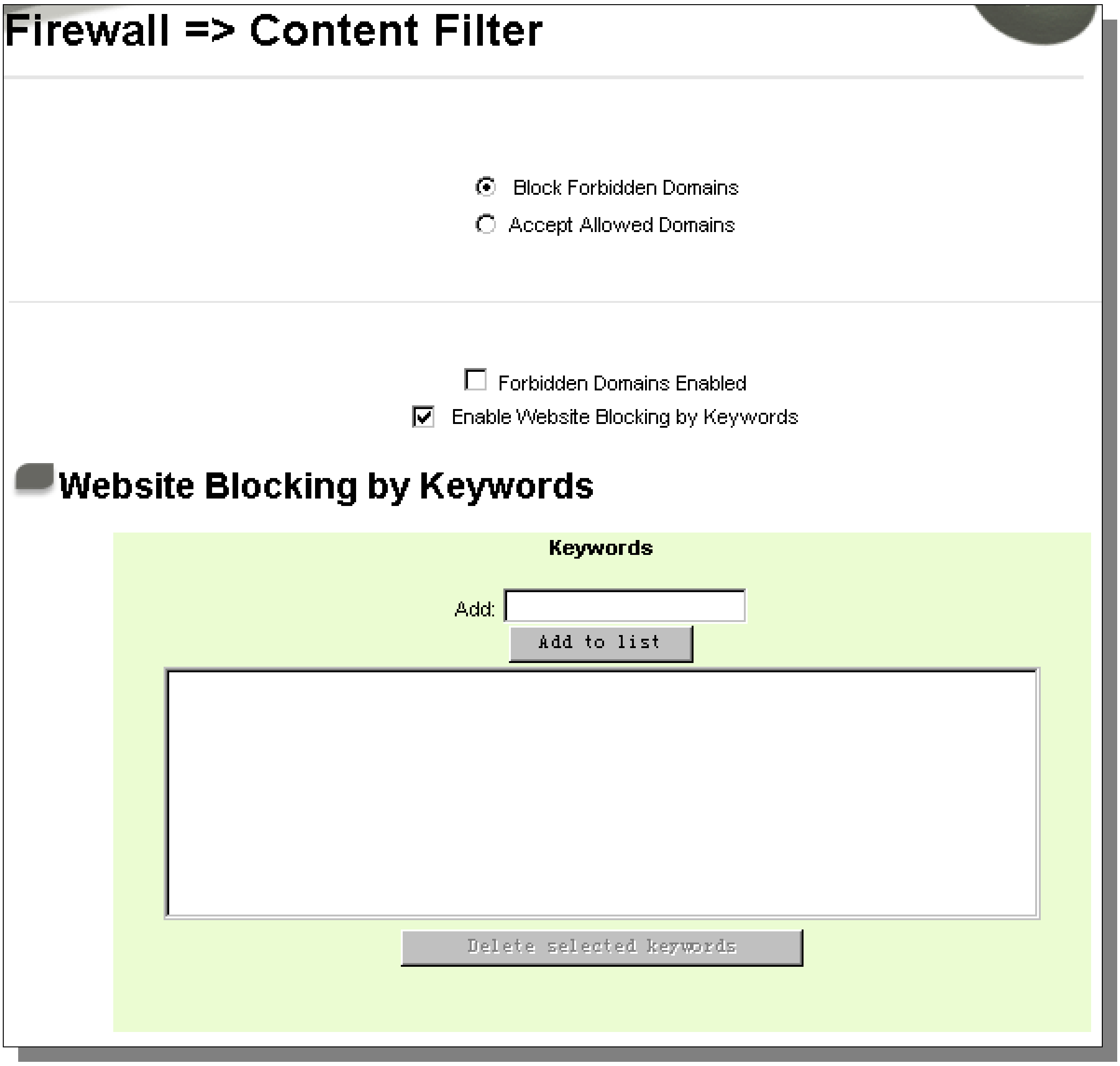
Forbidden Domains

Add:

Forbidden Domain Enabled:	Click to enable this feature. The default setting is Disabled.
Forbidden Domains:	Content filter list
Add:	Enter the websites to be controlled such as www.playboy.com

Website blocking by keyword：

If users enter the string ”sex”, any websites containing ”sex” will be blocked.



Firewall => Content Filter

● Block Forbidden Domains
○ Accept Allowed Domains

□ Forbidden Domains Enabled
☑ Enable Website Blocking by Keywords

Website Blocking by Keywords

Keywords

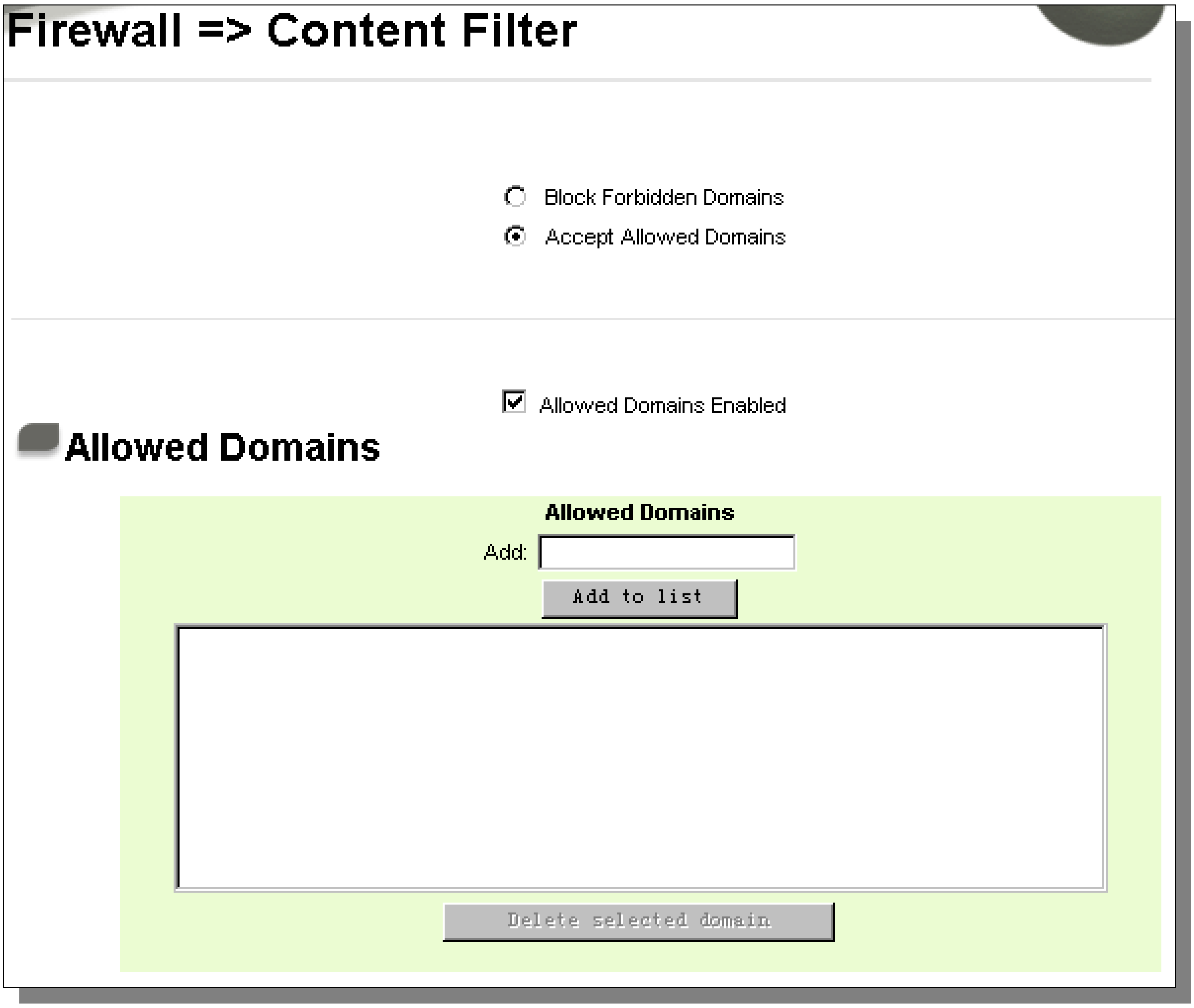
Add:

Enable Website Blocking by Keywords: Click to activate this feature. The default setting is disabled.

Add: Enter the keywords.

Accept Allowed Domains

The purpose for this feature is to set websites allowed to be visited. In some companies or schools, only some specific websites are allowed for employees or students.



Firewall => Content Filter

○ Block Forbidden Domains
● Accept Allowed Domains

☑ Allowed Domains Enabled

Allowed Domains

Allowed Domains

Add:

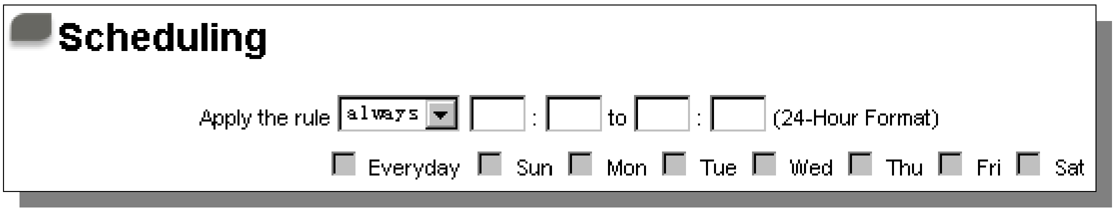
Allowed Domains Enabled : Click to activate this feature. The default setting is disabled.

Add: Enter the websites to be controlled such as www.playboy.com

Scheduling

Select **"Always"** to apply the rule on a round-the-clock basis. Select **"from",** and the operation will run according to the defined time. For example, if the control time runs from

8 a.m. to 6 p.m., Monday to Friday, users may control the operation according to the following illustrated example.



Scheduling

Apply the rule always ▾ [ ] : [ ] to [ ] : [ ] (24-Hour Format)

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

Always: Shows the rules is activated for 24 hours.

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

Day Control: ”**Everyday**” means this period of time will be under control everyday. If users only certain days of a week should be under control, users may select the desired days directly.

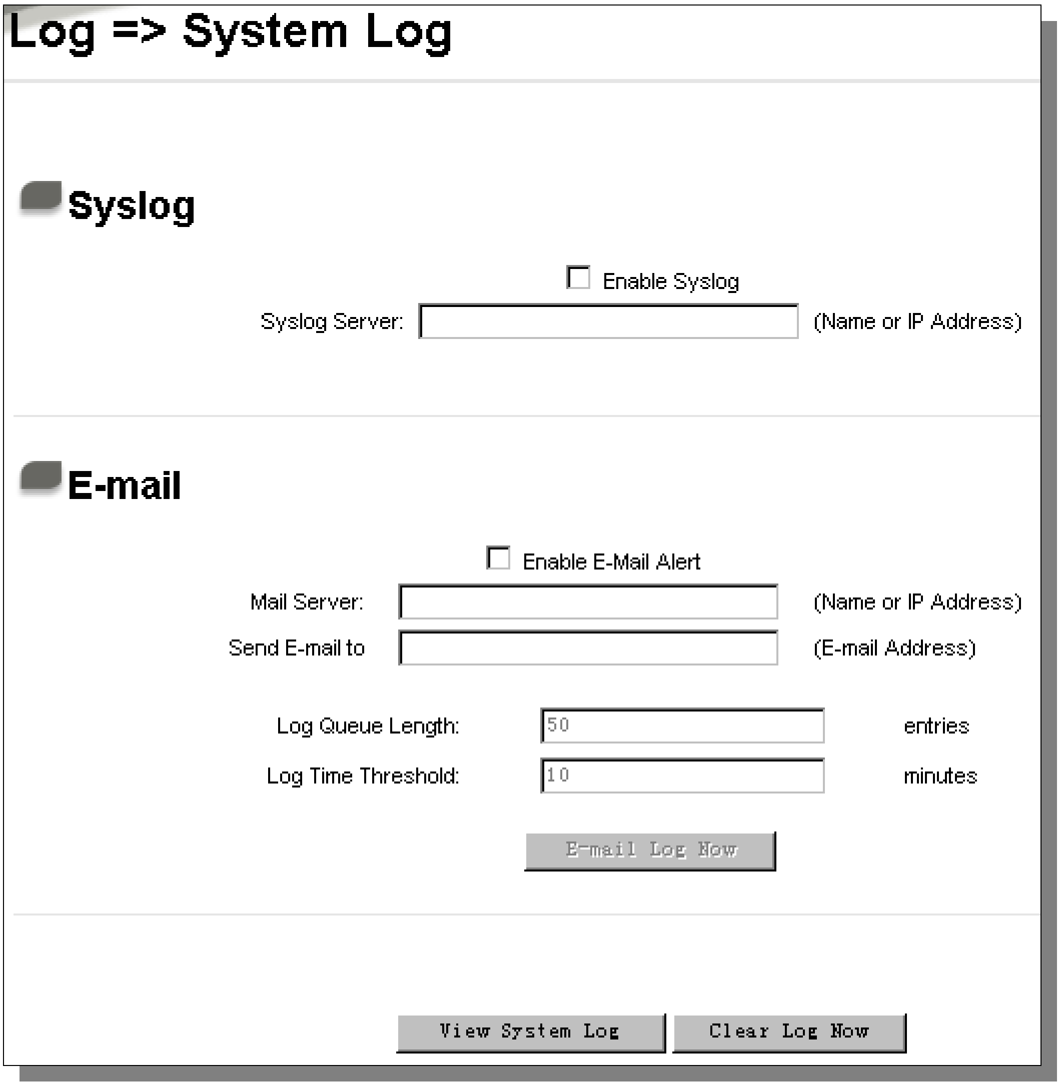
After modification, push **“Apply”** button to save the network setting or push **“Cancel”** to keep the settings unchanged.

7、Log

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

7.1 System Log

System Log offers two options: system log and E-mail alert.



Log => System Log

Syslog

☐ Enable Syslog

Syslog Server: (Name or IP Address)

E-mail

☐ Enable E-Mail Alert

Mail Server: (Name or IP Address)

Send E-mail to (E-mail Address)

Log Queue Length: 50 entries

Log Time Threshold: 10 minutes

Syslog

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

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

E-mail Alert

Enable E-Mail Alert: If this option is selected, E-mail Warning will be enabled.

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

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

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

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

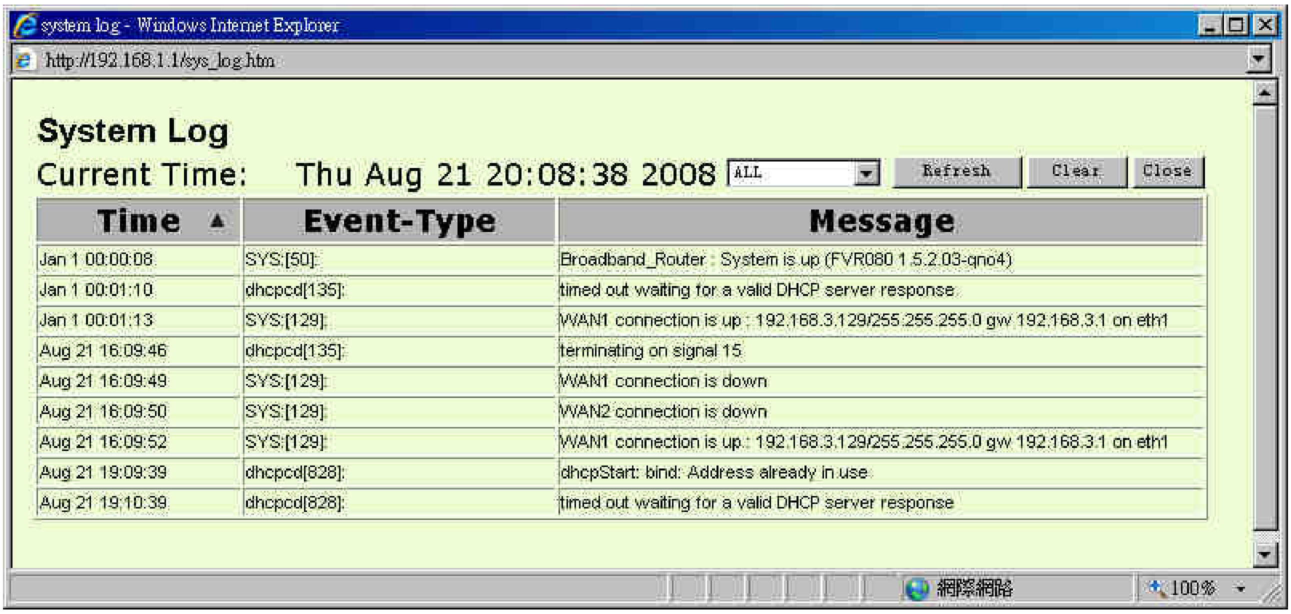
The device will detect which parameter (either entries or intervals) reaches the threshold first and send the log message of that parameter to the user.

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

Below is two button for log inqury:

View System Log：

This option allows users to view system log. The message content can be read online via the device. They include **All, System,** and **Firewall Log**. Click “Refresh” button for updating new logs, and Click : Clear” button for clearing all log messages, which is illustrated as below.


system log - Windows Internet Explorer
http://192.168.1.1/sys_log.htm
ALL
Refresh
Clear
Close
網際網路
100%

System Log

Current Time: Thu Aug 21 20:08:38 2008

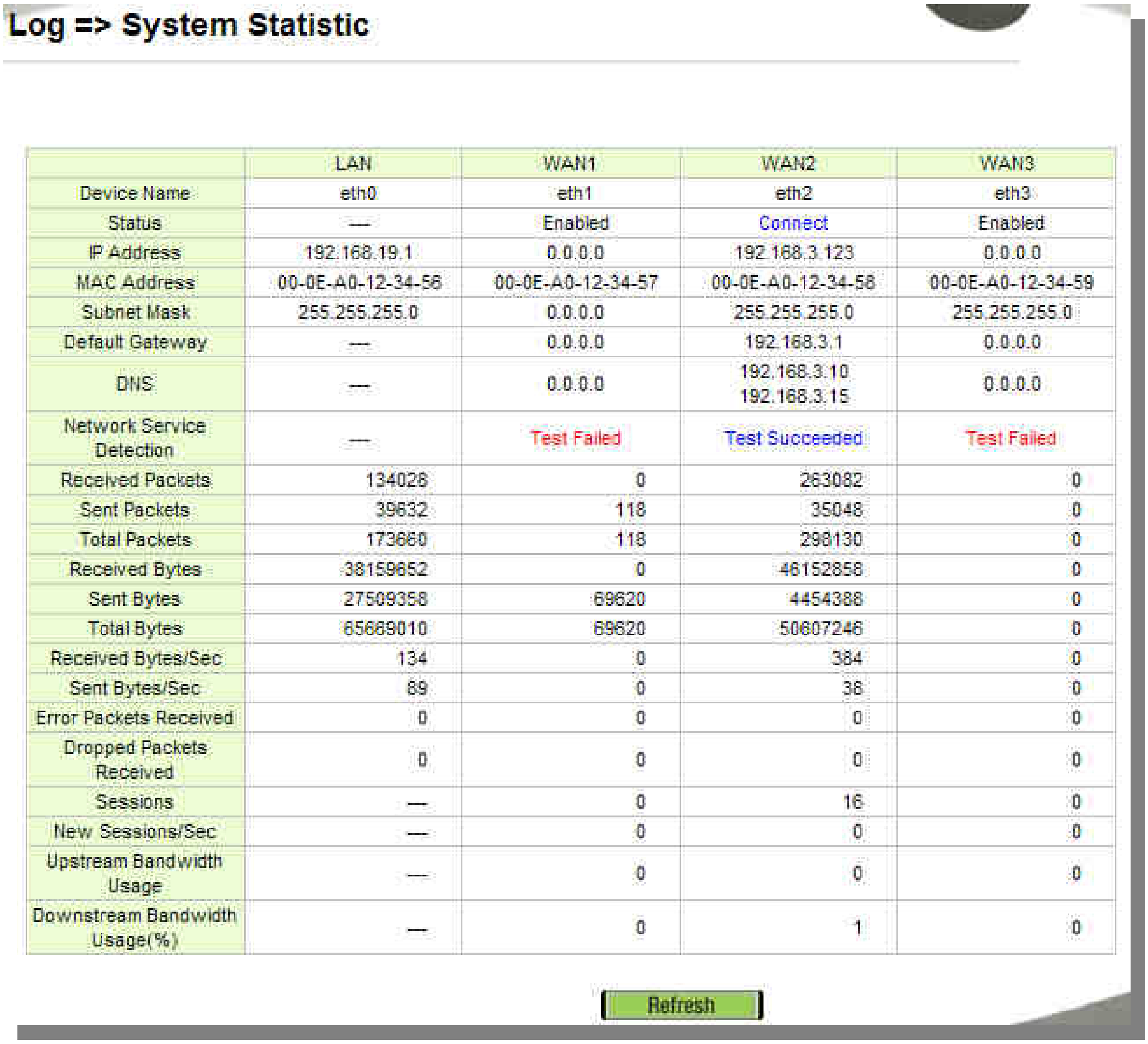
Time ▲	Event-Type	Message
Jan 1 00:00:08	SYS:[50]:	Broadband_Router : System is up (FVR080 1.5.2.03-qno4)
Jan 1 00:01:10	dhcpcd[135]:	timed out waiting for a valid DHCP server response
Jan 1 00:01:13	SYS:[129]:	WAN1 connection is up : 192.168.3.129/255.255.255.0 gw 192.168.3.1 on eth1
Aug 21 16:09:46	dhcpcd[135]:	terminating on signal 15
Aug 21 16:09:49	SYS:[129]:	WAN1 connection is down
Aug 21 16:09:50	SYS:[129]:	WAN2 connection is down
Aug 21 16:09:52	SYS:[129]:	WAN1 connection is up.: 192.168.3.129/255.255.255.0 gw 192.168.3.1 on eth1
Aug 21 19:09:39	dhcpcd[828]:	dhcpStart: bind: Address already in use
Aug 21 19:10:39	dhcpcd[828]:	timed out waiting for a valid DHCP server response

Clear Log Now：

This feature clears all the current information on the log.

7.2 System Statistic

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

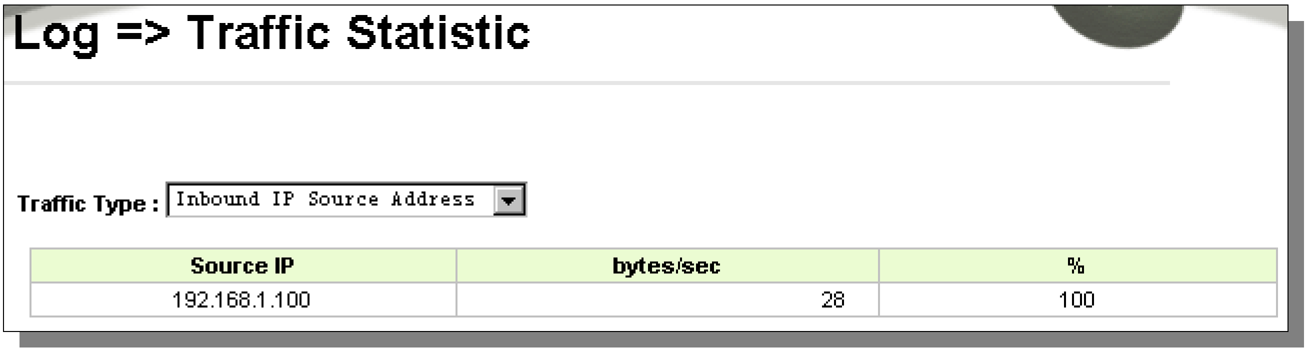


Log => System Statistic

	LAN	WAN1	WAN2	WAN3
Device Name	eth0	eth1	eth2	eth3
Status	—	Enabled	Connect	Enabled
IP Address	192.168.19.1	0.0.0.0	192.168.3.123	0.0.0.0
MAC Address	00-0E-A0-12-34-56	00-0E-A0-12-34-57	00-0E-A0-12-34-58	00-0E-A0-12-34-59
Subnet Mask	255.255.255.0	0.0.0.0	255.255.255.0	255.255.255.0
Default Gateway	—	0.0.0.0	192.168.3.1	0.0.0.0
DNS	—	0.0.0.0	192.168.3.10 192.168.3.15	0.0.0.0
Network Service Detection	—	Test Failed	Test Succeeded	Test Failed
Received Packets	134028	0	263082	0
Sent Packets	39632	118	35048	0
Total Packets	173660	118	298130	0
Received Bytes	38159652	0	46152858	0
Sent Bytes	27509358	69620	4454388	0
Total Bytes	65669010	69620	50607246	0
Received Bytes/Sec	134	0	384	0
Sent Bytes/Sec	89	0	38	0
Error Packets Received	0	0	0	0
Dropped Packets Received	0	0	0	0
Sessions	—	0	16	0
New Sessions/Sec	—	0	0	0
Upstream Bandwidth Usage	—	0	0	0
Downstream Bandwidth Usage(%)	—	0	1	0

7.3 Traffic Statistic

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



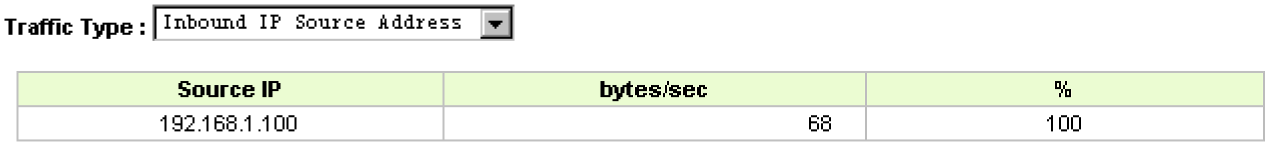
Log => Traffic Statistic

Traffic Type : Inbound IP Source Address

Source IP	bytes/sec	%
192.168.1.100	28	100

Inbound IP Address

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

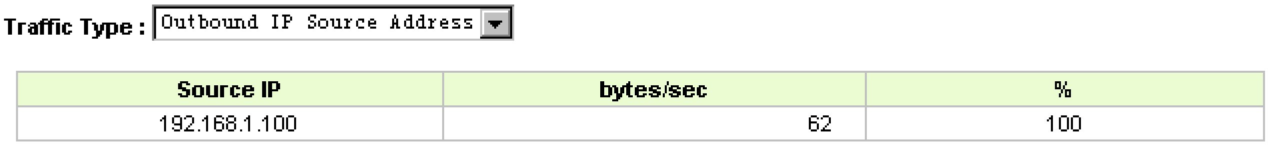


Traffic Type : Inbound IP Source Address

Source IP	bytes/sec	%
192.168.1.100	68	100

Outbound IP Address

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

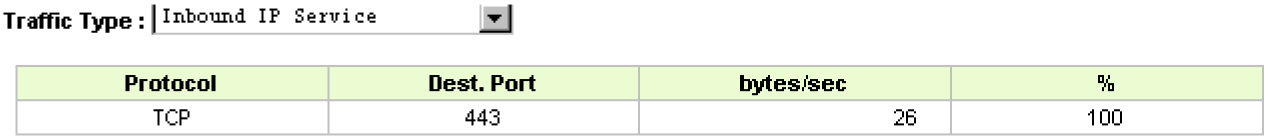


Traffic Type : Outbound IP Source Address

Source IP	bytes/sec	%
192.168.1.100	62	100

Inbound Service

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

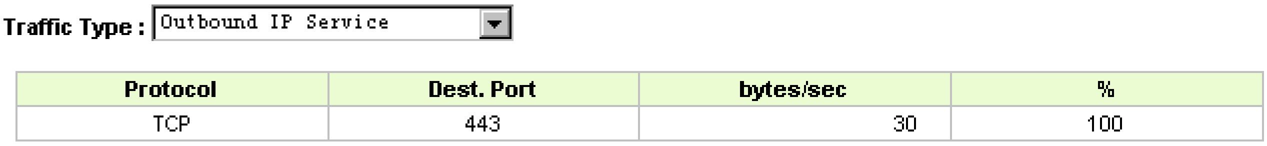


Traffic Type : Inbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	443	26	100

Outbound Service Ports

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



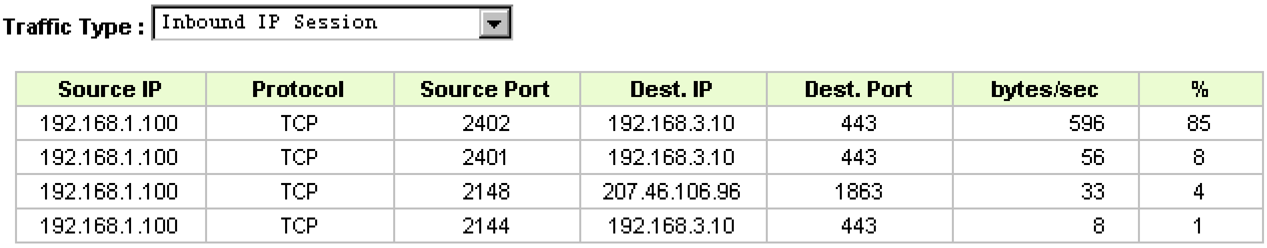
Traffic Type : Outbound IP Service

Protocol	Dest. Port	bytes/sec	%
TCP	443	30	100

Inbound Session

The figure displays the source IP address, network protocol type, source port, destination

IP address, destination port, bytes per second and percentage.

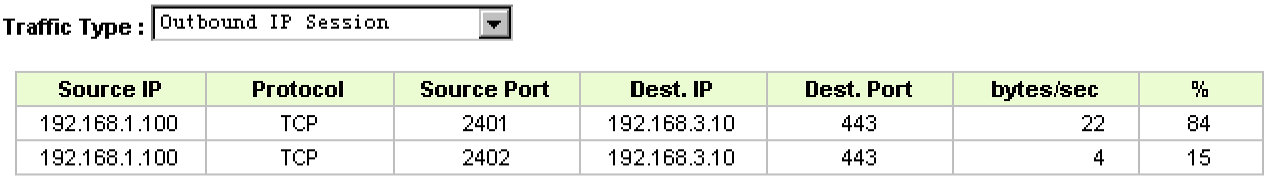


Traffic Type : Inbound IP Session

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2402	192.168.3.10	443	596	85
192.168.1.100	TCP	2401	192.168.3.10	443	56	8
192.168.1.100	TCP	2148	207.46.106.96	1863	33	4
192.168.1.100	TCP	2144	192.168.3.10	443	8	1

Outbound Session

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

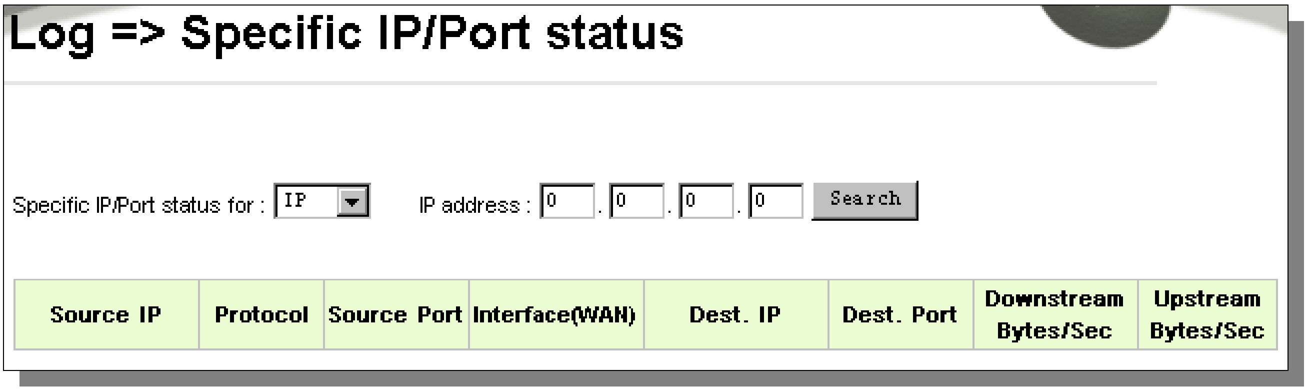


Traffic Type : Outbound IP Session

Source IP	Protocol	Source Port	Dest. IP	Dest. Port	bytes/sec	%
192.168.1.100	TCP	2401	192.168.3.10	443	22	84
192.168.1.100	TCP	2402	192.168.3.10	443	4	15

7.4 Specific IP/Port status

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



Log => Specific IP/Port status

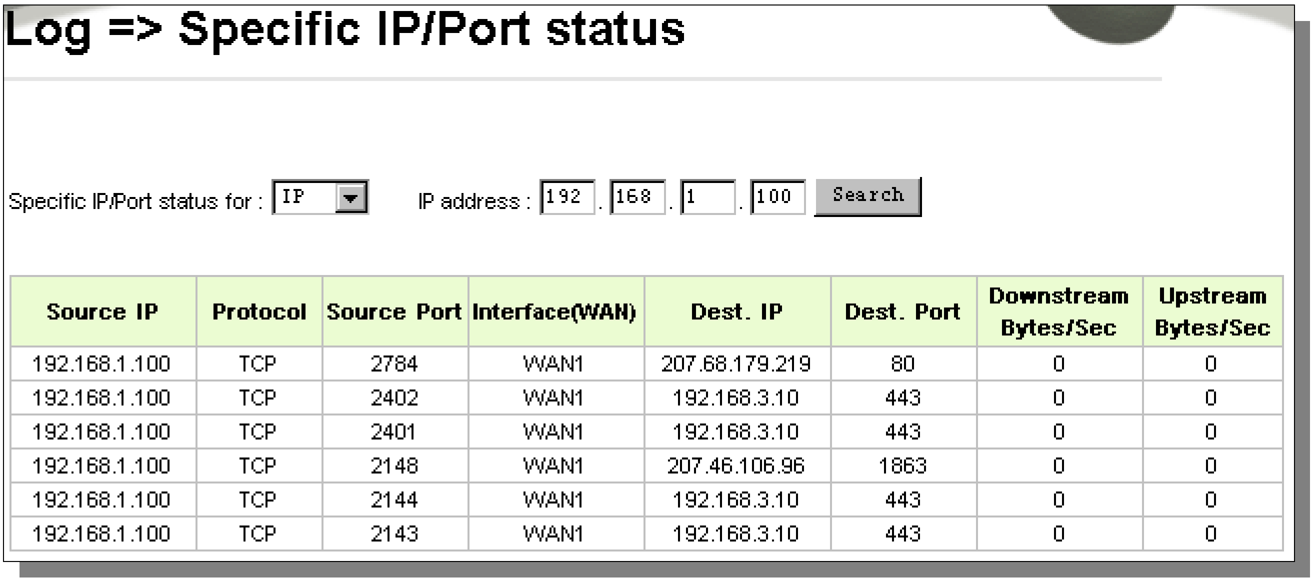
Specific IP/Port status for : IP

IP address : 0 . 0 . 0 . 0

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.



Log => Specific IP/Port status

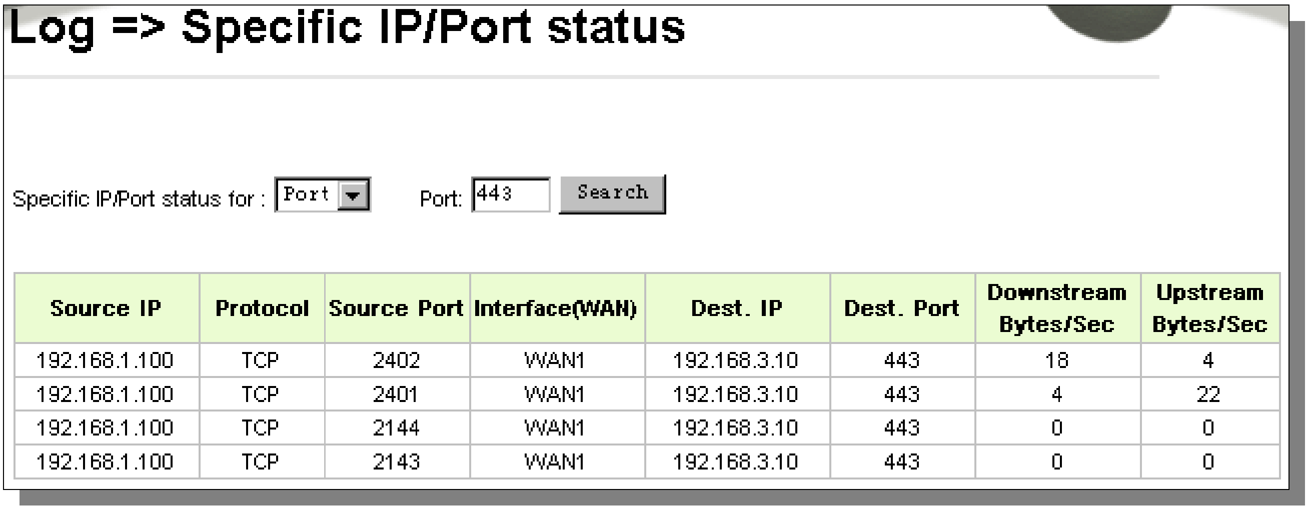
Specific IP/Port status for : IP

IP address : 192 . 168 . 1 . 100

Source IP	Protocol	Source Port	Interface(WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2784	WAN1	207.68.179.219	80	0	0
192.168.1.100	TCP	2402	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	2401	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	2148	WAN1	207.46.106.96	1863	0	0
192.168.1.100	TCP	2144	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	2143	WAN1	192.168.3.10	443	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.



Log => Specific IP/Port status

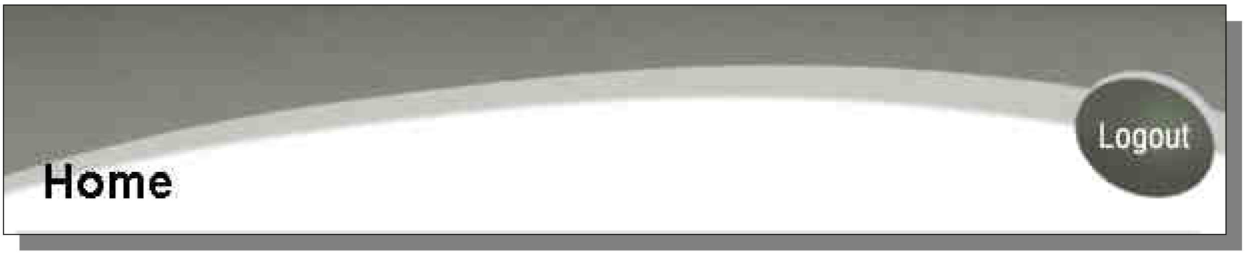
Specific IP/Port status for : Port

Port: 443

Source IP	Protocol	Source Port	Interface(WAN)	Dest. IP	Dest. Port	Downstream Bytes/Sec	Upstream Bytes/Sec
192.168.1.100	TCP	2402	WAN1	192.168.3.10	443	18	4
192.168.1.100	TCP	2401	WAN1	192.168.3.10	443	4	22
192.168.1.100	TCP	2144	WAN1	192.168.3.10	443	0	0
192.168.1.100	TCP	2143	WAN1	192.168.3.10	443	0	0

8、Logout

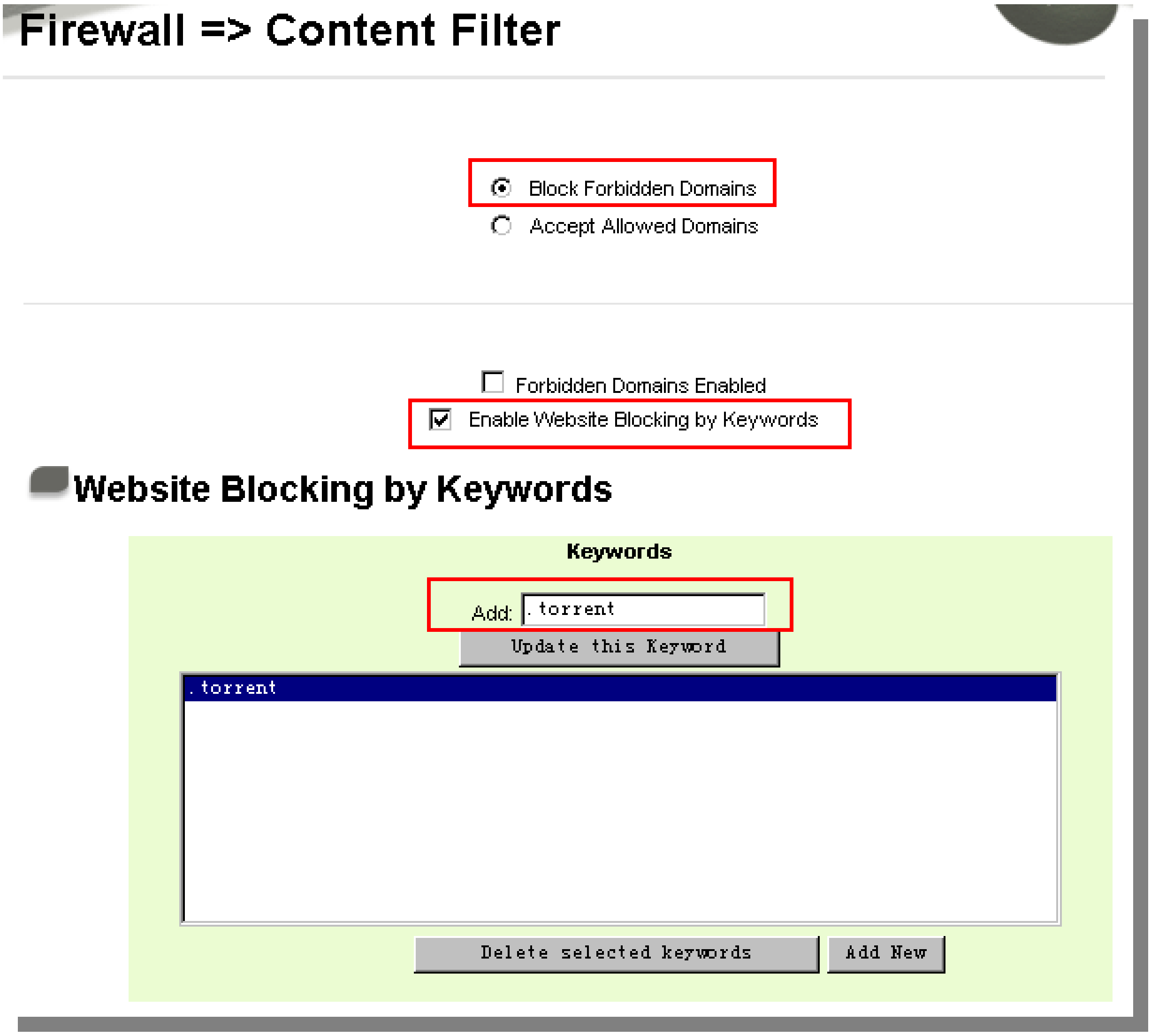
On the top right corner of the web- based UI, there is a Logout button. Click on it to log out of the web- based UI. To enter next time, open the Web browser and enter the IP address, user name and password to log in.



Appendix 1: Troubleshooting

（1） Block Basic BT Download Method

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



Firewall => Content Filter

● Block Forbidden Domains
○ Accept Allowed Domains

□ Forbidden Domains Enabled
☑ Enable Website Blocking by Keywords

Website Blocking by Keywords

Keywords

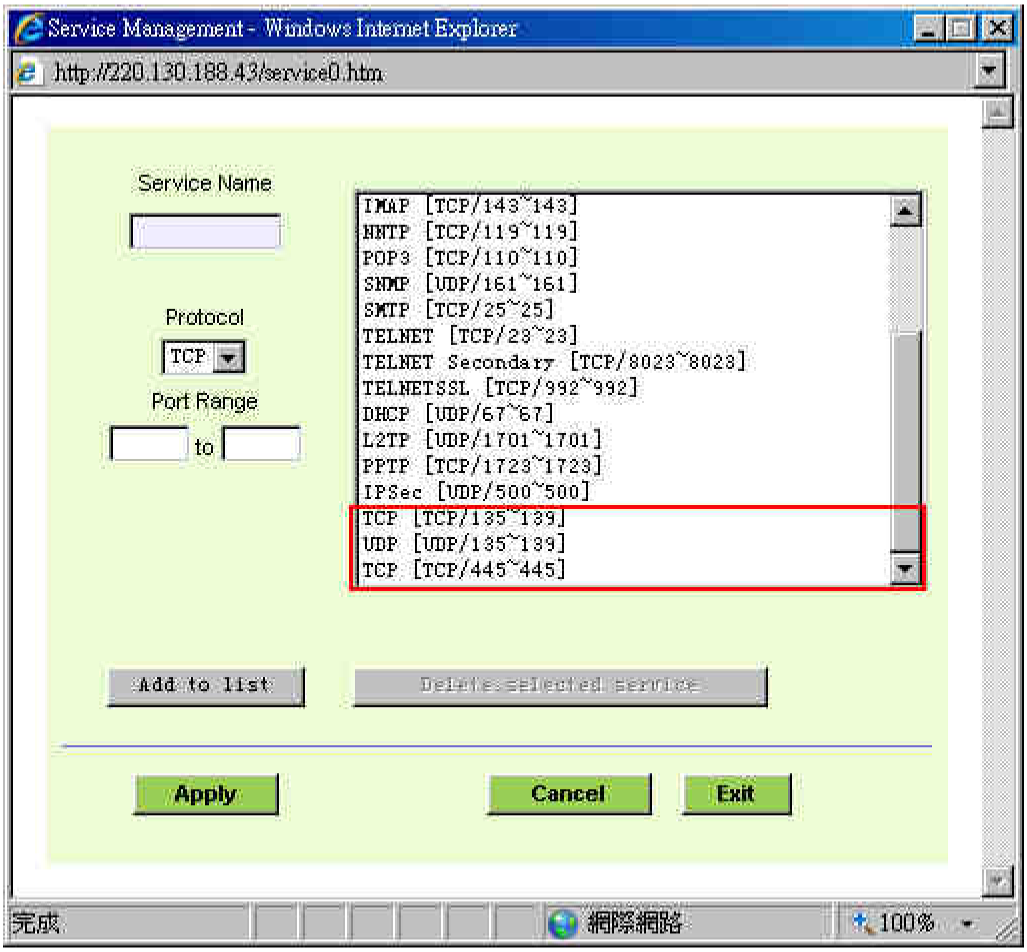
Add: .torrent

.torrent

（2） Prevention of Shock Wave and Worm Virus

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

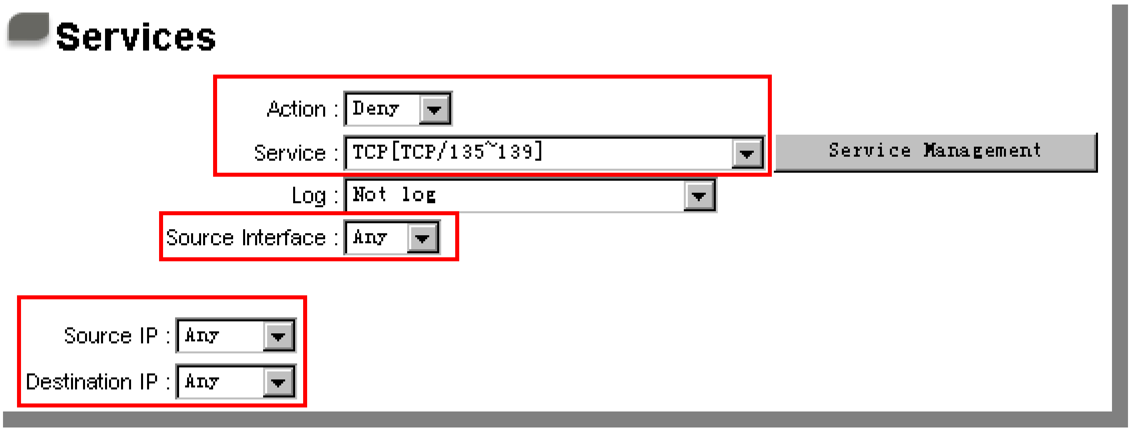
a. Add this TCP135-139, UDP135-139 and TCP445 Port:



Protocol: TCP

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

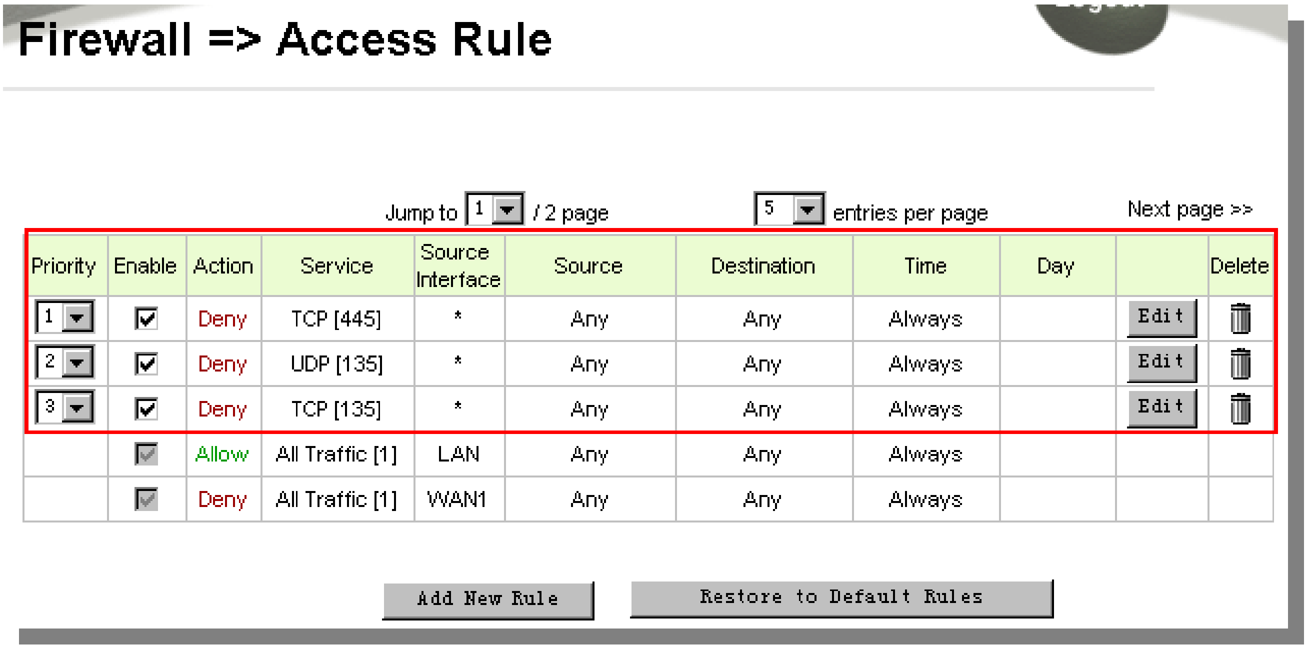
b. Use the "Access Rule" in the firewall and set to block these three ports:



Action : Deny
Service : TCP[TCP/135~139]
Log : Not log
Source Interface : Any
Source IP : Any
Destination IP : Any

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:



Firewall => Access Rule

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

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day		Delete
1	☑	Deny	TCP [445]	*	Any	Any	Always		Edit	🗑
2	☑	Deny	UDP [135]	*	Any	Any	Always		Edit	🗑
3	☑	Deny	TCP [135]	*	Any	Any	Always		Edit	🗑
	☑	Allow	All Traffic [1]	LAN	Any	Any	Always			
	☑	Deny	All Traffic [1]	WAN1	Any	Any	Always			

（3）ARP virus attack prevention

1）. ARP Issue and Information

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

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

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

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

For example, host A (192.168.1.5) transmits data to Host B (192.168.1.1) .Transmitting data, Host A searches for the destination IP address from the ARP Cache. If it is located, MAC address is known. Simply fill in the MAC address for transmission. If no corresponding IP address is found in ARP cache, Host A will send a broadcast. The MAC address is "FF.FF.FF.FF.FF.FF," which is to inquire all the host devices in the same network session about

"What is the MAC address of "192.168.1.1"? Other host devices do not respond to the ARP inquiry except host device B, which responds to host device A when receiving this frame: "The MAC address of 192.168.1.1 is 00-aa-00-62-c6-09". So Host A knows the MAC address of Host B, and it can send data to Host B. Meanwhile, it will update its ARP cache.

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

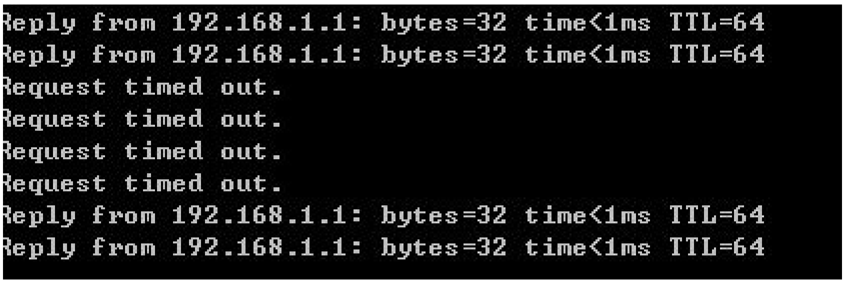
Such virus program as PWSteal. lemir or its transformation is worm virus of the Trojan programs affecting Windows 95/ 98/ Me/ NT/ 2000/ XP/ 2003. There are two attack methods affecting the network connection speed: cheat on the ARP table in the device or LAN PC. The former intercepts the gateway data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

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

2）. ARP Diagnosis

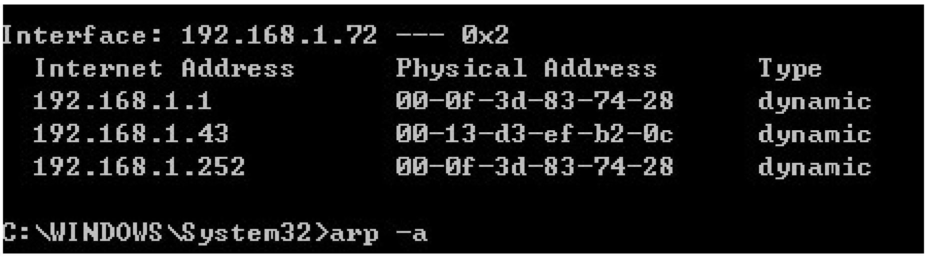
If one or more computers are affected by the ARP virus, we must learn how to diagnose and take appropriate measures. The following is experience shared by Qno technical engineers with regard to the ARP prevention.

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



```
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 lf later there is connection, it is possible that the system is attacked by ARP. To verify the situation, we may judge by checking ARP table. Enter the ARP -a command as illustrated below.



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

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

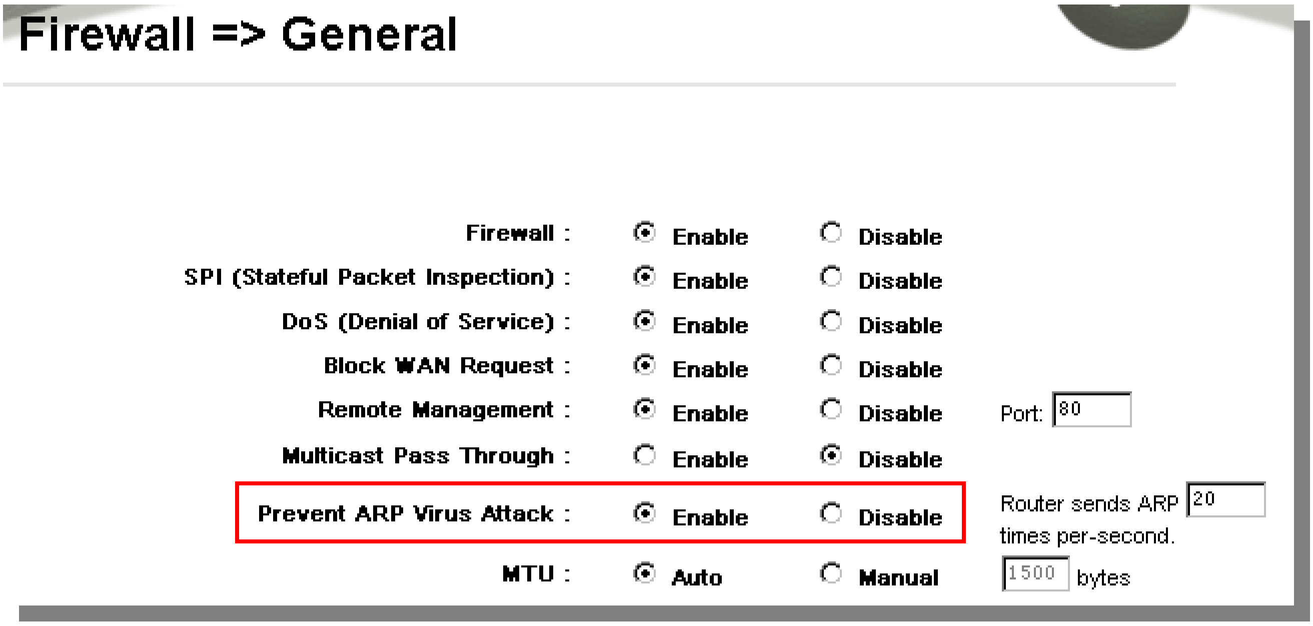
It is found that the IP of 192.168.1.1 and 192.168.252 points to the same MAC address as 00-0f-3d-83-74-28. Evidently, this is a cheat by ARP.

3）. ARP Solution

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

a) Enable "Prevent ARP Virus Attack":

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

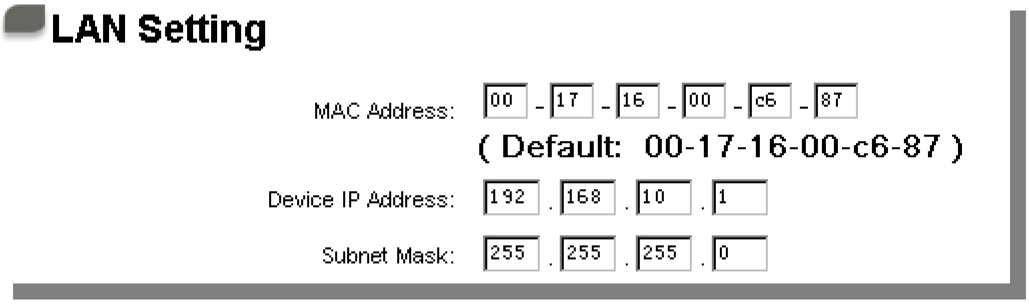


Firewall => General

Firewall :	● Enable	○ Disable	
SPI (Stateful Packet Inspection) :	● Enable	○ Disable	
DoS (Denial of Service) :	● Enable	○ Disable	
Block WAN Request :	● Enable	○ Disable	
Remote Management :	● Enable	○ Disable	Port: 80
Multicast Pass Through :	○ Enable	● Disable	
Prevent ARP Virus Attack :	● Enable	○ Disable	Router sends ARP 20 times per-second.
MTU :	● Auto	○ Manual	1500 bytes

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

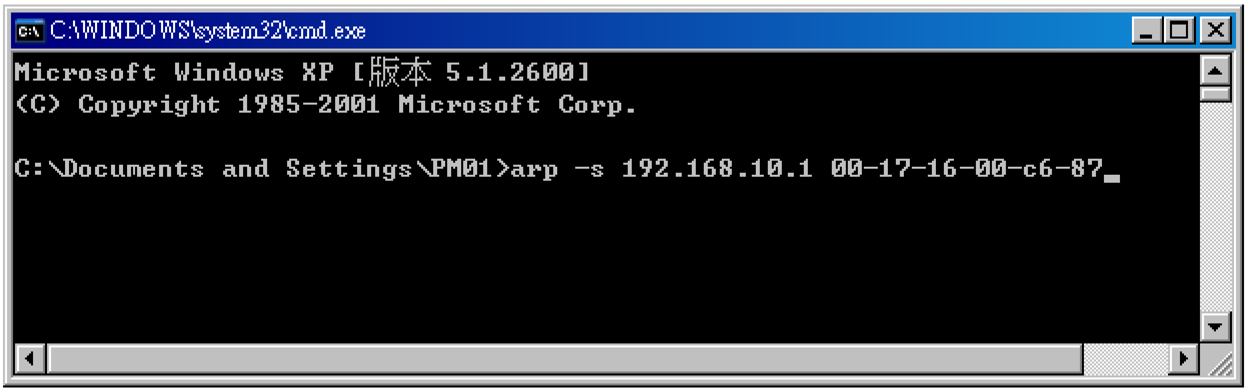
MAC Address: 00 - 17 - 16 - 00 - c6 - 87

(Default: 00-17-16-00-c6-87)

Device IP Address: 192 . 168 . 10 . 1

Subnet Mask: 255 . 255 . 255 . 0

On every PC, start or operate cmd to enter the dos operation. Enter arp –s 192.168.10.1 00-17-16-00-c6-87 so as to finish the binding of pc01.As illustrated in Figure 7



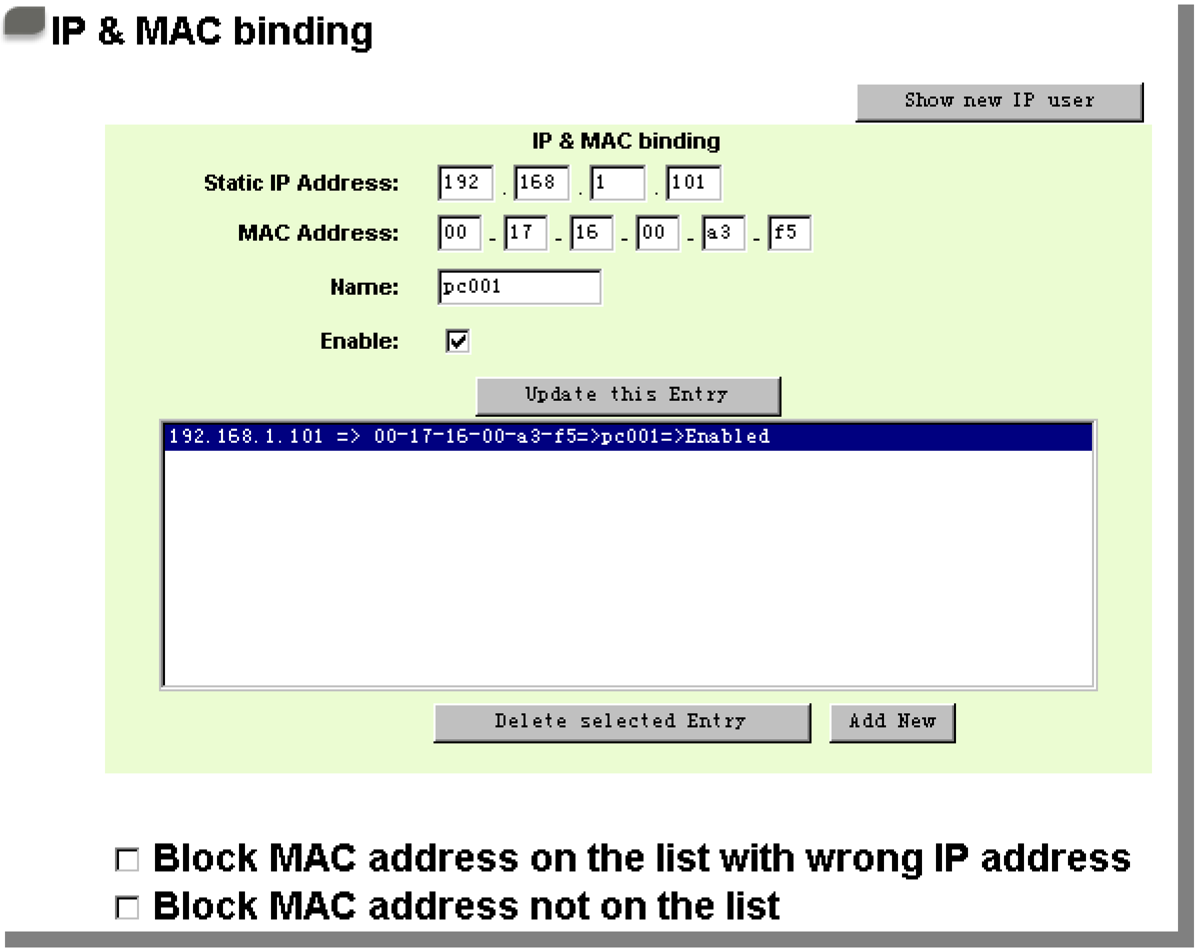
```
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\PM01>arp -s 192.168.10.1 00-17-16-00-c6-87_
```

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.



IP & MAC binding

Static IP Address: 192 . 168 . 1 . 101

MAC Address: 00 - 17 - 16 - 00 - a3 - f5

Name: pc001

Enable: ☑

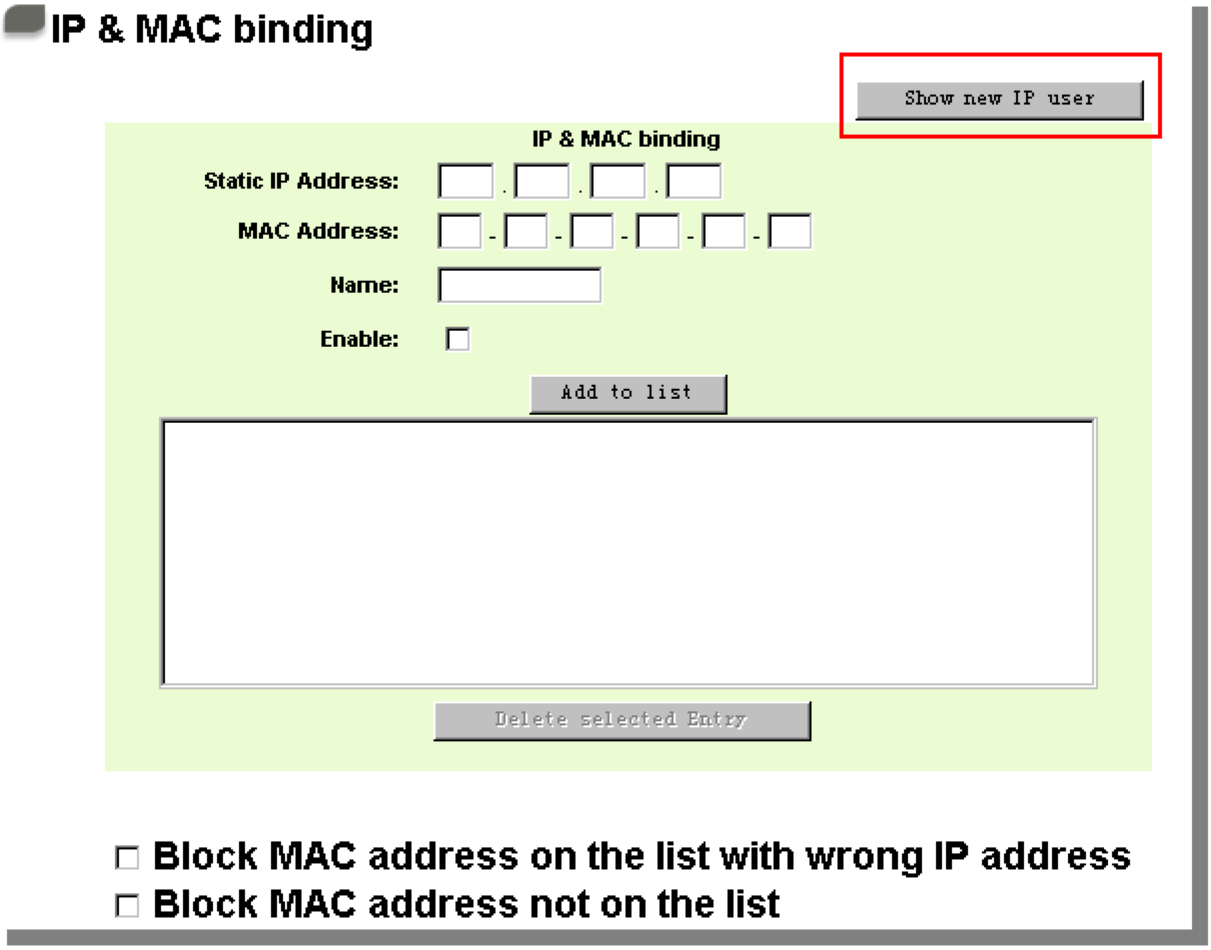
```
192.168.1.101 => 00-17-16-00-a3-f5=>pc001=>Enabled
```

□ Block MAC address on the list with wrong IP address

□ Block MAC address not on the list

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

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



IP & MAC binding

IP & MAC binding

Static IP Address: [ ] . [ ] . [ ] . [ ]

MAC Address: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

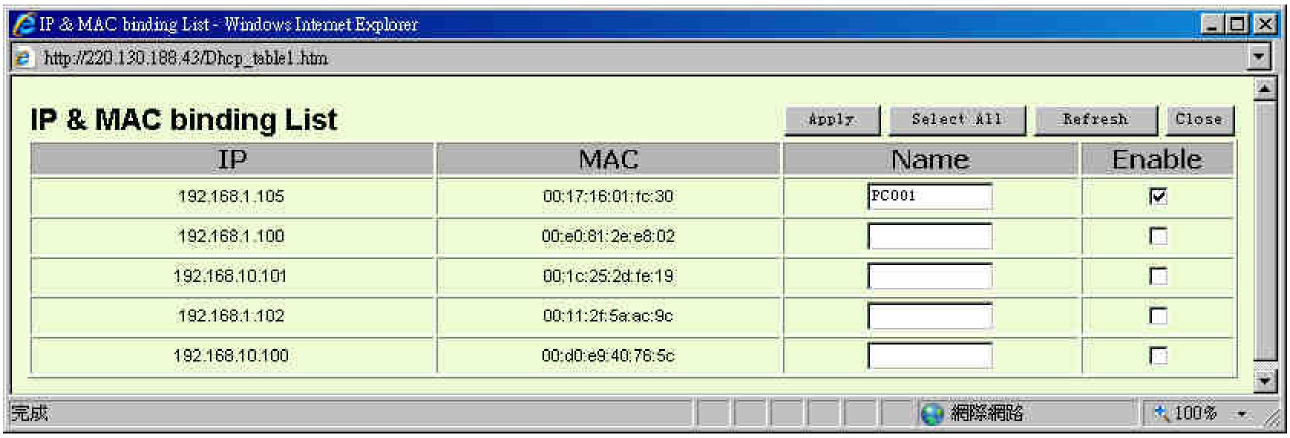
Name: [ ]

Enable: □

□ 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.

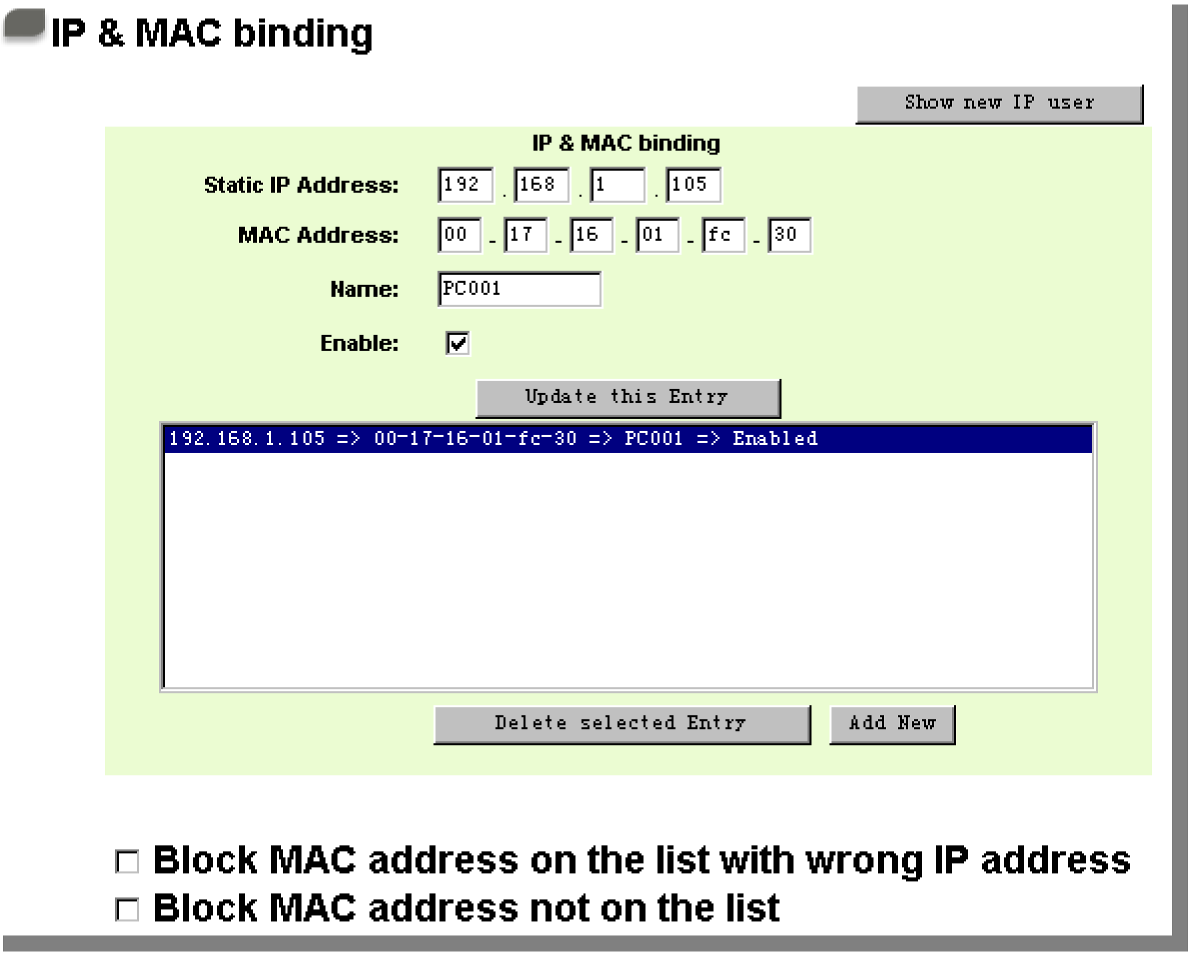


IP & MAC binding List - Windows Internet Explorer
http://220.130.188.43/Dhcp_table1.htm
Apply
Select All
Refresh
Close
完成
網際網路
100%

IP & MAC binding List

IP	MAC	Name	Enable
192.168.1.105	00:17:16:01:fc:30	PC001	☑
192.168.1.100	00:e0:81:2e:e8:02		□
192.168.10.101	00:1c:25:2d:fe:19		□
192.168.1.102	00:11:2f:5a:ac:9c		□
192.168.10.100	00:d0:e9:40:76:5c		□

Now the bound options will display on the IP and MAC binding list and click "Apply" to finish binding.



IP & MAC binding

IP & MAC binding

Static IP Address: 192 . 168 . 1 . 105

MAC Address: 00 - 17 - 16 - 01 - fc - 30

Name: PC001

Enable: ☑

```
192.168.1.105 => 00-17-16-01-fc-30 => PC001 => Enabled
```

□ Block MAC address on the list with wrong IP address

□ Block MAC address not on the list

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

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

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

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

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

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

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

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

４）. Summary

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

Appendix 2: Qno Technical Support Information

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

Qno Offical Website：http://www.Qno.com.tw

Taiwan Tehcnical Center：

E-mail：QnoFAE@qno.com.tw