

Contents

Chapter One Product Introduction	3
1.1 Product Introduction	3
1.2 Main features	4
1.3 Product Specifications	6
Chapter Two: Product Overview	8
2.1 Quick Installation	8
2.1.1 PPPOE	10
2.1.2 Dynamic IP	10
2.1.3 Static IP	11
Chapter Three: Configuration	13
3.1 Launch and login	13
3.2 Running Status	14
3.2.1 WAN Status	14
3.2.2 LAN Status	15
3.2.3 Information	16
3.3 Wizard	17
3.4 LAN Settings	17
3.4.1 LAN Settings	17
3.4.2 MAC Address Clone	18
3.4.3 DNS Server	19
3.4.4 Router's Access Limit	20
3.5 WAN Settings	20
3.5.1 WAN Settings	21
3.5.1.1 Dynamic IP	21
3.5.1.2 Static IP	22
3.5.1.3 PPPOE	22
3.5.2 WAN Parameters	23
3.6 DHCP Server	24
3.6.1 DHCP Server Setting	24
3.6.2 DHCP Client List	26
3.6.3 Static Assign	26
3.7 Dual WAN Settings	27

3.7.1 Dual WAN Settings	28
3.7.1.1 Work mode	28
3.7.1.2 ISP Circuitry Setting	29
3.7.2 Cable Detection	30
3.8 Virtual Server	31
3.8.1 Virtual Server	31
3.8.2 UPnP Settings.....	33
3.8.3 DMZ Host.....	34
3.9 Security Settings	34
3.9.1 Client Filter	35
3.9.2 URL Filtering	37
3.9.3 MAC Filter	39
3.9.4 WAN IP filter.....	41
3.10 QoS Settings	42
3.10.1 QoS Settings.....	42
3.10.2 QoS Rule	43
3.10.2.1 QoS Rule list.....	43
3.10.2.2 QoS Rule Configuration	45
3.11 LAN IP Control	45
3.12 ARP Bind.....	47
3.13 System Tools.....	47
3.13.1 Time Setting	48
3.13.2 Remote Web Manage	49
3.13.3 Backup/Resume settings	50
3.13.4 Software Upgrade	50
3.13.5 Restore Factory Settings.....	51
3.13.6 Restart the Router	52
3.13.7 Change Password.....	52
3.14 System Log	53
3.14.1 Log Settings	53
3.14.2 Log Configuration.....	54
3.14.3 Log Display	54
3.15 Logout.....	55

Chapter One Product Introduction

1.1 Product Introduction

Thanks for purchasing NE-480T+/490T+/R6000+ Enterprise/Net-bar level router. NE-480T+/490T+/R6000+ is NGN latest multifunctional broadband access products specially designed for Net-bar, community, enterprise and school. With main Frequency up to 533 MHz, NE-480T+/490T+/R6000+ adopts Intel IXP high-end network processor of high quality and high stability trusted in the whole world. It adopts six-layer PCB professional design, fully ensuring the powerful and stable performance. With bidirectional forwarding rate up to 200Mbps, it supports more than 70,000 Link counts and data packing is fast and stable. Powerful Firewall can effectively prevent various hacker attacks, ARP attack and cheat, ARP virus etc.

Besides being equipped with common functions of all the other broadband routers, NE-480T+/490T+/R6000+ provides multiple advanced functions such as client real-time flow view, bandwidth control based on IP address, single PC's connection limit, ARP bind, UPnP, DDNS, VPN Pass-through, Firewall, and management switch.

Attack defense effectively improves network reliability of Internet bars. It supports LAN and WAN attack defense against scanning, DoS, suspicious packages and packages containing IP options. It can detect and defense against various network attacks such as IP cheat, source routing attacks, IP and ports scanning and DoS. Moreover, it provides reliable security for Internet bars and effectively defense against virus attacks such as Nimda, Shock wave and Trojan virus.

QoS based on IP or port can limit the bandwidth of single PC and link counts to

effectively prevent users from using P2P special application excessively occupying network resources, which makes network games more smooth.

Furthermore, it provides detail traffic statistics list.

It supports ARP bind and effectively prevents from ARP attacks.

With two WAN ports, NE-480T+/490T+/R6000+ adopts unique circuit load balance technology and can automatically select the optimum circuit according to circuit situation. Different ISP data flow selects the corresponding WAN circuit transmission. It ensures special application through the same WAN port transmission (such as part of the game) is completed successfully.

Supports port mirroring for facilitating the monitoring of Internet bars. Transmission data of Internet bars, providing reference data for analyzing or solving network problems, can be copied to monitoring port on requirements to meet Internet bars' monitoring requirements of Public Security Department.

Limit extranet IP or port to ensure LAN security.

NE-480T+/490T+/R6000+ provides Web-based management with easy configuration and supports online software upgrade to satisfy high-performance, multifunctional, high-reliability and high-security requirements of Internet bars' users.

1.2 Main features

- Compliant with IEEE802.3, IEEE802.3u and IEEE802.3x standards
- Supports PPPoE, PPP, IP, ARP, DHCP, TCP, UDP, HTTP, FTP, DNS protocols

- Supports 2 10/100Mbps Auto-Negotiation WAN ports, connectable to xDSL/Ethernet/Cable
- Provides 3 10/100Mbps Auto-Negotiation LAN ports, connected to LAN
- Supports port bandwidth control, port VLAN and port mirroring
- Supports traffic statistics function, which enables administrator to analyze the use of the whole network resources
- Supports WAN physical parameter modification to meet users' special requirements
- Support VPN Pass-through, UPnP and DDNS
- Supports QoS configuration based on IP or Port, which can limit the single PC's bandwidth
- Supports ARP bind to prevent from ARP attacks effectively
- Supports virtual server, special software program, DMZ and static routing
- Supports link count configuration and limit the single PC's link count
- Supports to display WAN bandwidth use rate and in time find out the use of network bandwidth
- Supports router access control and forbids unauthorized IP address to access the router Web
- According to circuit situation, automatically select the optimum circuit
- Different ISP data flow selects the corresponding WAN port circuit transmission

Ensures specific application through the same WAN port transmission (such as part of the game) is completed successfully

- With built-in firewall, it supports IP address filter, URL Filter, MAC Address Filter
- Provides attack defense against network and virus attack

- Prevents from DoS attack, ARP attack, able to separate the computer with virus
- Because of two cables, outlet bandwidth is multiplied and download speed greatly enhances
- Supports MAC address modification or clone and provides configuration file backup and load
- Limit extranet IP or port to ensure LAN security
- Supports remote Web management and English configuration Interface with simple and easy configuration guide
- Provides syslog function and external syslog server to record status
- Provides detail attack, system and security log
- Supports circuit detection function to know ISP circuit situation in time
- Provides built-in power, 1U steel chassis and 19-inch standard rack

1.3 Product Specifications

Standards and protocols supported		IEEE 802.3, IEEE 802.3u, IEEE 802.3x, TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP, DNS, ARP
Ports	LAN ports	3 10/100M Auto-Negotiation RJ-45 ports (Auto MDI/MDIX)
	WAN ports	2 10/100M Auto-Negotiation RJ-45 ports (Auto MDI/MDIX)
Network media		10Base-T: Cat.3 or above UTP 100Base-TX: Cat.5 UTP

LED Indicator	LAN/WAN ports	Link/Act (connection/work) 100Mbps (speed)
	Others	Power SYS
Dimension (L x W x H)		294mm x 180mm x 44mm
Environments		Operating Temperature: 0°C~ 40°C; Storage Temperature: -40°C~70°C; Operating Humidity : 10% ~90% RH no condensing; Storage Humidity: 5%~90% RH no condensing
Power and Consumption		Input: 110-240VAC, 50/60Hz Maximum Consumption: 5.2W


Chapter Two: Product Overview

2.1 Quick Installation

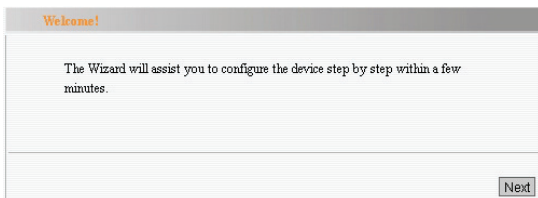
This product provides a browser-based configuration interface and this configuration is also suitable for any MS Windows, Macintosh or UNIX platforms.

Open IE and input <http://192.168.0.1> in the address bar. Then press Enter.

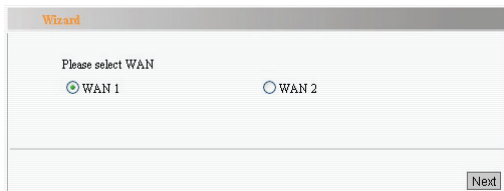
After connection, you can see login interface. The browser will display the Interface for administrator's mode. Please enter the user name and password (the default value for user name and password are "admin"). To enter into management screen fast next time, please select "Remember my password".

 **Notice:** For your router security, please modify system default user name and password after login.

If you correctly enter the user name and password, the browser will enter management screen and fast Setup Wizard will appear. Click "next" and enter Internet mode selection screen.

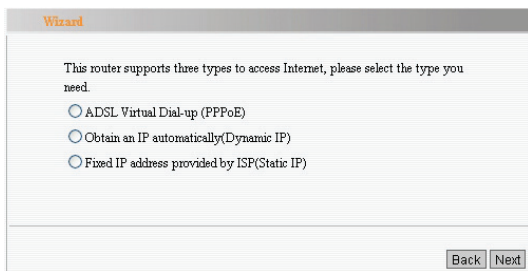


Please select the number of WAN ports to be configured and click “Next” to configure.



The router supports three common types to access the Internet (the default access type: dynamic IP access).

- **PPPOE Dial-up (ADSL):** Adopts PPPOE virtual dial-up to access the Internet
- **Dynamic IP:** Broadband networks or cables through DHCP server for the users to assign IP address
- **Static IP:** Ethernet broadband access type, ISP provides fixed IP address



According to your requirement, click “Next” and enter basic network parameters to access the internet.

2.1.1 PPPOE

If you access to the Internet through “ADSL Virtual Dial-up (PPPoE)”, please just enter the user name and password provided by the ISP into the dialogue box.

Wizard-ADSL

When you apply for ADSL dial-up service, The ISP may provide you account and password. If you forget or don't know well please refer to ISP.

User Name:

Password:

- User Name: Enter ADSL Internet account provided by your ISP. If you are not clear, please inquire ISP
- Password: Enter ADSL Internet password provided by your ISP. If you are not clear, please inquire ISP

2.1.2 Dynamic IP

If you access to the Internet through “Dynamic IP”, you are able to obtain dynamic IP address from the ISP to access the Internet without other configuration. Please click “Next” to save.

Notice: Router’s WAN IP address and LAN IP address should be in the same segment, or the router can’t work normally. When it meets emergency, please use the Reset button on the panel to reset.

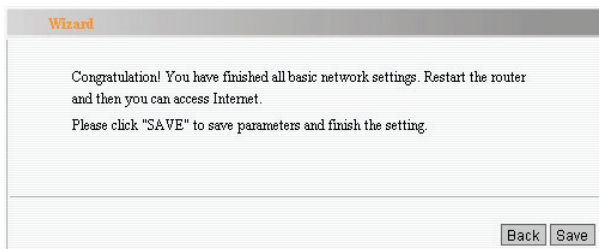
2.1.3 Static IP

If you access to the Internet through “Static IP”, please enter IP address, Sub-net mask, Gateway, Main DNS and Secondary DNS provided by your ISP. Then, please click “Next” to save.

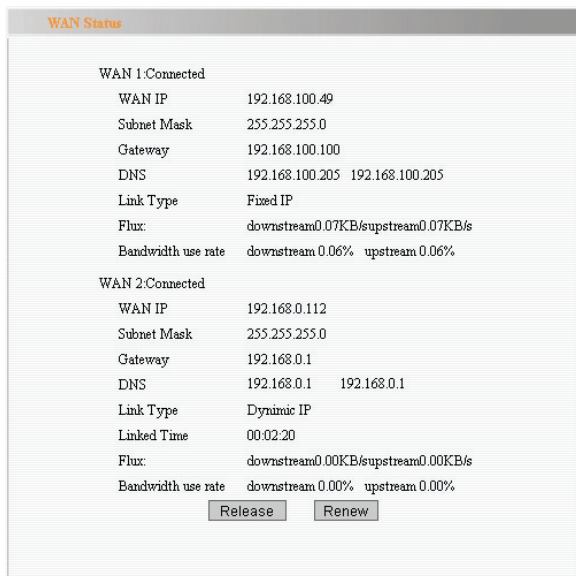
- **IP Address:** Router’s WAN IP address provided by your ISP. If you are not clear, please inquire ISP
- **Subnet mask:** Router’s WAN subnet mask provided by your ISP. If you are not clear, please inquire ISP
- **Gateway:** Input gateway provided by your ISP. If you are not clear, please inquire ISP
- **DNS Server:** input DNS provided by your ISP. If you are not clear, please inquire ISP
- **Secondary DNS (optional) :** If ISP provides two DNS server addresses, you can enter the other DNS server address here

Notice: IP address and LAN IP address appointed by Router’s WAN port should be in the same segment, or the router can’t work normally. When it meets emergency, please use the Reset button on the panel to reset.

After entering the basic network parameters to access the Internet, you will enter into Wizard screen.



After finishing all settings, go to "Running Status">"WAN Status" to view the configuration information.



Chapter Three: Configuration

3.1 Launch and login

After launching and Logging in successfully, the browser will display the administrator's mode screen as below figure shown. In the left-hand menu bar, there are eighteen buttons including Run status, Wizard, WAN settings, LAN settings, DHCP server, Dual WAN settings, Virtual server, Security settings, QoS settings, LAN IP control, ARP bind, Flux statistics, Switch settings, Router settings, System tools, System log and Logout. Single click a certain button and you are able to configure the corresponding function.

The screenshot displays the 'WAN Status' page of a New Generation Networks router. The interface features a dark red header with the company logo and name. A left-hand menu bar contains 18 items, with 'Run Status' selected. The main content area shows the status of two WAN connections, WAN 1 and WAN 2, both of which are connected. Each connection's details, including IP address, subnet mask, gateway, DNS, link type, flux, and bandwidth usage, are listed. A 'Refresh' button is located in the top right corner of the main content area. At the bottom of the WAN 2 section, there are 'Release' and 'Renew' buttons.

WAN 1 Connected	
WAN IP	192.168.100.49
Subnet Mask	255.255.255.0
Gateway	192.168.100.100
DNS	192.168.100.205 192.168.100.205
Link Type	Fixed IP
Flux:	downstream:0.07KB/s upstream:0.07KB/s
Bandwidth use rate	downstream:0.06% upstream:0.06%

WAN 2 Connected	
WAN IP	192.168.0.112
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
DNS	192.168.0.1 192.168.0.1
Link Type	Dynamic IP
Linked Time	00:09:45
Flux:	downstream:0.00KB/s upstream:0.00KB/s
Bandwidth use rate	downstream:0.00% upstream:0.00%

3.2 Running Status

3.2.1 WAN Status

Here, display current WAN linked status, WAN IP, Subnet mask, Gateway, DNS, Secondary DNS, WAN flux, Bandwidth use rate and Link type.

WAN Status	
WAN 1:Connected	
WAN IP	192.168.100.49
Subnet Mask	255.255.255.0
Gateway	192.168.100.100
DNS	192.168.100.205 192.168.100.205
Link Type	Fixed IP
Flux:	downstream0.07KB/supstream0.07KB/s
Bandwidth use rate	downstream 0.06% upstream 0.06%
WAN 2:Connected	
WAN IP	192.168.0.112
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
DNS	192.168.0.1 192.168.0.1
Link Type	Dynamic IP
Linked Time	00:02:20
Flux:	downstream0.00KB/supstream0.00KB/s
Bandwidth use rate	downstream 0.00% upstream 0.00%
<input type="button" value="Release"/> <input type="button" value="Renew"/>	

- WAN connection Status: Display WAN connection Status
 Not connected: Shows WAN ports aren't connected with network cables.
 Connecting: Shows WAN ports are connected and is obtaining IP address
 Connected: Shows router has normally connected to ISP.
- WAN IP: IP address provided by ISP
- Subnet mask: Subnet mask provided by ISP
- Gateway: Gateway provided by ISP

- DNS server: DNS server provided by ISP
- Secondary DNS server: Secondary DNS server provided by ISP
- WAN flux: Shows current bandwidth that the router has been already used.
The unit is KB/S.
For example: ISP assigns bandwidth 2Mbps=256KBps=2048Kbps
- Bandwidth use rate: The actual overall bandwidth rate that has been already used.
Please configure the real overall bandwidth in the QoS settings. Only after enabling QoS rule, this function can take effect, or this function can be disabled. Enter correctly overall bandwidth in the QoS setting, or bandwidth use rate will over 100%.
- Link Type: Shows current access type

3.2.2 LAN Status

Here, display current IP address, Subnet mask, DHCP server, NAT and Firewall.

LAN Status	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
NAT	Enable
Firewall	Disable

- IP Address: Display current IP address
- Subnet Mask: Display current Subnet mask
- DHCP Server: Display DHCP server "Enable" or "Disable" status which should be consistent with "DHCP server" → "DHCP server settings"

- NAT: Display router's work mode
- Firewall: Display current firewall status and the default status is "Disable". The firewall status can become "Enable" only when users select one option from "Security Settings" including "Client Filter", "URL Filter" and "MAC Address Filter"

3.2.3 Information

Display router current Running time, System time, Client count, NAT count, Bootcode version, LAN MAC address, WAN MAC address and Hardware version as below figure shown.

Information	
Running Time	00:00:20
System Time	2007-12-21 19:24:59
Client Count	2
NAT	3
Firmware Version	Ver 1.0.0.1
Bootcode Version	Ver 0.9.1
LAN MAC Address	00:02:B3:00:E0:00
WAN-1 MAC Address	00:02:B3:00:E0:01
WAN-2 MAC Address	00:02:B3:00:E0:02
Hardware Version	Ver 0.9.5

- Running Time: Display Running time after the system normally launches
- System Time: Display system renew time
- Client Count: Display connected computer count
- NAT Count: Display NAT Count that has been used by the router
- System Version: Display router's software version
- Bootcode Version: Display router's Bootcode version
- LAN MAC Address: Display router's LAN MAC address

- WAN-1 MAC Address: Display router's WAN-1 MAC address
- WAN-2 MAC Address: Display router's WAN-2 MAC address
- Hardware Version: Display router's Hardware version

3.3 Wizard

Please refer to chapter three: Quick Installation

3.4 LAN Settings

In the “LAN Settings” drop-down menu, there are four sub-items including “LAN Settings”, “MAC Clone”, “DNS Server” and “Access Limit”. Please click a certain sub-item and you can configure the corresponding function. We will give brief introduction about the four sub-items as follows:



3.4.1 LAN Settings

LAN Setting

Basic LAN parameter setting

MAC 00:02:B3:00:E0:00

IP 192.168.0.1

Netmask 255.255.255.0

Save Cancel Help

- IP Address: This refers to the LAN IP address of the router. Default IP address is 192.168.0.1, which you can change according to your requirement.
- Netmask: This refers to the LAN Subnet mask of the router, which you can input manually

3.4.2 MAC Address Clone

MAC Clone

WAN MAC Clone

WAN-1 MAC: 00:02:B3:00:E0:01 Factory Default

WAN-2 MAC: 00:02:B3:00:E0:02 Factory Default

Current PC MAC: 00:0A:E4:F5:82:7A Clone To WAN 1

Save Cancel Help

Some ISPs will bind users' PC MAC address. Please copy Current PC MAC address which is used by administrators to WAN MAC address or change MAC address manually. After changing MAC Address, the corresponding WAN MAC address will change.

- MAC Address: Default setting displays WAN MAC address and you can enter MAC Address manually
- Restore to Factory MAC: After clicking "Factory Default", factory MAC address will be displayed in MAC Address bar

- **MAC Address Clone:** After clicking “Clone”, current PC MAC address will be displayed in MAC Address bar

⚠ Notice: After changing MAC address, you need to restart the router and then the setting can take effect. However, if your ISP can't bind MAC Address, please don't use such function to avoid appearing other problems.

3.4.3 DNS Server

DNS Server	
DNS Setting	<input type="checkbox"/> Enable
DNS Agent	<input checked="" type="checkbox"/> Enable
DNS	<input type="text" value="192.168.100.205"/>
Standby DNS1(optional)	<input type="text" value="192.168.100.2"/>
Standby DNS2(optional)	<input type="text" value="192.168.0.1"/>
Standby DNS3(optional)	<input type="text" value="192.168.0.10"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

- **DNS Setting:** Default setting is “Disable”. After rebooting, the PC can obtain DNS 192.168.100.205 as above figure shown
- **DNS Agent:** Default setting is “Enable”. Assign router's IP address as DNS server address to PC
- **DNS Server:** Please enter DNS provided by ISP. If you are not clear, please inquire ISP
- **Standby DNS (optional):** If ISP provides you with four DNS servers, you can enter the other three DNS servers here, which should be the same as standby DNS address in the “DHCP Settings”. However, the system can come into effect only after modifying the parameters here. If you modify standby DNS server in the “DHCP Settings”, the system won't save.

⚠ Notice: DNS main function is that it can translate DNS (websites) that we

input into IP address.

3.4.4 Router's Access Limit

In order to increase the security of the router management, you can specify the computer's IP address and change the port to manage.

- Enable: Open access limit of router Web function
- IP Address: Enter LAN IP address of the PCs
- Port: Default port is 80. Please enter port number which can access the Web interface

⚠ Notice: After setting the appointed IP address, PCs with other IP addresses can't log in the router's Web management interface. After changing the router's access port, you are required to restart the router. For example: If router's address and IP address are 192.168.0.1 and access port is changed to 8888, login router's management screen will show 192.168.0.1:8888

3.5 WAN Settings

In the "WAN Settings" drop-down menu, there are two sub-items including "WAN Settings" and "WAN Parameters". Click a certain sub-item and you can configure the

corresponding function. We will give brief introduction about the two sub-items as follows:



3.5.1 WAN Settings

According to WAN port and WAN link type that you select to configure, you can change them correspondingly. The default type of accessing to the Internet is “Dynamic IP”

3.5.1.1 Dynamic IP

If you access to the Internet through dynamic IP, you are able to obtain IP address from the ISP automatically.

WAN Settings

WAN configuration(You should set two WAN separately.)

Please select WAN port:

WAN 1 Link Type:

MTU: (default 1500)

- MTU: the default value is 1500. You can change it according to your requirement.

3.5.1.2 Static IP

- **Static IP:** If you access to the Internet through static IP, you will have the fixed IP address provided by your ISP. The default value is 1500.

WAN Settings

WAN configuration (You should set two WAN separately.)

Please select WAN port:

WAN 1 Link Type:

IP Address:

Subnet Mask:

Gateway:

DNS:

Secondary DNS:

MTU: (default 1500)

- **MTU:** The default value is 1500. You can change it according to your requirement.

3.5.1.3 PPPOE

If you access to the Internet through ADSL virtual dial-up, in this page, you can change and configure other parameters.

WAN Settings

WAN configuration (You should set two WAN separately.)

Please select WAN port:

WAN 1 Link Type:

User Name:

Password:

MTU: (Default 1492)

Service: (Not necessary)

AC NAME: (Not necessary)

Please select the connecting mode according to your requirement:

Connecting automatically when power on or link lost.

Connecting manually.

Connecting if needed.

Waiting time when automatically break off: (60-3600 seconds)

Connecting automatically in period of time.

Notice: This function may take effect only if system time is set in "System Tool" setting.

Connecting period: from hour min to hour min

- **User Name:** This refers to your user name. Please input the ADSL user name provided by your ISP
- **Password:** Please input the ADSL password provided by your ISP. If you are not clear, please inquire ISP
- **Service:** Input the login Service provided by your ISP. (Optional)
- **MTU:** The default value is 1492. You can change it according to your requirement. However, the maximum MTU value can't exceed 1492.
- **Connecting automatically:** Connect automatically when power on or break off
- **Connecting manually:** This enables the user to connect manually.
- **Connecting if needed:** Connect automatically when there are data access
- **Connecting automatically in period of time:** Connect automatically at fixed time

3.5.2 WAN Parameters

This page provides settings of port status, port flow control, port speed rate etc. Please correctly configure parameters as below figure shown.

WAN Parameter					
	Port State	Flux Control	Negotiation Mode		
WAN1	Enable	Disable	Auto Negotiation		
WAN2	Enable	Disable	Auto Negotiation		
	Negotiation	Port State	Link Speed(Mbps)	Duplex Mode	Flux Control
WAN1	Connected	Connected	100	Full-Duplex	Disabled
WAN2	Connected	Connected	100	Full-Duplex	Disabled
	Ingress Mode	Ingress Speed	Egress Mode	Egress Speed	
WAN1	No Limit		<input type="checkbox"/> Enable		
WAN2	No Limit		<input type="checkbox"/> Enable		

Save Cancel Help

3.6 DHCP Server

In DHCP server drop-down menu, there are three sub-items including “DHCP Server” and “DHCP Client List” and “Static Assign”. We will have detail descriptions on these three functions as follows:




3.6.1 DHCP Server Setting

TCP/IP settings include IP address, Subnet mask, Gateway and DNS server. It is not an easy thing for all your LAN PCs to configure TCP/IP correctly. However, DHCP server can solve such problem. If you use DHCP server of this router, DHCP

server can automatically assign TCP/IP to all LAN PCs.

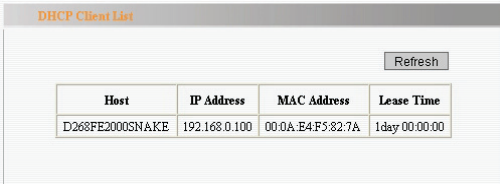
DHCP Server Setting	
DHCP Server	<input checked="" type="checkbox"/> Enable
Start IP	192.168.0.10
End IP	192.168.0.100
Lease Time	1440 (1-2880min)
Prime DNS(optional)	192.168.100.205
Standby DNS 1 (optional)	192.168.100.205
Standby DNS 2 (optional)	192.168.0.1
Standby DNS 3 (optional)	192.168.0.1
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

- **DHCP Server:** If you want to use DHCP to configure TCP/IP parameter automatically, please enable this option
- **Start IP:** The starting IP address for DHCP server to assign IP address automatically
- **End IP:** The ending IP address for DHCP server to assign IP address automatically
- **Lease Time:** Set the lease time for DHCP to assign IP address. The default value is 1440 minutes
- **Primary DNS server and standby DNS servers:** The values can change with primary DNS server and standby DNS servers of “LAN Settings” → “DNS Setting”. If you want to change the values, please enter into “LAN Settings” → “DNS Setting” screen.

 **Notice:** In order to use the DHCP server function of this router, the TCP/IP protocol of the LAN PCs should be set as “Automatically Obtain an IP Address”

3.6.2 DHCP Client List

This **DHCP** client list can display all the Host names, IP addresses, MAC addresses and Lease time through DHCP.



Host	IP Address	MAC Address	Lease Time
D268FE2000SNAKE	192.168.0.100	00:0A:E4:F5:82:7A	1day 00:00:00

- **Host:** the host name of the client
- **IP Address:** the IP address applied by the client
- **MAC Address:** the MAC address of the PC which applies the IP address successfully
- **Lease Time:** The use time for the host to obtain the IP address through DHCP server.

3.6.3 Static Assign

In order to make you conveniently control LAN PC IP address, this router provides built-in static assign, which can reserve the static IP address for the PC with appointed MAC address. When the PC requests DHCP server to obtain IP address, DHCP server will assign the reserved IP address to the PC.

The screenshot shows a web-based configuration interface titled "Static Assign". It contains a "Static Assign" section with two rows of input fields: "IP Address" (with the value "192.168.0." and a trailing empty box) and "MAC Address" (with six individual empty boxes for each octet and an "Add" button to the right). Below these inputs is a table with four columns: "No.", "IP Address", "MAC Address", and "Delete". At the bottom of the interface are "Save", "Cancel", and "Help" buttons.

- MAC Address: The MAC address of reserved IP PC
- IP Address: Reserved IP Address
- Add: Add the reserved IP address and MAC address to the table
- Delete: Delete connected static assign information

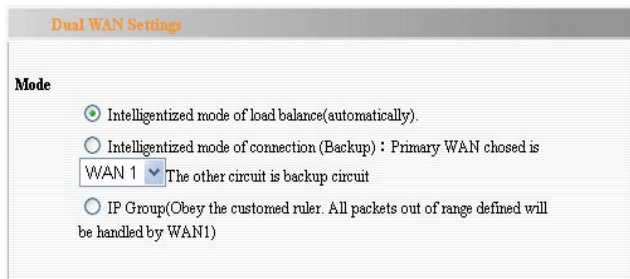
3.7 Dual WAN Settings

In "Dual WAN Settings" drop-down menu, there are two sub-items including "Dual WAN Settings" and "Cable Detection" as below figure shown. Click a certain sub-item. You can view and configure the corresponding function.



3.7.1 Dual WAN Settings

3.7.1.1 Work mode



As above figure shown, the router provides three kinds of load balance mechanisms:

- **Intelligentized mode of load balance (automatically):**
When you select this mode, the router will assign linked PCs automatically, according to linked PC count and your WAN bandwidth, to realize load balance of linked PCs. Circuit bandwidth setting is based on your entering bandwidth. For example, when up bandwidth of two WAN circuits is 512Kbit/sec, the automatic load balance ratio is 1:1. When up bandwidth of one circuit is 1024kbit/sec and up bandwidth of the other circuit is 512kbit/sec, the automatic load balance ratio is 2:1 and please enter uplink download bandwidth.
- **Intelligentized mode of connection (Backup):**
Please choose primary WAN. The other circuit is backup circuit. When you select this mode, all the data of LAN PCs will be removed from primary WAN. For example, if there is something wrong with primary WAN, the router will automatically switch to backup circuit so the PCs won't be drop-line.
- **IP Group (Obeeyed the customed rule. All packets out of range defined will be handled by WAN1).** When you select this mode, user customed load setting is

priority. All packets out of range will be handled by WAN1. If there is something wrong with WAN1 circuit, the router will automatically switch to WAN2.

Intelligentized mode of load balance, Intelligentized mode of connection (Backup) or IP Group should be matched with “user customized load setting”, which can be more flexible use of your bandwidth. You can use specific application service to access the specific intranet IP or specific WAN to access the specific destination IP.

3.7.1.2 ISP Circuitry Setting

ISP circuitry real bandwidth	
Input ISP assign real bandwidth	
WAN 1: Up bandwidth	Down bandwidth
<input type="text" value="512"/> Kbit/s	<input type="text" value="2000"/> Kbit/s
WAN 2: Up bandwidth	Down bandwidth
<input type="text" value="512"/> Kbit/s	<input type="text" value="2000"/> Kbit/s

NE-480T+/490T+/R6000+ router will be in accordance with real upload bandwidth data that you input as a basis for automatic load balance ratio of two WAN ports. For example, when up bandwidth of two WAN circuits is 512Kbps, the automatic load balance ratio is 1:1. When up bandwidth of one circuit is 1024kbit/sec and up bandwidth of the other circuit is 512kbit/sec, the automatic load balance ratio is 2:1. Please input the real up bandwidth and down bandwidth in order that the router can realize load balance when the router reaches the real circuit.

3.7.2 Cable Detection

When using two WAN cables, you can enable this function to avoid the router misjudging the cable for disconnection caused by the excessive WAN flux. The router can automatically detect according to users' settings.

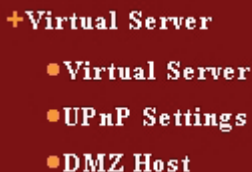
- **Detection times again:** Retry times detecting external linked PCs. The default value is 5. During the detection times again, if the internet hasn't responded, we can judge the external cable is interrupted
- **Response delay time:** Detection time (second) to external linked PCs. The default value is 30 seconds. After the setting time, please detect external linked PCs again.
- **Cable detection mechanism:** When ISP connection failing is detected, the system will only save this error information to syslog but it will remain to keep this cable not to be removed.
- **Default Gateway:** The gateway whose extranet IP can be obtained by the router.

- **ISP Server:** Enter ISP's DNS server etc. When setting the IP address, please ensure the IP address can respond fast and stably.
- **Remote Server:** Indicates remote network node detection locations which can response fast and stably (recommend to enter ISP's DNS IP).
- **Using DNS Server as domain name translation:** This field can be only allowed to enter websites such as www.google.com (Don't enter IP address). Besides, the field of both WAN cables can't be entered the same websites.

3.8 Virtual Server

In the "Virtual Server" drop-down menu, there are three sub-items including "Virtual Server", "UPnP Settings" and "DMZ Host". Click a certain sub-item, you are able to view and configure the corresponding function.

3.8.1 Virtual Server



Virtual Server is defined as a service port. All access to service of WAN will be reorientation to network server of LAN appointed by IP address.

Virtual Server

Virtual server define the mapping relationship between service port of WAN and network server of LAN. All access to service of WAN will be reorientation to network server of LAN appointed by IP address.

ID	WAN	Port sect	Private IP	Protocol	Enable	Delete
1.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
2.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
3.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
4.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
5.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
6.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
7.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
8.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
9.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>
10.	WAN 1			Both	<input type="checkbox"/>	<input type="checkbox"/>

Normal service port: DNS(53) Fill To ID 1

Save Cancel Help

- WAN ports: Select the number of WAN ports to be configured
- Service port section: LAN service port. This refers to the private service port which should be connected to the WAN service port.
- Private IP: Please input the internal host IP which requires to enable virtual service.
- Protocol: Please select protocol type of TCP/UDP/ALL for data transferring.
- Enable: After selecting “Enable”, all the settings of this item can take effect.
- Delete: Delete this rule.



Notice: Two WAN ports can't be configured the same rules.

3.8.2 UPnP Settings

NE-480T+/490T+/R6000+ supports the latest Universal Plug and Play. It will take effect under Windows ME/ Windows XP or above operating system (Remarks: The system should be integrated, and installed with Directx 9.0 or above version.), or under the software which supports UPnP. For example, a computer under Windows ME/Windows XP with MSN Messenger is able to use UPnP protocol when using voice-and-video.

UPnP Settings

Enable UPnP

UPnP Mapping Table

ID	Ext.Host	Ext.Port	Int.Host	Int.Port	Protocol	Description	WAN Port
----	----------	----------	----------	----------	----------	-------------	----------

Refresh

Save Cancel Help

- ID: Creates serial number of tables
- External Host: Receive or send the description of the response external host
- External Port: The router's port number for port switch
- Internal Host: Receive or send the description of the response internal host
- Internal port: The host port number for port switch
- Protocol: Indicates the port switch to TCP or UDP
- Lasting time: Indicates the time section to respond
- Description: Mapping port and software information

3.8.3 DMZ Host

Some programs require many connections such as Internet games, video meeting and Internet phone. Because the firewall of the router exists, these programs are not able to work under pure virtual services. In this case, you can set the computer as DMZ host.

DMZ

In some specially situation, a computer need to exposure entirely to WAN in order to ,please set the computer as DMZ host.


(Notice: The firewall setting related to the IP will abate if you set the DMZ host)

DMZ Host 1 IP: Enable

DMZ Host 2 IP: Enable

Save Cancel Help

Configuration steps: As above figure shown, at first, please input IP of LAN PC set as DMZ Host into the “DMZ Host IP”. Then please click “Enable” to complete the DMZ Host settings.

 **Notice:** The WAN and LAN firewall related to the IP will abate if you set the DMZ.


3.9 Security Settings

In “Security Settings” drop-down menu, there are seven sub-items including “Client Filter”, “URL Filter”, “MAC Filter”, “IP Filter”, “ARP Defense”, “Defense Attack”

and “Attack list”. We will give detail introduction as follows:



3.9.1 Client Filter

 Only after enabling “Client Filter”, other options can be displayed and configuration files to be set can come into effect.

- Filtering Mode: Select “Enable” or “Disable”. You can’t select both of them
- Disable: Just forbids the rules of data packets which are set to pass the router.

Other unlimited packets can pass the router. If selecting filtering mode "Disable", ten access policies will be forbidden.

Enable: Just allow the rules of data packets which are set to pass the router.

Other packets are forbidden to pass the router. If selecting filtering mode "Enable", ten access policies will be allowed

- **Access Policy:** Select the access police to be configured
- **Enable:** After selecting "Enable", this configuration file will take effect
- **Policy name:** The simple description of the configuration files' definition
- **LAN IP Section:** Enter IP addresses of controlled LAN PC. You can use IP address range
- **WAN Port Section:** Enter the ports to be controlled. You can specify a port range. When it is void, it specifies all the ports among 1-65535
- **Type:** Select all protocols used by controlled data packets ("All" includes TCP/UDP)
- **Time:** Enter the start time and end time when this rule is effective. If you don't set time, the default value will be 0, which indicates 24 hours
- **Date:** Select corresponding options according to your requirement
- **Save:** Complete settings

For example: If you hope the LAN PCs of IP address among 192.168.0.11-192.168.0.22 can not browse Web sites during 8:00 - 18:00 every week and the other computers are not limited, at this time, you need to specify filtering table of data packets as the below figure shown.

The screenshot shows the 'Client Filter' configuration window. It includes the following settings:

- Client Filtering Settings:** (checked)
- Filtering:** Disable, Enable (selected)
- Mode:** Disable, Enable (selected)
- Access Policy:** 10 (dropdown)
- Enable:** Delete the Policy (button: Clear)
- Policy Name:** office (text box)
- LAN IP sect:** 192.168.0.11 - 192.168.0.22 (text boxes)
- WAN port sect:** 80 - 80 (text boxes)
- Type:** Both (dropdown)
- Times:** 8 - 18 (dropdowns)
- Date:** Everyday, Sun, Mon, Tue, Wed, Thr, Fri, Sat (checkboxes)
- Buttons:** Save, Cancel, Help

3.9.2 URL Filtering



Only after enabling "URL Filter", other options can be displayed and configuration files to be set can come into effect.

The screenshot shows the 'URL Filter' configuration window. It includes the following settings:

- URL Filter Setting:** Enable
- Filtering:** Disable, Enable (selected)
- Mode:** Disable, Enable (selected)
- Access Policy:** (dropdown)
- Enable:** Delete the Policy (button: Clear)
- Policy Name:** (text box)
- Start IP:** 192.168.0. (text box)
- End IP:** 192.168.0. (text box)
- URL:** (text box)
- Times:** 0 - 0 (dropdowns)
- Date:** Everyday, Sun, Mon, Tue, Wed, Thr, Fri, Sat (checkboxes)
- Buttons:** Save, Cancel, Help

- **Filtering Mode:** Select “Enable” or “Disable”. You can’t select both of them.
Disable: Just forbids the rules of data packets which are set to pass the router. Other unlimited packets can pass the router. If selecting filtering mode “Disable”, ten access policies will be forbidden.
Enable: Just allow the rules of data packets which are set to pass the router. Other packets are forbidden to pass the router. If selecting filtering mode “Enable”, ten access policies will be allowed.
- **Access Policy:** Select the access policy to be configured. If you have already configured filtering requirement, please directly select configuration files.
- **Enable:** After clicking “Enable”, this configuration file will take effect
- **Policy name:** The simple description of the configuration files’ definition
- **Start IP:** Enter IP address of controlled LAN PCs
- **End IP:** Enter IP address of controlled LAN PCs
- **URL String:** Please input the filtered domain name or part of the filtered domain name.
- **Time:** Enter the start time and end time when this rule is effective. If you don’t set time, the default values will be 0, which indicates 24 hours.
- **Date:** Select corresponding options according to your requirement.
- **Save:** Complete settings

For example: If you hope the LAN PCs of IP address among 192.168.0.33~192.168.0.33 can't browse Web sites with "sex" string and the other PCs can normally browse Web sites with "sex" string, you need to specify filtering table of data packet as below figure shown.

3.9.3 MAC Filter



Only after enabling "URL Filter", other options can be displayed and configuration files to be set can come into effect.

- **Filtering Mode:** Select “Enable” or “Disable”. You can’t select both of them.
 Disable: Just forbids the rules of data packets which are set to pass the router. Other unlimited packets can pass the router. If selecting filtering mode “Disable”, ten access policies will be forbidden.
 Enable: Just allow the rules of data packets which are set to pass the router. Other packets are forbidden to pass the router. If selecting filtering mode “Enable”, ten access policies will be allowed.
- **Policy Name:** The simple description of the configuration files’ definition
- **MAC:** Enter MAC address that you want to control or select MAC address of manual setting.
- **Time:** Enter the start time and end time when this rule is effective. If you don’t set time, the default values will be 0, which indicates 24 hours.
- **Date:** Select corresponding options according to your requirement.
- **Save:** Complete settings
- **Delete:** Delete the corresponding rule

For example: If you hope the LAN PCs of MAC address 00:E0:38:03:10:50 can’t access the internet while the other LAN PCs can normally access the Internet, you need to specify filtering table of data packet as below figure shown.

MAC Filter

MAC Filtering Setting Enable

Filtering Mode Disable access the Internet
 Enable

Policy Name:

MAC:

Manual setting

Times: -

Date: Everyday Sun Mon Tue Wed Thu Fri Sat

Name	MAC	Times	Date	Delete
	00:E0:38:03:10:50	8:0-18:0	Everyday	<input type="button" value="Delete"/>

3.9.4 WAN IP filter

When you know WAN IP address or ports, you can forbid all the data into LAN to defense your network against WAN attack and hacker attack.

ID	WAN start IP	WAN end IP	Service port sect	Enable	Delete
1.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
9.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10.	<input type="text"/>	<input type="text"/>	<input type="text"/> - <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save Cancel Help

- ID: WAN IP filtering number
- WAN start IP and WAN end IP: Please input WAN start IP and WAN end IP that you need to control
- Service port section: please input WAN ports or port section that you want to control
- Enable: Enable the rules that have been set
- Delete: Delete the rules that have been set
- Protocol: Default setting is all protocols

For example: If you hope the LAN PCs can't access WAN IP address 58.60.112.222 and all ports (1-65535), you need to specify filtering table of data packet as below figure shown.

ID	WAN start IP	WAN end IP	Service port sect	Enable	Delete
1.	58.60.112.222	58.60.112.222	1 65535	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.				<input type="checkbox"/>	<input type="checkbox"/>
3.				<input type="checkbox"/>	<input type="checkbox"/>
4.				<input type="checkbox"/>	<input type="checkbox"/>
5.				<input type="checkbox"/>	<input type="checkbox"/>
6.				<input type="checkbox"/>	<input type="checkbox"/>
7.				<input type="checkbox"/>	<input type="checkbox"/>
8.				<input type="checkbox"/>	<input type="checkbox"/>
9.				<input type="checkbox"/>	<input type="checkbox"/>
10.				<input type="checkbox"/>	<input type="checkbox"/>

Save Cancel Help

3.10 QoS Settings

In the “QoS Settings” drop-down menu, there are two sub-items including “QoS Settings” and “QoS Rule”. Click a certain sub-item and you can view and configure the corresponding function.



3.10.1 QoS Settings

This page allows you to enable/disable QoS settings. Only after enabling QoS, the following QoS rules and bandwidth use rate of the running status will go into effect.

QoS Settings

This page allows you to enable/disable QoS settings. Only enable QoS is checked first, the following QoS rules selected will go into effect. Otherwise, the selected rules will work nothing.

Enable QoS


WAN 1:Upstream overall bandwidth Kbps

Downstream overall bandwidth Kbps

WAN 2:Upstream overall bandwidth Kbps

Downstream overall bandwidth Kbps

Save Cancel Help

- Enable QoS: After enabling, QoS rule and bandwidth use rate will go into effect.
- Upstream overall bandwidth: Enter real upstream speed value assigned by ISP.
- Downstream overall bandwidth: Enter real downstream speed value assigned by ISP.
- Unit: If ISP assigns upstream bandwidth 0.5M and downstream bandwidth 2M, after the unit conversion, you should enter upstream speed 512 Kbps and downstream speed 2048Kbps.
-  **Notice:** If WAN upstream and downstream overall bandwidth is entered by error, it will affect the accuracy of QoS rules and bandwidth use rate. If you are not clear, please inquire ISP.

3.10.2 QoS Rule

QoS rule includes QoS rule list and QoS rule configuration.

3.10.2.1 QoS Rule list

In QoS rule list, you can view all the rules created by users. Every rule item is

described as follows

- **ID:** Indicates the serial number of the rules
- **Remarks:** the remark information of this rule
- **IP Address Range:** IP address of LAN PCs to be controlled.
- **Protocol:** Includes All, TCP and UDP three options.
- **Port Range:** Enter port number or port range to be controlled
- **Mode:** Includes dedicated bandwidth and shared bandwidth. Dedicated bandwidth indicates the dedicated upstream and downstream bandwidth values separately owned by addresses or ports. Shared bandwidth indicates the shared upstream and downstream bandwidth values shared by addresses or ports.
- **Upstream bandwidth:** The maximum and minimum upload speed limit through WAN ports to be allowed. The default value is 0.
- **Downstream bandwidth:** The maximum and minimum download speed limit through WAN ports to be allowed. The default value is 0.
- **Enable:** The rule status
- **Configuration:** Edit or delete rules.

3.10.2.2 QoS Rule Configuration

In the QoS rule configuration, you can create or change the rules that have existed. The items to be configured as follows:

- **Enable:** After clicking it, this rule comes into effect.
- **Remarks:** The remark information of this rule
- **Address Range:** IP address of LAN PCs to be controlled.
- **Port Range:** Enter port number or port range to be controlled
- **Protocol:** Includes All, TCP and UDP three options.
- **Mode:** Includes dedicated bandwidth and shared bandwidth. Dedicated bandwidth indicates the dedicated upstream and downstream bandwidth values separately owned by addresses or ports. Shared bandwidth indicates the shared upstream and
- **Upstream bandwidth:** The maximum and minimum upload speed limit through WAN ports to be allowed. The default value is 0.
- **Downstream bandwidth:** The maximum and minimum download speed limit through WAN ports to be allowed.
- **Save:** Save the configuration information of this rule

3.11 LAN IP Control

In this page, you can set single PC's connection limit to PCs appointed IP addresses.

If over the connection limit, the new connection isn't allowed to pass the router.

However, the PCs which are not appointed IP addresses can establish the connection without limit.

LAN IP Control

Notice: no limit if the value is 0

Enable

Start IP	End IP	Connect Limit	Operation
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add

Save Help

- Enable: Enable LAN IP control function.
- Start IP and End IP: Enter PC IP address range or IP address to be controlled
- Connection Limit: The maximum connection that the computer allows.
- Operation: Add this rule to connection limit table.

For Example: You can configure as below figure shown, if you hope your limit PC IP address range is among 192.168.0.11-192.168.0.11 and the maximum connection is 200; or your limit PC IP address range is among 192.168.0.12-192.168.0.20 and the maximum connection is 150.

LAN IP Control

Notice: no limit if the value is 0

Enable

Start IP	End IP	Connect Limit	Operation
<input type="text"/>	<input type="text"/>	<input type="text"/>	<<Add
192.168.0.11	192.168.0.11	200	Delete
192.168.0.12	192.168.0.20	150	Delete

Save Help

3.12 ARP Bind

As below figure shown, this page sets match rule of single PC's MAC and IP, prevent other illegal IP and illegal MAC into the network, and prevent ARP cheat.

ARP bind indicates the appointed IP host whose MAC address and IP address should be the same is allowed to pass the router when sending the ARP request.

Otherwise, it is illegal and isn't allowed to use its ARP request through the router.

ARP Bind

This page set match rule of single PC's MAC and IP.

Note: For automatic bind turn to **Advanced Setting->Statistic** or directly **Load All**

Note: Only IP in following table can visit network when rules are enable.

ARP Bind Disable Enable

ID	LAN IP	MAC	Bind	reserve	Config
<div style="display: flex; justify-content: space-between;"> Add Item Enable Item </div> <div style="display: flex; justify-content: space-between;"> Delete All Search Item </div>					

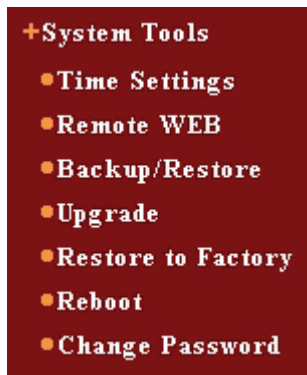
Refresh Help

- Load all: Only load IP and MAC address in the “Statistic” page. Add LAN IP and MAC address manually
- ARP Bind: Enable/disable IP and MAC bind. After clicking “Enable”, only IP and MAC address in the ARP bind table can access the Internet
- Add Item: Add new item in the static list
- Enable Item: Make all items in the static list come into effect
- Delete Item: Delete all the items in the static list
- Search Item: Search IP and MAC address items in the static list

3.13 System Tools

In the “System Tools” drop-down menu, there are seven sub-items including “Time Settings”, “Remote Web”, “Backup/Restore”, “Upgrade”, “Restore to Factory”,

“Reboot” and “Change Password”. Click a certain sub-item and you can configure the corresponding function. The detail information is described as follows:



3.13.1 Time Setting

Time setting

After setting the system timezone of router in this page, you can obtain standard GMT time from Internet.

Notice: When the router power is off, the time information will be lost and router will obtain GMT time automatically. You must set timezone in this page and connect Internet to obtain GMT time so the time restriction of other function for example can go into effect.

Enable periodic Calibration Calibration period: two hours

Time zone: (GMT+08:00)Beijing,China, Hong Kong,Singapore,Taipei

(Notice:only on Internet can obtain GMT time)

Please input date and time:

2007 Year 12 Month 21 Day 20 Hour 01 Minute 30 Second

You can set time zone by yourself and obtain standard GMT time from Internet. Only after connecting internet, you can obtain GMT time which you can enter manually.

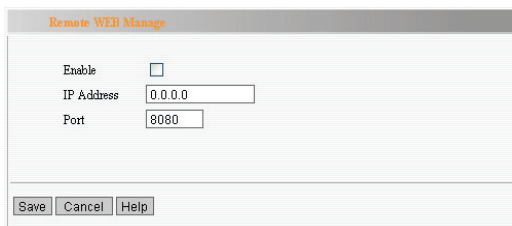
- Enable periodic Calibration: The system time can be obtained from network

automatically.

- Calibration period: The period that the system can calibrate from the network. According to your requirement, please select the corresponding calibration period. The system default value is 2 hours.
- Time zone: Select your local time zone.

3.13.2 Remote Web Manage

Generally speaking, only the LAN users can manage the router. If you have special requirement, this function can make you remotely manage your router.



Remote WEB Manage	
Enable	<input type="checkbox"/>
IP Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="8080"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	



Notice:

- 1、 According to your requirement, you can change your router's default remote manage. With the mode of 'IP address: "Port"' (e.g.: <http://192.168.0.1:8080>), you can log in router to execute remote management.
- 2、 The default IP of remote Web management is 0.0.0.0. When enabling this function, all WAN hosts can log in router and you can execute remote Web management. If you change the default IP (e.g.: changed into 58.60.111.221), only the host with specified IP (58.60.111.221) can log in Web management page.

3.13.3 Backup/Resume settings

Here, you can backup/restore current router's settings.

The screenshot shows a web interface titled "Backup/Resume settings". It contains the following elements:

- A header bar with the text "Backup/Resume settings" in orange.
- A main content area with the text: "You could backup or resume the router settings."
- A form with two input fields:
 - "Choose file name:" with the value "backup.bin" entered.
 - "Select TFTP Server:" with the value "192.168.0.100" entered.
- Two buttons at the bottom: "Backup" and "Resume".

The configuration steps for backup/restore settings:

- Log in our company's website and download TFTP Server application program, which will be saved into a fixed directory to run.
- Click "Backup" to generate a system backup file in the directory of TFTP program.
- In the same way, we just need to place the configuration files which require to be uploaded into the directory of TFTP. After clicking "Resume" and rebooting the router, the files can restore to the previous system configuration.

3.13.4 Software Upgrade


By upgrading router's software, you will obtain more stable router version and value-added routing function.

The screenshot shows a web interface titled "Upgrade". It contains the following elements:

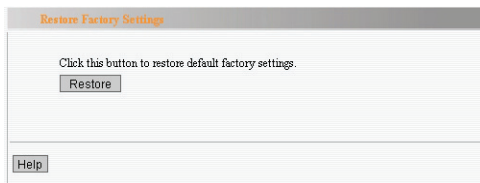
- A header bar with the text "Upgrade" in orange.
- A main content area with the text: "You may obtain new functions by upgrading router software."
- A form with three input fields:
 - "Select Firmware File:" with the value "upgrade.bin" entered.
 - "Select TFTP Server:" with the value "192.168.0.100" entered.
 - "Current Version:" with the value "Ver 1.0.0.1-Dec 21 2007 14:32:46" displayed.
- A notice block: "Notice: You can't shut down the router power when upgrading otherwise the router will be damaged. If upgrading succeed, the router will restart automatically. It will take some minutes to upgrade, please wait."
- Two buttons at the bottom: "Upgrade" and "Help".

The steps for software upgrade:

- Log in our company's website and download higher version software.
- Enable a TFTP Server of LAN PCs. Please using WinRAR, decompress the downloaded file and place it into the directory of the TFTP server.
- Please click "Upgrade" to have software upgrade.
- After upgrading, the router will restart automatically.

 Notice: You can't shut down the router power when upgrading. Otherwise, the router will be damaged. If upgrading succeeds, the router will restart automatically. It will take some minutes to upgrade, please wait.

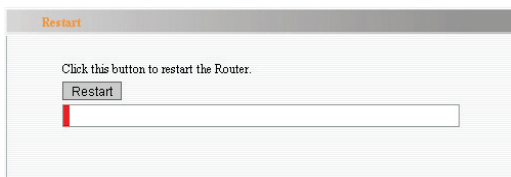
3.13.5 Restore Factory Settings



Click "Restore" button to restore factory settings. The detail information is described as follows:

- Default User Name: admin
- Default Password: admin
- Default IP: 192.168.0.1
- Default Subnet Mask: 255.255.255.0
- You should restart the router to take effect after restoring factory settings

3.13.6 Restart the Router




By clicking “Restart” button, some settings, which can become active after restarting the routers, will come into effect. Before the router restarts, the network connectivity will be disconnected automatically.

3.13.7 Change Password

A dialog box titled "Password" with a grey header. It contains five rows of labels and input fields: "Old User name" with the text "admin" in the field; "Old password" with a field of seven dots; "New User name" with an empty field; "New password" with a field of seven dots; and "Confirm new password" with a field of seven dots. At the bottom, there are three buttons: "Save", "Cancel", and "Help".

- In this page, you can change the user Name and password
- Please input your new user name, old password, and new password. Then click “Save”. The user name and password will be changed successfully if the password that you input is correct.

 **Notice:** Considering the security, we strongly recommend you to change the default user name and password.

3.14 System Log

In the “System Log” drop-down menu, there are three sub-items including “Log Settings”, “Log Configuration” and “Log Display”. Click a certain sub-item and you can configure the corresponding function. The detail information is described as follows:



3.14.1 Log Settings

This page sets syslog service to send the log generated by system to the syslog server of appointed PC, which is very convenient for users to view system information.

Log Settings

Enable Syslog

Syslog Server			
NO.	Enable	Host IP Address	Port
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="514"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="514"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="514"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="514"/>

Save Cancel Help

- Enable syslog: Select if you will enable syslog service

- **Enable:** Select if you will enable this syslog server
- **Host IP Address:** IP address of the syslog server
- **Port:** Protocol port of syslog service (default value: 514). According to the syslog server's setting port, you can change the port which must be consistent with syslog server

3.14.2 Log Configuration

In this page, you can configure the syslog display range. In the default situation, just display general log configuration. If you need more display information, please enable the options that you need.

Log Configuration

Alert Log

Syn Flooding ARP attack

Land Attack UDP Flooding

ARP cheat WinNuke

ICMP Flooding IP cheat

Port scan

General Log

System boot information DDNS updated information

Dynamic access information Time updated information

Static access information PPPoE dial-up information

3.14.3 Log Display

- In the system log, you can view all kinds of system situations after restarting. Besides you can view if there is network attack
- **Clear:** Clears system log

Log Display			
Index		Log Content	
1	2005-2-1 12:30:0	system	system init finish
2	2005-2-1 12:30:15	SYSTEME	update successful
3	2007-12-21 19:38:3	DHCPS	ACK[COA80064] to D268FE2000SNAKE[00-0A-E4-F5-82-7A]
4	2007-12-21 19:38:5	DHCPS	ACK[COA80064] to D268FE2000SNAKE[00-0A-E4-F5-82-7A]

3.15 Logout

After completing settings, click "Logout" to exit from Web management screen.