



Niveo Professional NR50

Multi WAN VPN Router

Manual v1.4

Copyright Statement

niveo is the registered trademark of Netstar Products BV. All the products and product names mentioned here are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Netstar Products BV. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Netstar Products BV. If you would like to know more about our product information, please visit our website at www.niveoprofessional.com.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Niveo Professional reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. Niveo Professional does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Warranty, complaints and return of goods

Niveo warrants that the goods delivered by it are free of design, material and manufacturing faults, such for a period of 12 months following delivery. The Warranty issued by Niveo will never exceed the Warranty issued by Niveo's own supplier in respect of the goods, such in full compliance with the relevant terms of Warranty of this supplier. The Warranty is not valid if the damage is the result of incorrect handling by the buyer and/or if the buyer has acted contrary to the instructions (of use) for the products. Without prejudice to the above, Niveo will never be held to extend its Warranty beyond replacement or crediting of the value of the faulty product delivered, such at the discretion of Niveo. The buyer will only have a right to replacement if it turns out impossible to repair the goods in question. Details of the Niveo Professional warranty can be found on www.niveoprofessional.com

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Niveo, (c) the product damage was caused by use with non-Niveo products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Niveo, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Niveo does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY NIVEO WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Niveo does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Niveo does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party’s service for which this product’s use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NIVEO BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF NIVEO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL NIVEO’ LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above l

Technical Support

Website: www.niveoprofessional.com

Tel: +31 (0)297 256 161

Email: support@niveoprofessional.com

Contents

Copyright Statement	I
Disclaimer	I
Technical Support	II
Contents	III
Chapter 1 Getting to Know Your Router	1
1 Product	1
2 Features	1
3 Specifications	2
4 Package	3
5 Hardware Description	3
Front Panel	3
Back Panel	4
Chapter 2 Quickly Installing Your Router	5
Step 1: Connect the Devices	5
Step 2: Configure Your Computer	5
Step 3: Configure Your Router	10
Login to the Web Manager	10
Basic Network Parameters Setting	12
Chapter 3 Advanced Settings	15
1 System Status	15
WAN Status	15
LAN Status	16
System Information	17
2 Setting Wizard	18
3 Network Parameters	18
LAN Setting	18
WAN Setting	19
1. WAN Port Setting	19

	DHCP Server	23
	Access Control	26
	Port Parameters Setting	28
4	Filter Setting	31
	Group Setting.....	31
	Port Filter	34
	URL Filter	36
	Bandwidth Setting.....	38
5	Security Setting	40
	MAC Address Filter	40
	Attack Defence	42
	IP-MAC Binding.....	44
6	Advanced.....	46
	Virtual Server	46
	DMZ	48
	UPnP	49
	DDNS.....	50
	Route Table	51
	E-bulletin	52
	Mail BCC	53
	Address Masquerading	54
7	VPN Setting	55
	PPTP & L2TP Clients.....	56
	PPTP & L2TP Servers.....	58
	Certificate Management	64
	IPSEC.....	69
8	System Monitoring.....	81
	Traffic Statistics	81
	Log Viewing	81
	Log Setting.....	82

9	System Tools	84
	Date and Time	84
	Software Upgrade	85
	Backup and Restore	85
	Restore Factory Default	86
	User Name and Password	87
	Reboot	87
	Appendix 1: Commands Introduction	89
	Appendix 2: Safety Statement & Emissions	90

Chapter 1 Getting to Know Your Router

1 Product

Niveo Professional Multi-WAN VPN Router is a new-generation hardware network access device. Multiple load balance VPN termination and flexible bandwidth control ensure a stable networking environment.

2 Features

- Complies with IEEE 802.3, IEEE 802.3u, IEEE 802.3ab and IEEE 802.3x standards, etc.
- CPU capability is up to 550MHz; Perfect NAT forwarding performance, allowing more access.
- Supports multiple access, intelligent load balance (which can be set according to a certain ratio)
- Provides one 10/100M/1000M auto-negotiation Ethernet (WAN) interface, to connect the exterior network.
- Provides three 10/100M/1000M auto-negotiation Ethernet (WAN/LAN) interfaces, which can be switched as a WAN/LAN interface when needed.
- Provides one 10/100M/1000M auto-negotiation Ethernet (LAN) interfaces to connect the interior LAN.
- Supports Access Control on the LAN/WAN interface, and allows the host with the specified address to manage the Router via SSL.
- Builds up the DHCP Server within the Router, which supports static IP address assignment.
- Supports MAC Address Clone.
- Supports Interface Mode, in which users can select different WAN interface negotiation mode when needed.
- Supports Interface Mirroring
- Builds up Firewall to accurately control the Internet Surfing time; supports Clients Filtering, MAC Filtering, and URL Filtering.
- Supports Website Classification filtering, which is more convenient for the management of domains.
- Supports IP-MAC Address Binding, to prevent the Router from ARP Attacks, ARP Disguising and Non-authorization Users Access.
- Supports Attack-defense, to assure the network of safety and stability.
- Supports Multiple Virtual Server and DMZ hosts.

- Supports UPnP and DDNS (Dynamic Domain Name Analysis) and Static Routing.
- Supports BBS
- Supports UPnP for users to configure any IP to connect to the Internet.
- Supports Mail BCC
- Supports Address Masquerading.
- Supports PPTP/L2TP/IPsec VPN Server, and support 15 groups of users accessing the Router at the same time.
- Offers System Logs and Traffic Statistics.
- Supports Configuration File Backup and Restore.

3 Specifications

Standards & Protocols		IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, TCP/IP, DHCP, ARP, NAT, PPPoE, SNTP, HTTP, DNS, ICMP
Network Medium		10Base-T: Cat. 3 or higher UTP 100Base-TX: Cat. 5 UTP 1000Base-T: Cat. 5e UTP
Interface & LEDs	WAN/LAN Interface	3 “WAN/LAN” LED indicators and 3 “1000M” LED Indicators
	WAN Interface	1 “WAN” LED indicator and 1 “1000M” LED Indicator
	LAN Interface	1 “LAN” LED indicator and 1 “1000M” LED Indicator
	Others	Power (Power LED), SYS (System Status LED)
Size(L * W * H)		440mm*209mm*44mm
Environment		Operating Temperature: 0°C~45°C; Storage Temperature: -30°C~70°C; Operating Humidity: 10%~90% RH non-condensing; Storage Humidity: 10%~90% RH non-condensing.
Power & Consumption		Input: AC 110V / 220V 50Hz Consumption: Up to 24W

4 Package

Open the package once you get it. Verify the following items. Note that if there’s any item not covered here, contact your local reseller.

- NW50 Router
- One Power Cord
- One Manual CD
- Two L-shaped Mounts
- Four Footsteps

5 Hardware Description

Front Panel



LED Indicator

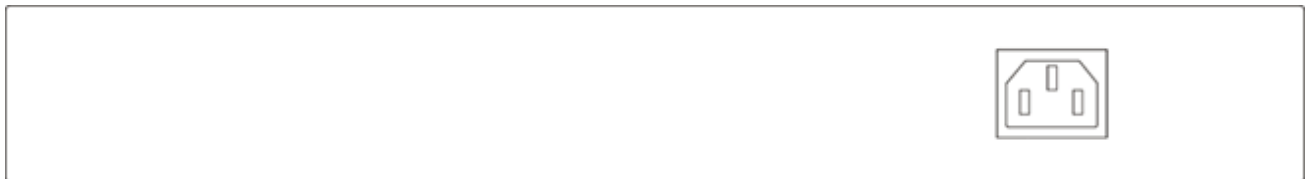
LED Indicator	Status	Indication
Power	On	The power supply is OK.
SYS	Blinking	The system is OK.
	On/Off	The system is not proper.
ACT	On	The corresponding interface is connected.
	Blinking	The corresponding interface is transmitting data.
	Off	The corresponding interface is not connected.
100/1000M	On/Blinking (Green)	The corresponding interface is under 1000M mode.
	On/Blinking (Orange)	The corresponding interface is under 100M mode.

Interface & Button

Interface	Description	Indication
WAN	The Router has 4 Gigabit WAN interfaces (RJ45), of which 3 ones can be set as the LAN interfaces.	Used for connecting the Router to the Internet.
LAN	The Router has 4 Gigabit LAN interfaces (RJ45), of which 3 ones can be set as the WAN interfaces.	Used for connecting the Router to your computer, or for stacking to a hub/switch.
Reset	Like a pin-hole on the front panel	Pressing the Reset button with a needle for over 7 seconds to restore the Router to factory defaults. Then the Router will automatically restart.

Back Panel

Power Interface: Used for connecting to the power adapter to supply power to the Router.



Chapter 2 Quickly Installing Your Router

Step 1: Connect the Devices



Tip:

1. Before installing the Router, ensure that the broadband service is fine and you can access the Internet by directly connecting the Ethernet cable from the incoming Internet side to your computer, or connect to the gateway provided by your ISP; if you cannot, consult your network ISP to help you out.
2. For your safety, when installing, keep your hands dry and unplug the power plug by using both your hands.
3. Do not expose the Router to moist and dust.

Install the Router under the following guidelines:

- 1 Connect your hub/switch/computer in LAN to the LAN interface of the Router, for connecting to the Intranet.
- 2 Connect the xDSL/Ethernet cable to the WAN interface of your Router, for connecting to the Internet.
- 3 Connect the power adapter cord to the power socket of your Router and to the power plug beside the Router.

Step 2: Configure Your Computer

Power up the Router. When the system LED starts blinking regularly, indicating the Router is working, you can begin to set the Router.

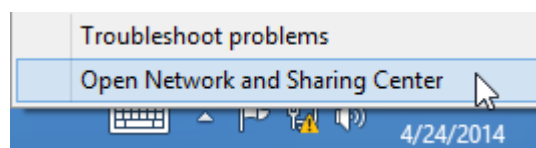
Connect your computer to one of the LAN interfaces of the Router via an Ethernet cable. Configure the Network of your computer and access the Internet.



Settings here take Win8 operation system as an example. Settings in Win7 operation system are similar to this.

- 1 Click the icon  on the bottom right corner of your desktop.

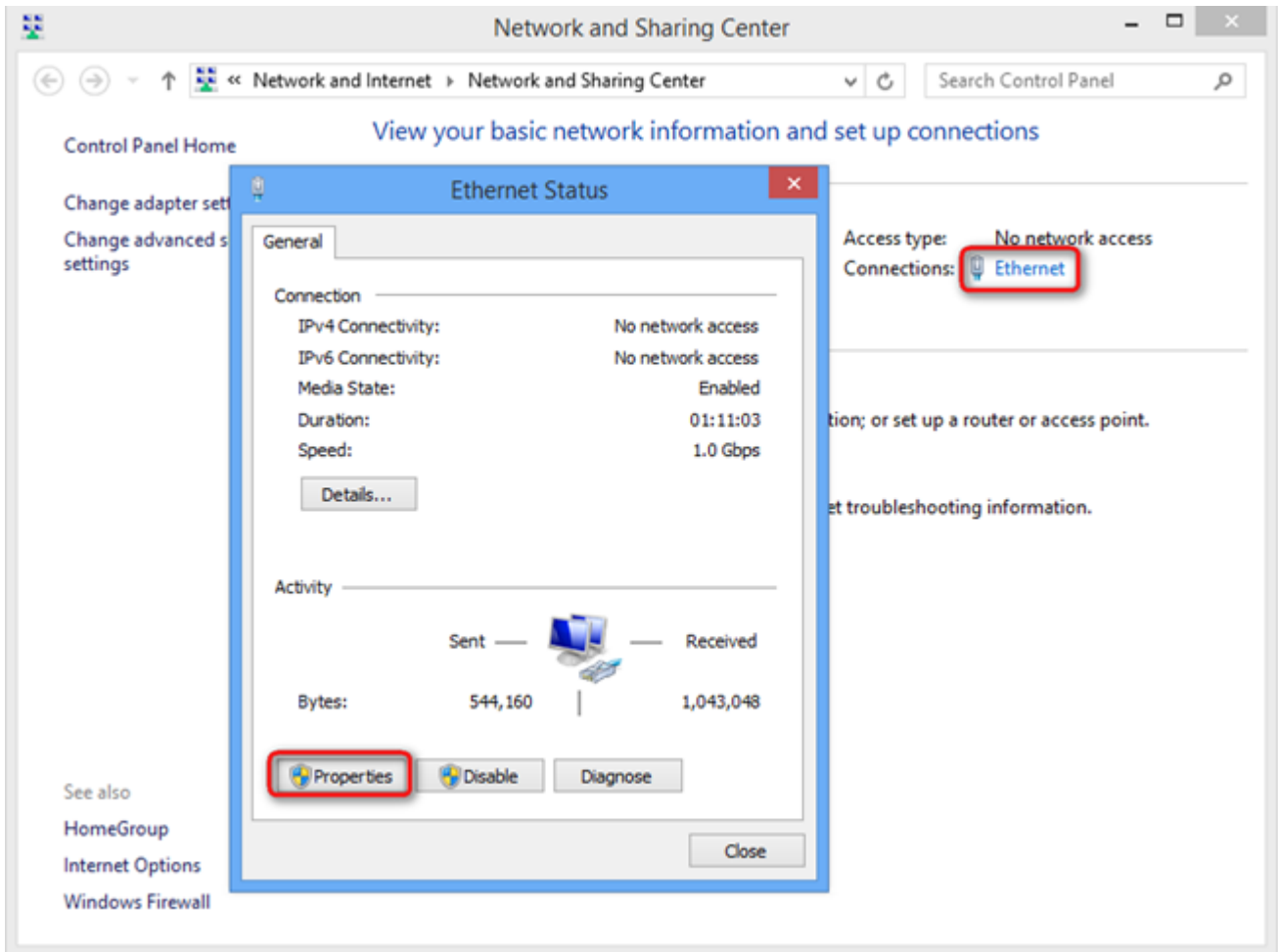


- 2 Click **Open Network and Sharing Center**.

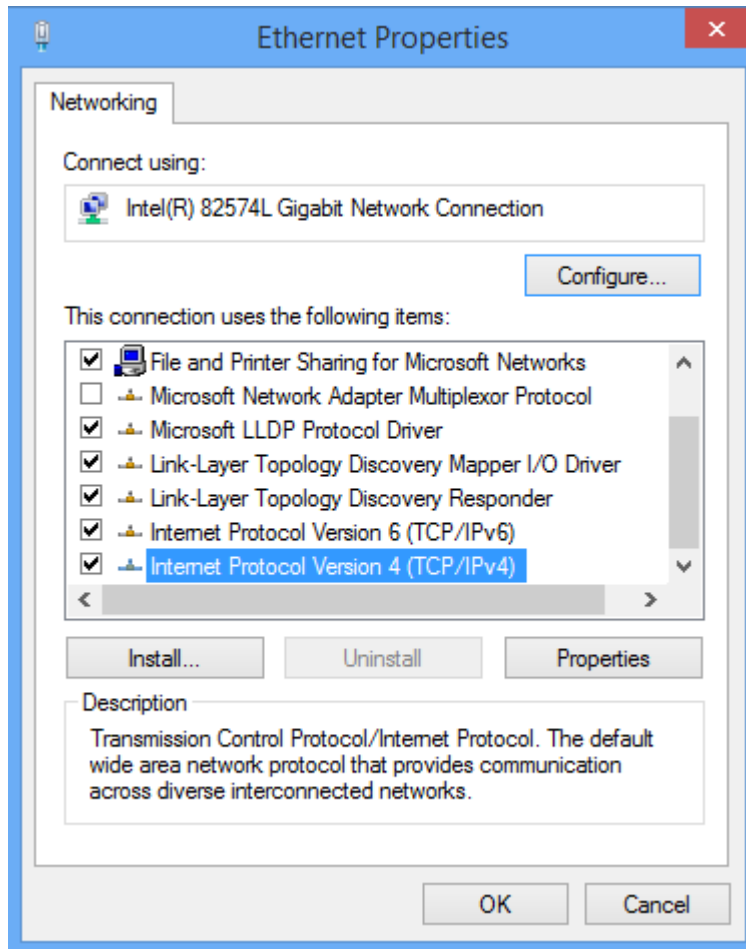


 **Tip:** If you cannot find the icon  on the bottom right corner of your desktop, follow steps below: Right click **Start** -> Click **Control Panel** -> **Network and Internet** -> **Network and Sharing Center**.

3 Click **Ethernet** -> **Properties**.

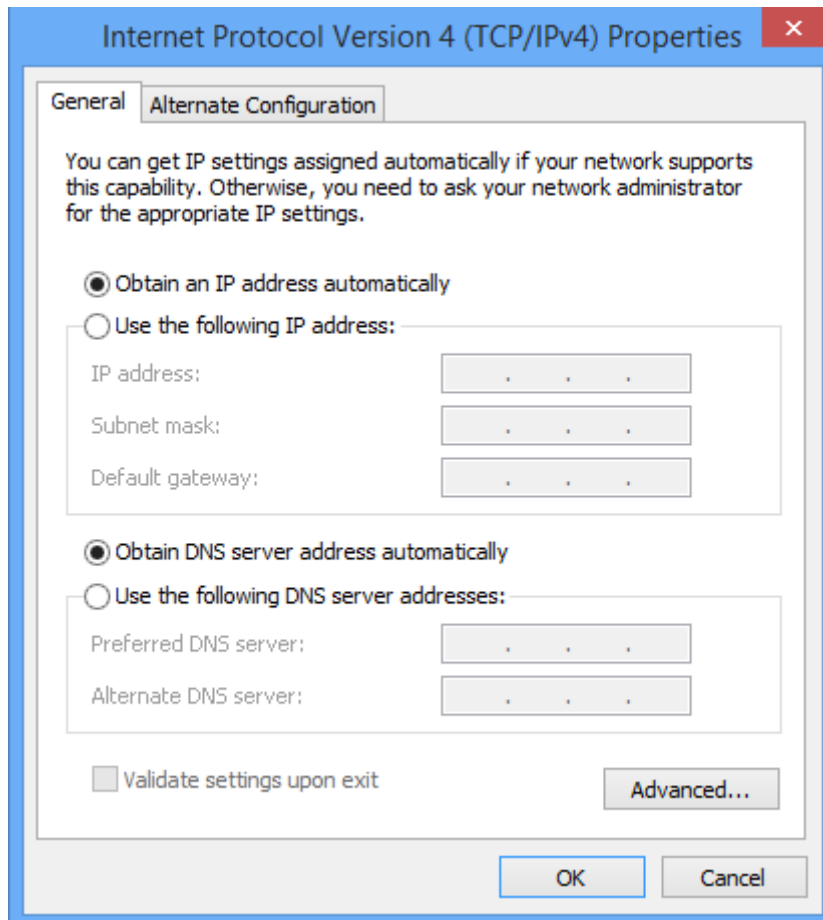


- 4 Find and double click **Internet Protocol Version 4(TCP/IPv4)**.

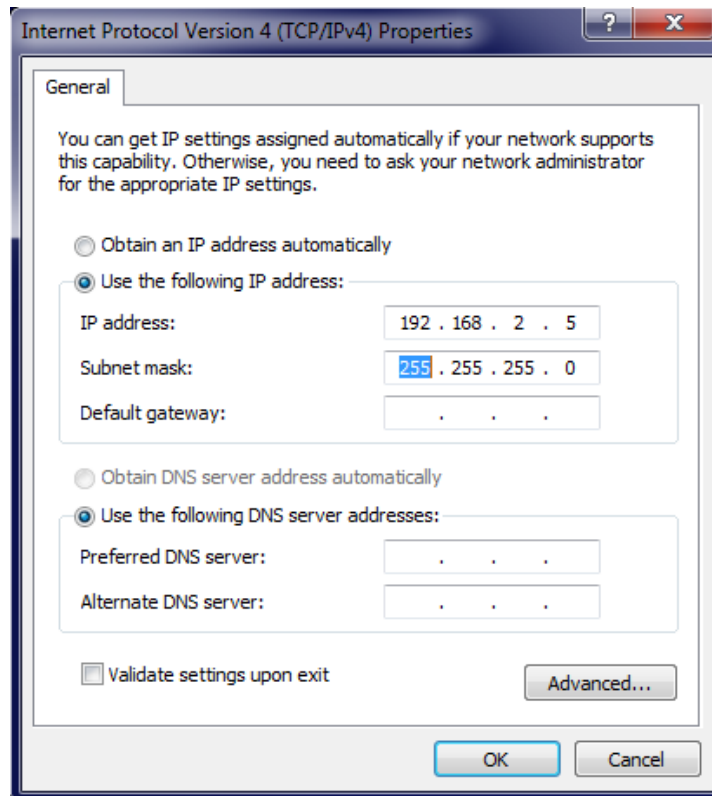


- 5 On the following screen, you can select to obtain an IP automatically or to use the IP address you set manually.

- **Method 1:** Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



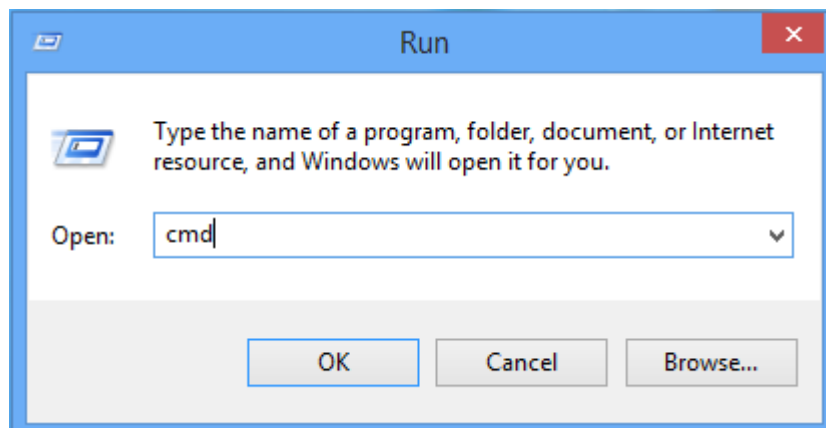
- **Method 2:** Select **Use the following IP address**, IP address: **192.168.2.x** (2~254); Subnet mask: **255.255.255.0**; Default gateway: 192.168.2.254, Preferred DNS server (consult your network ISP for specific data) and click **OK**.



6 Click **OK** on the **Local Area Connection Properties** window (see 4 for the screenshot).

After the configuration above, launch Ping Command to check the connection between your computer and the Router as followings.

1 Right click **Start**-> Click **Run**, input **cmd** in the **Open** field, and then press **OK**.



2 Input ping 192.168.2.254 and press Enter.

➤ If there're responses shown as the figure below, it means your computer and the Router connects well.

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.2.254
Pingen naar 192.168.2.254 met 32 byte gegevens:
Antwoord van 192.168.2.254: bytes=32 tijd<1 ms TTL=64
Antwoord van 192.168.2.254: bytes=32 tijd<1 ms TTL=64
Antwoord van 192.168.2.254: bytes=32 tijd<1 ms TTL=64
Antwoord van 192.168.2.254: bytes=32 tijd<1 ms TTL=64
Ping-statistieken voor 192.168.2.254:
    Pakketten: verzonden = 4, ontvangen = 4, verloren = 0
    (<0% verlies>). De gemiddelde tijd voor het uitvoeren van één bewerking in milliseconden:
    Minimum = 0ms, Maximum = 0ms, Gemiddelde = 0ms
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
  
```

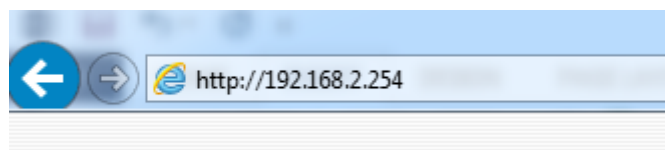
- If not, it's recommended to check:
 - Whether the Router is powered on;
 - Whether your computer and the Router are well-connected;
 - Whether the TCP/IP parameters on your computer are configured correctly.

Step 3: Configure Your Router

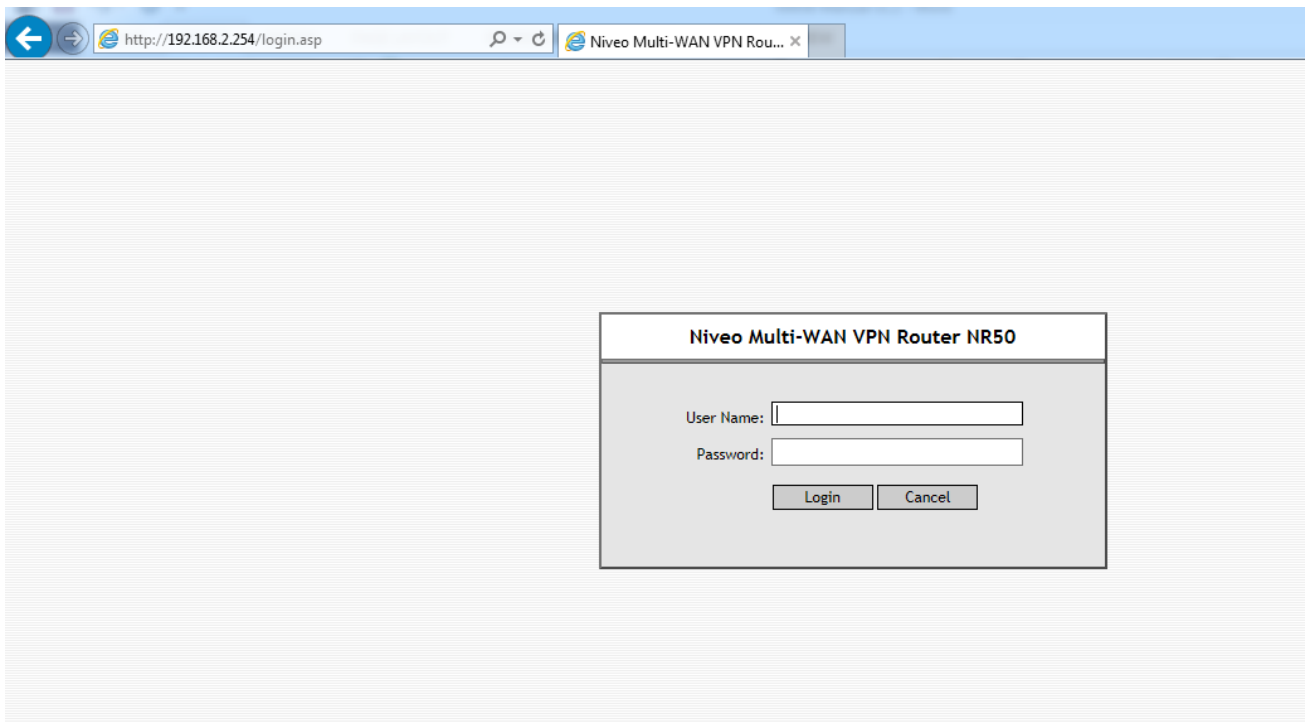
Login to the Web Manager

The Router is configured on a browser, which is also adaptive to the work plane of MS Windows, Macintosh or UNIX. Launch the Web Browser.

- 1 Input **http://192.168.2.254**, and press **Enter**.



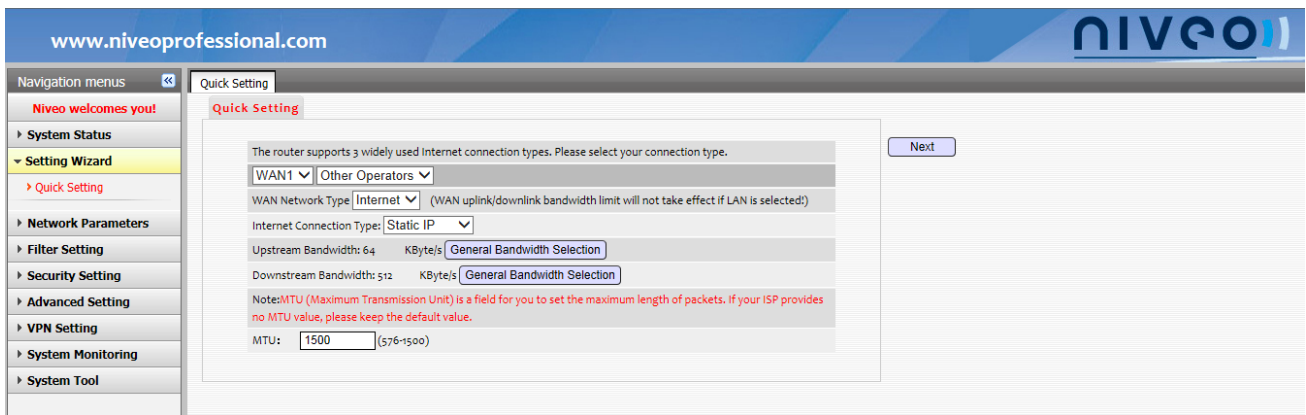
- 2 After the connection is created, and then the login interface will prompt. You need to login to the web manager of the Router and input the user name and login password (by default both are **admin**).



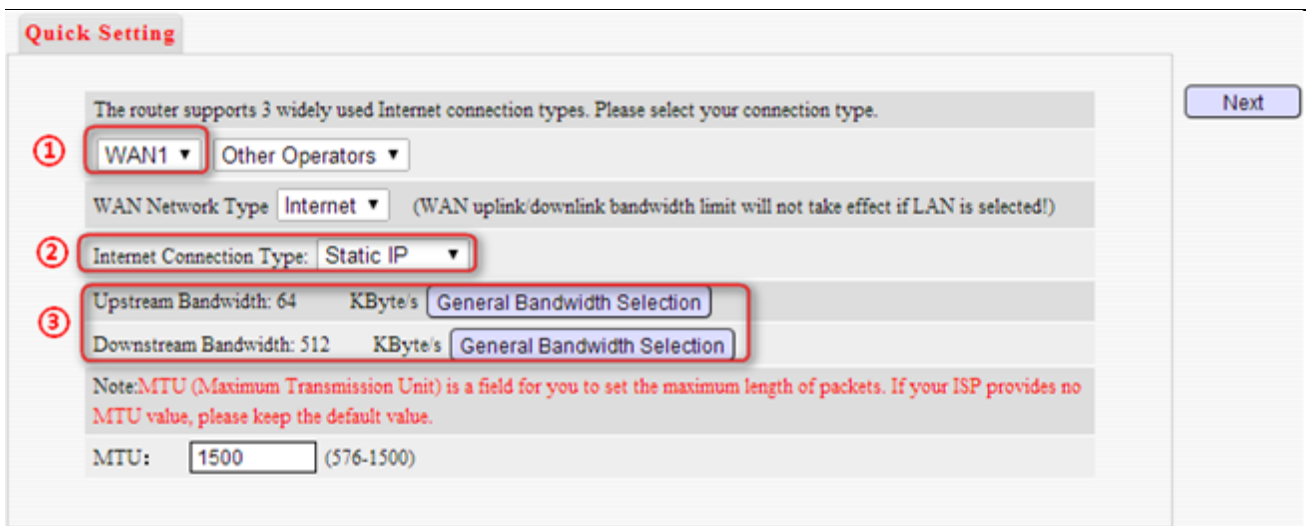
⚠ Note:

- 1 For security of the Router, go to **System Tool-> User Name and Password** to change the default user name and password after you login to it at the first time.
- 2 By default WAN1/LAN4 and WAN2/LAN3 on the front panel of your Router are WAN interfaces, WAN3/LAN3 and WAN4/LAN1 are LAN interfaces. If you connect your Ethernet cable from the Internet side to WAN3/LAN3 or WAN4/LAN1 interface, before configuring your Internet connection, you need to go to **Network Parameters-> Port Parameters Setting-> WAN Port Setting** to set the WAN ports you want to enable. For example, you connect your Ethernet cable to WAN3/LAN3, you need to select 3 or 4 from the pull-down menu.

3 On the following interface, click **Setting Wizard-> Quick Setting**, to configure your Internet connection.



Basic Network Parameters Setting



1 Select WAN1/2/3/4 as the WAN port from the pull-down menu.

You can start to configure the WAN interface according to your needs as long as you select one interface as the WAN port from the four interfaces on the front panel firstly. The selected interface should be the one you connect to the Internet with an Ethernet cable. Only WAN1 and WAN2 are here on the pull-down menu. If you enable WAN3/LAN3 or WAN4/LAN1 interface as the WAN port, the pull-down menu will have WAN1, WAN2, WAN3 or WAN4.

2 Select your access type from the pull-down menu.

You need to select the right ISP according to your actual Internet service.

Three Internet connection types are supported on the Router. Dynamic IP is the default connection type.

- **Dynamic IP:** Select this type without entering any IP information, you can still get the IP address automatically assigned by the network ISP.
- **Static IP:** Select this type if your ISP offers you static IP information, by entering which you can access the Internet.
- **PPPoE:** Select this type if you use PPPoE dail-up to access the Internet.

3 Select proper Upstream and Downstream bandwidths from the General Bandwidth Selection windows.

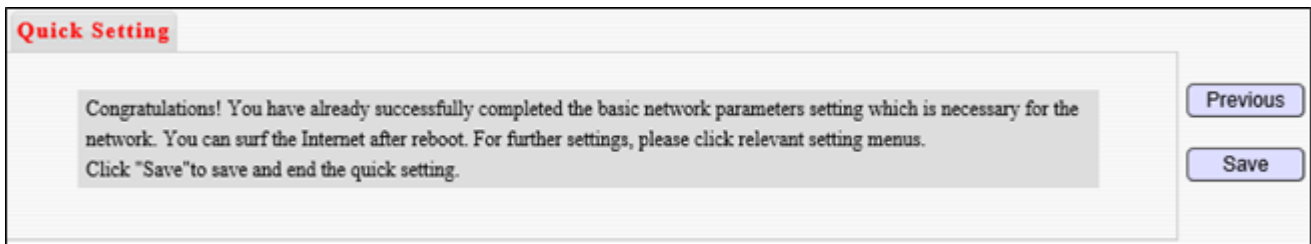
The bandwidth unit is KByte/s. Assume your ISP offers 2M bandwidth under PPPoE mode, the Upload speed is 512Kbps, the Download speed is 2Mbps. The unit switchover is as the followings:

Upload speed: 512Kbps = 64KByte/s

Download speed: 2Mbps = 2048Kbps = 256KByte/s

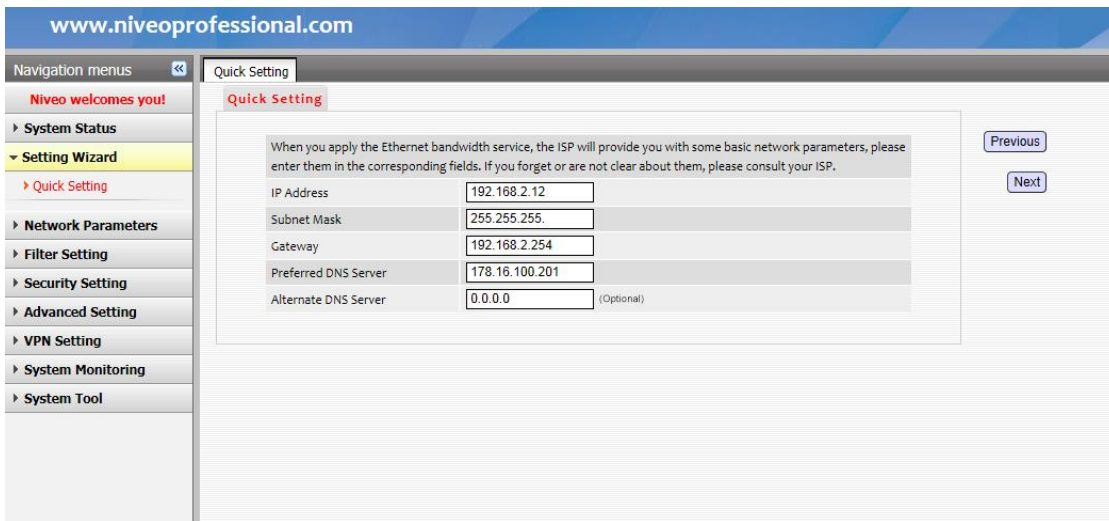
4 Click Next to input network parameters for accessing the Internet.

- If you select **DHCP** in step 2, the following interface will be displayed.



Just click **Save** to save the previous settings.

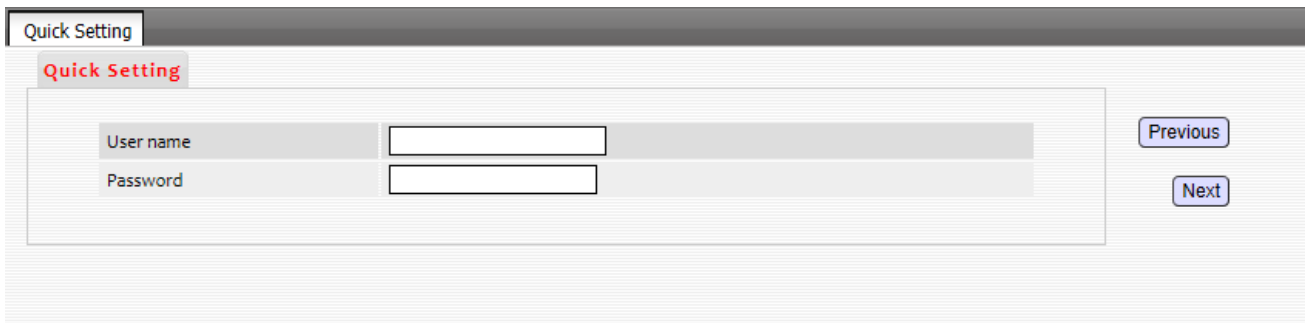
➤ If you select **Static IP** in step 2, the following interface will be displayed. Parameters here are examples.



Your network information will be provided by your ISP, including IP Address, Subnet Mask, Gateway and Preferred DNS Server as well as Alternative DNS Server. Just click **Save** after you finish the setting.

Note that WAN IP and the LAN IP of your Router should not be in the same network segment. In emergency, Press the Reset button with a needle in the front panel to restore the Router to factory default.

➤ If you select **PPPoE** in step 2, the following interface will be displayed. Parameters here are examples.



The User name and Password will be provided by your ISP. Just click **Save** after you finish the setting.

Chapter 3 Advanced Settings

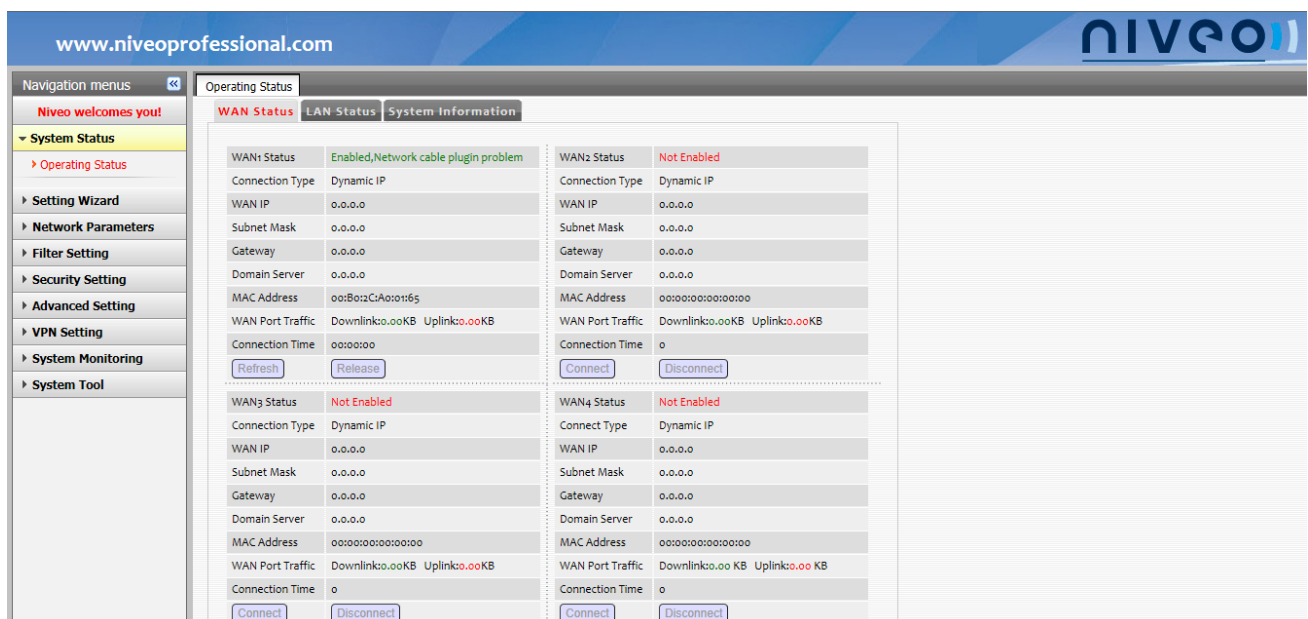
This chapter helps you to configure each function on the Web interface for you to easily use and manage the Router. The following 9 functions with their configurations will be introduced. If you have any questions when configuring the Router, simply click the **Help** button.

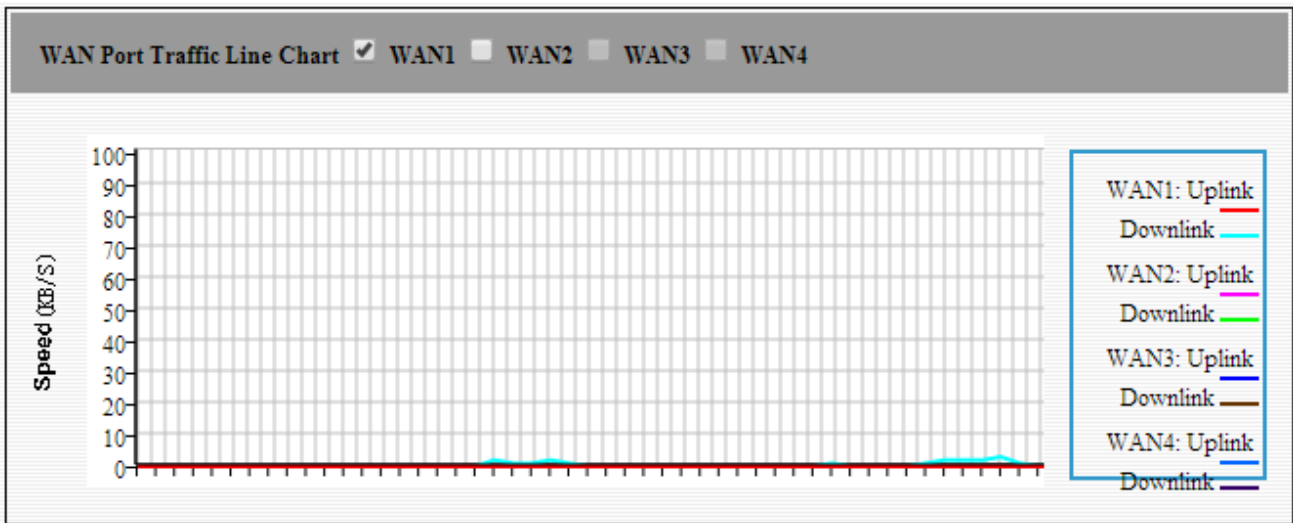
➤ System Status	Operating Status
➤ Setting Wizard	Quick Setting
➤ Network Parameters	LAN Setting, WAN Setting, DHCP Server, Access Control, Port Parameters Setting
➤ Filter Setting	Group Setting, Client Filter, URL Filter, Bandwidth Setting
➤ Security Setting	MAC Address Filter, Attack Defence, IP-MAC Address Binding
➤ Advanced Setting	Virtual Server, DMZ, UPnP, DDNS, Route Table, Electronic Bulletin, UPnP, Mail BCC, Address Masquerading
➤ VPN Setting	PPTP-L2TP Client, PPTP-L2TP Server, Certificate Management, IPSEC
➤ System Monitoring	Traffic Statistics, Log Viewing, Log Setting
➤ System Tool	Date and Time, Software and Upgrade, Backup and Restore, Restore Factory Default, User Name and Password, Reboot.

1 System Status

WAN Status

Click **System Status->Operating Status->WAN Status** to view the current connection status on WAN interfaces, WAN IP address, Subnet mask and Gateway.

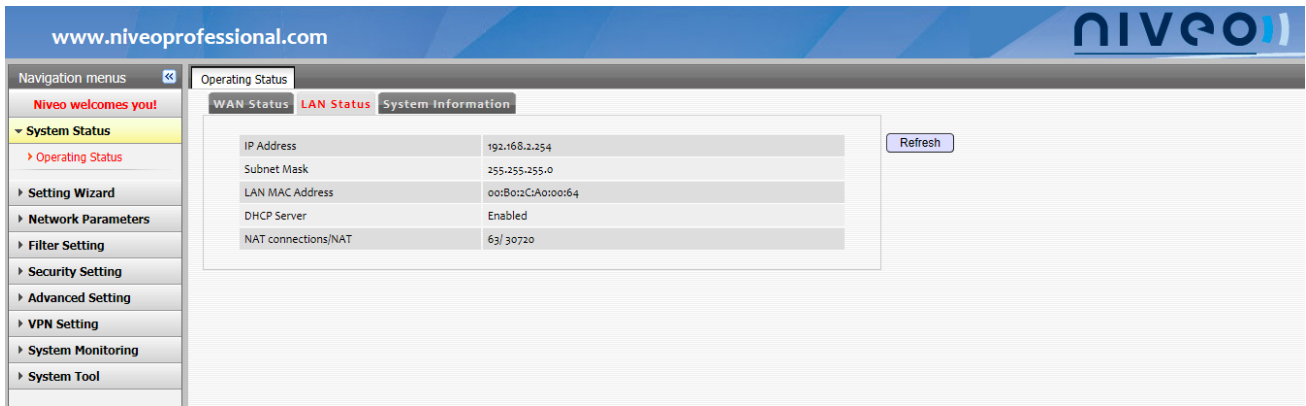




- **WAN Status:** Connection status of WAN interfaces
 - Enabled, Network cable plugin problem** ↔ This WAN interface is disconnected.
 - Enabled, Connecting** ↔ This WAN interface is connecting to the Internet and is obtaining the IP address.
 - Enabled, Connected** ↔ This WAN interface is connected to the Internet, i.e. the Router connected to the Internet.
- **Connection Ways:** Your current access mode, Dynamic IP, Static IP, or PPPoE.
- **WAN IP, Subnet Mask, Gateway and Domain Server (i.e. the Preferred Server):** Information provided by your ISP.
- **MAC Address:** The MAC address of the WAN interface.
- **WAN Port Traffic:** The bandwidth (KB/s) used on the Router.
- **Connection Time:** The time range after the Router is connected to the ISP (just for Dynamic IP and PPPoE).

LAN Status

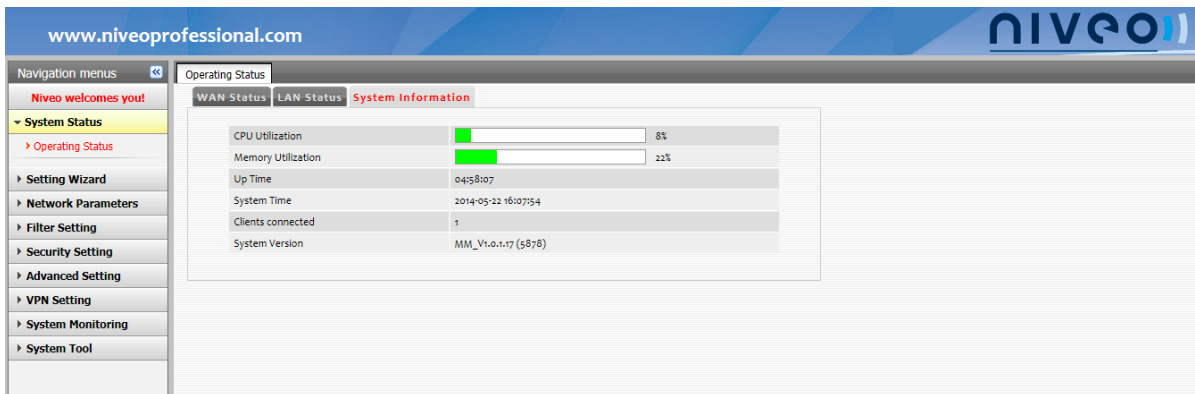
Click **System Status->Operating Status->LAN Status** to view the current IP Address of the Router, together with Subnet mask, LAN MAC Address, DHCP Server and NAT connection number/NAT, shown as the following.



- **IP Address:** The current Router’s IP address.
- **Subnet Mask:** The current Router’s Subnet Mask.
- **LAN MAC Address:** The Router’s LAN MAC address.
- **DHCP Server:** To show the DHCP server is disabled or enabled.
- **NAT Connections/NAT:** The NAT connection number and the total NAT connection numbers.

System Information

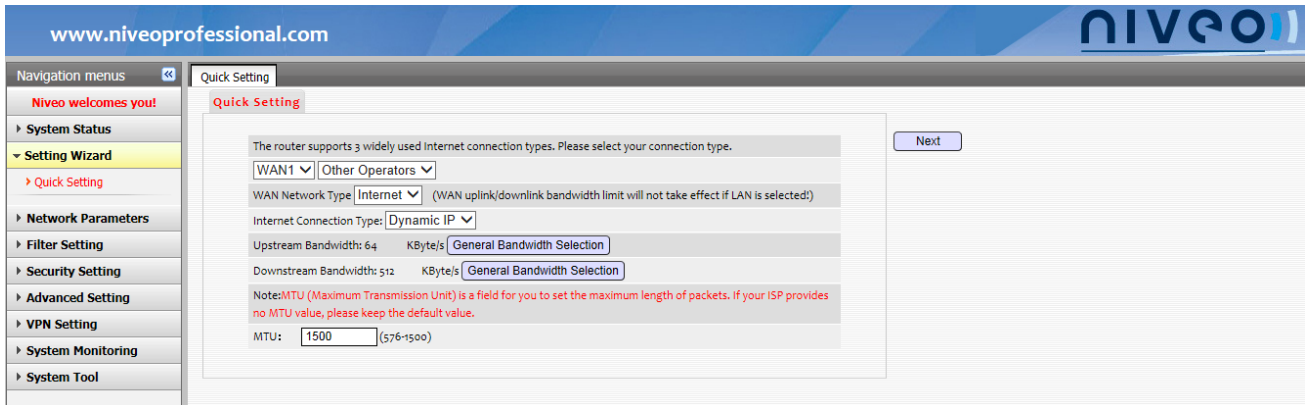
Click **System Status->Operating Status->System Information** to view the Router’s CPU Utilization, Memory Utilization, UP Time, System Time, Clients connected, and the System Version, shown as below.



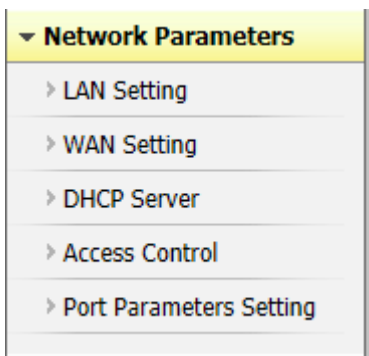
- **Router’s CPU Utilization, Memory Utilization:** The current status of the Router
- **UP Time:** The work time of the system since it started.
- **System Time:** The system renew time.
- **Clients connected:** The number of connected computers or other devices.
- **System Version:** The software version of the Router.

2 Setting Wizard

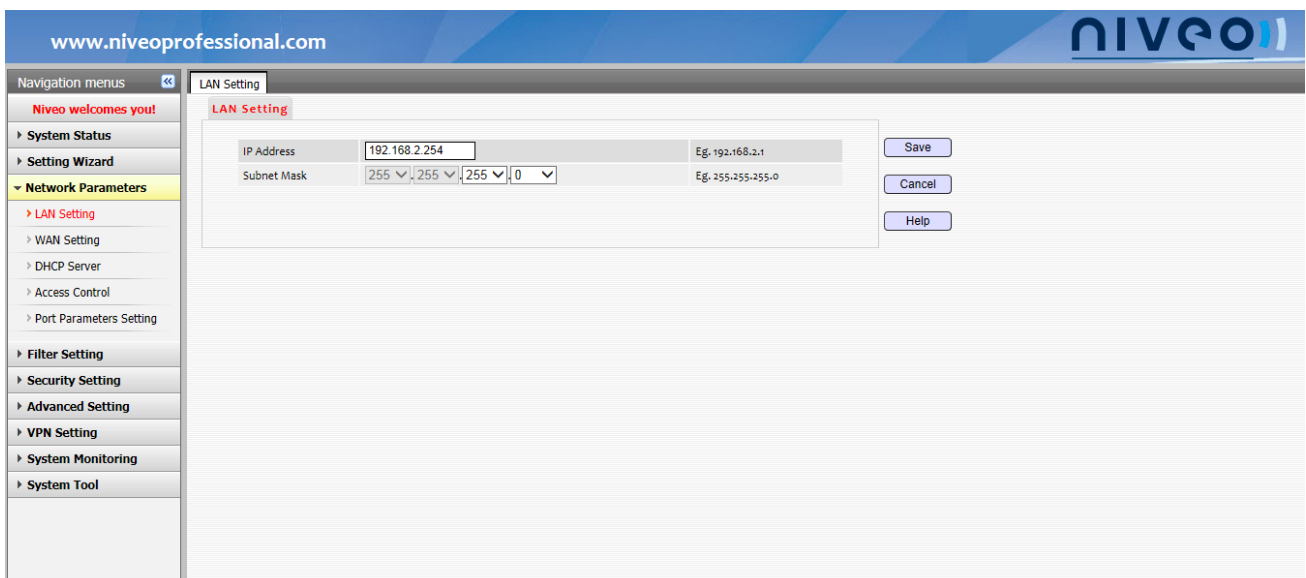
Click **Setting Wizard->Quick Setting**, to set the basic information for the Router, configuration details mentioned before on **Chapter 2->Step 3->2. Basic Network Parameters Setting**.



3 Network Parameters



LAN Setting



1 **IP Address:** Input the LAN IP address you want when needed, i.e., change the default value 192.168.2.254 into a new IP address.

2 **Subnet Mask:** Set the LAN subnet mask.

3 **Save:** Click to save the current setting on the interface.

Cancel: Click to cancel the setting you did just now and restore the parameters to the default setting.

Note:

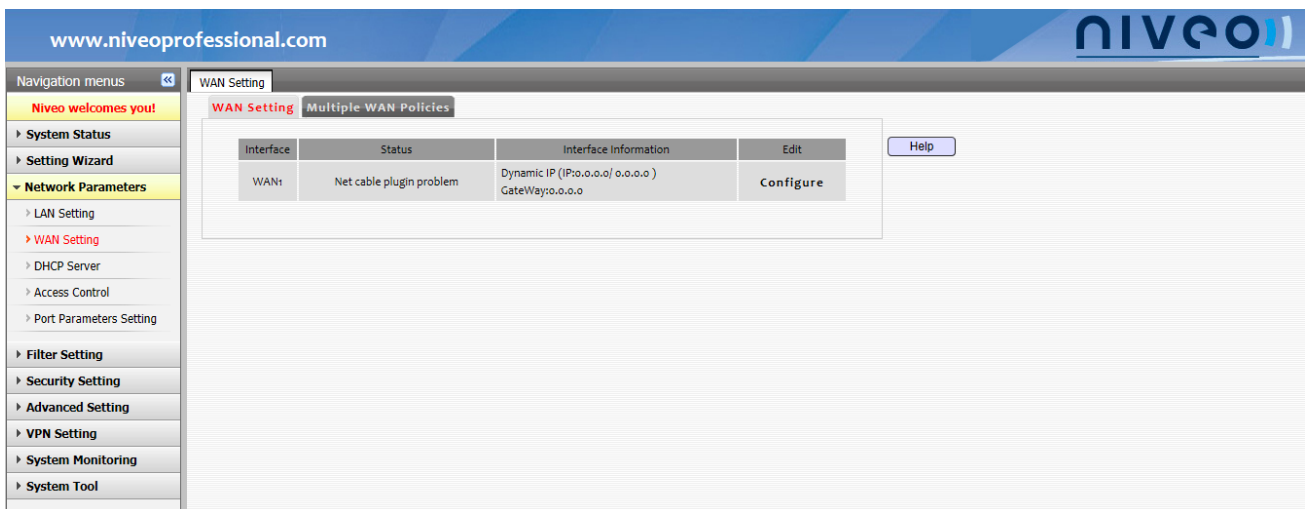
1. If you change the LAN IP address, and you save rebooted the Router, you need to reenter the Router web management interface by using the new IP address you have previously set.
2. Meanwhile, computers on the downlink of the Router need to be set a default gateway that's the same with this new IP address you have set.
3. **Note that** WAN IP and the LAN IP of your Router should not be in the same network segment. In emergency, Press the Reset button with a needle in the front panel to restore the Router to factory default.

WAN Setting

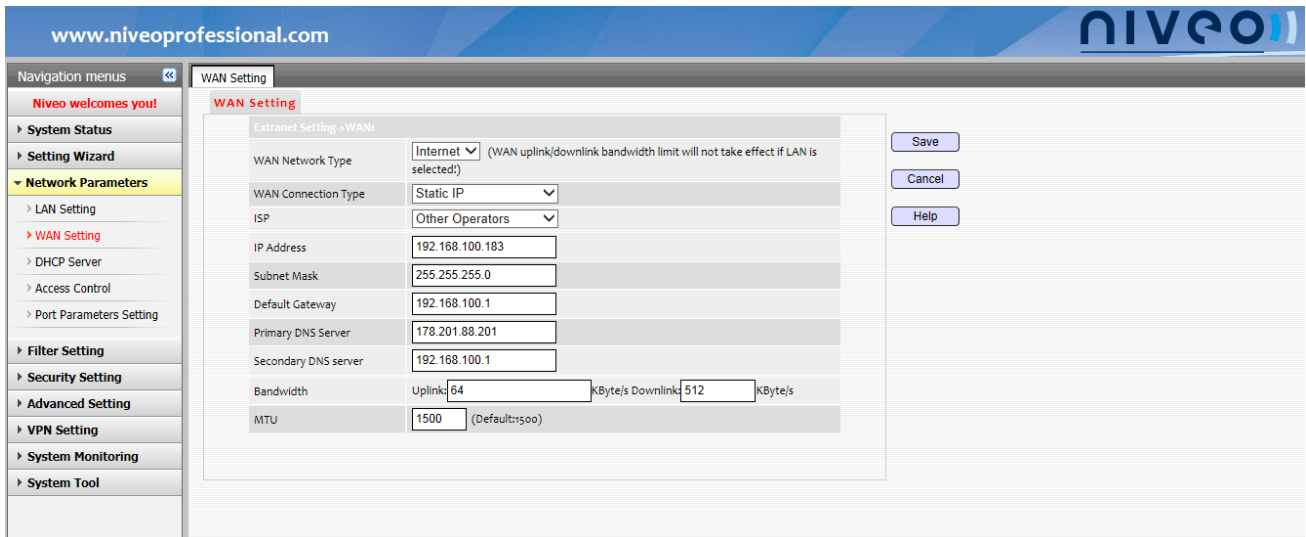
1. WAN Port Setting

To configure each WAN port to connect to the Internet according to their actual ISPs,

1 Click **Network Parameters->WAN Setting->WAN Setting**.



2 Select the WAN interface you want to configure and click **Configure** to enter the setting interface.



3 WAN Port: Select **Internet** if your WAN interface is accessing to the Internet; if not, select **LAN**.

ISP: Select the ISP of your WAN port.

4 WAN Port Type: Select the network connection type of the WAN port from the pull-down menu, **Static IP**, **Dynamic IP** or **PPPoE**.

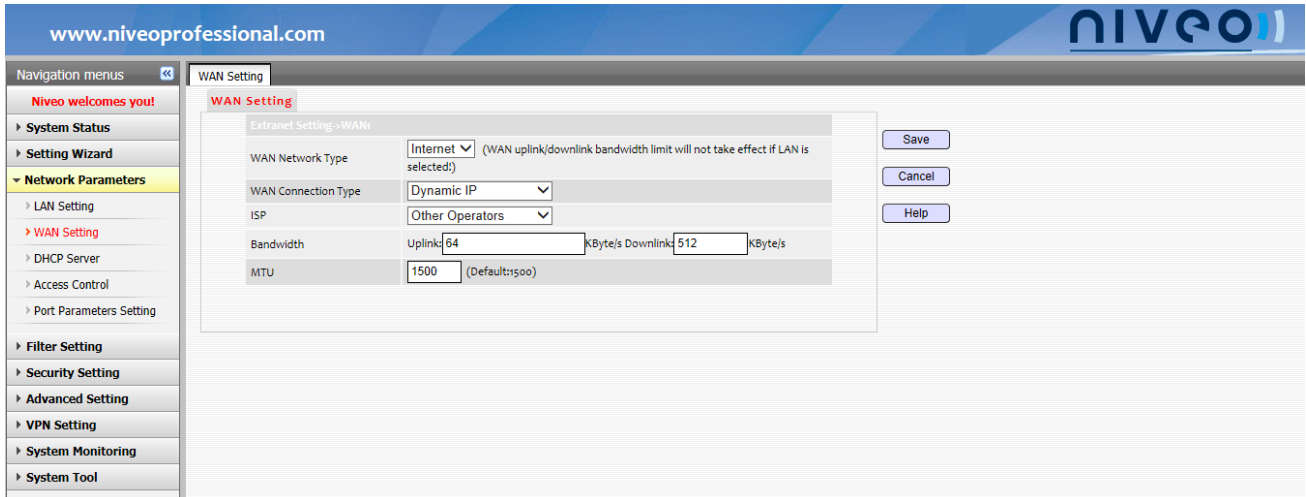
When selecting Static IP, continue to finish the following 5 6 7 settings,

5 IP Address, Subnet Mask, Default Gateway, Primary DNS Server, Secondary DNS Server: Input the WAN IP address and other network information provided by your ISP.

6 Bandwidth: The bandwidth of the static router on the WAN interface you're configuring. Consult the value from the ISP.

7 MTU: The default value is 1500. It's recommended to keep this parameter the default value, because improper MTU value will decrease the network performance, even worse have the network stop working.

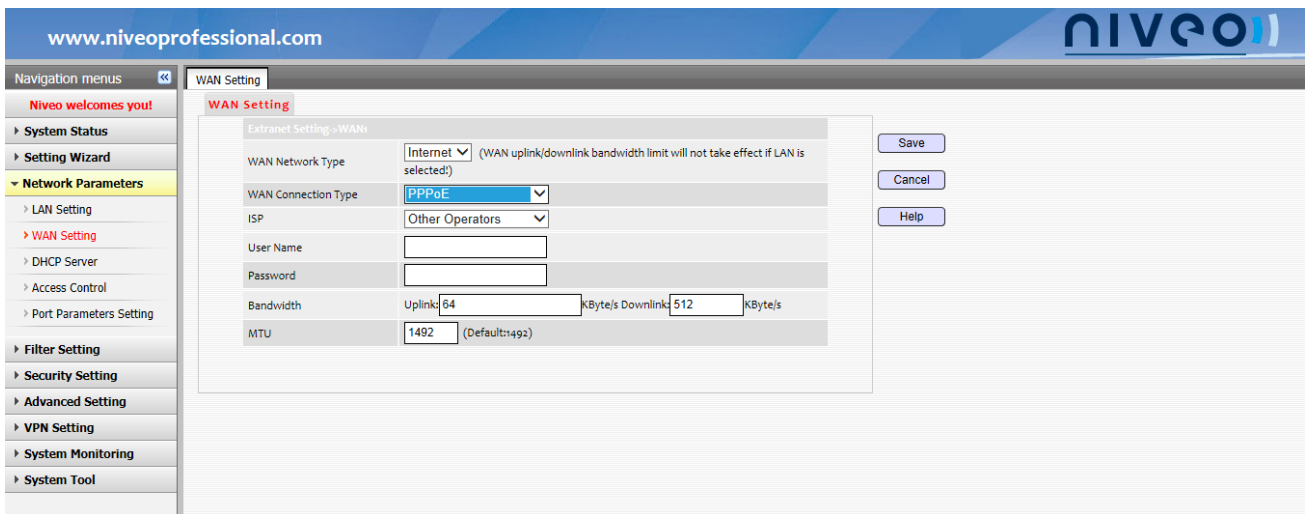
When selecting Dynamic IP, continue to finish the following 5 6 settings,



5 Bandwidth: The bandwidth of the dynamic IP route on the WAN interface you're configuring. Consult the value from the ISP.

6 MTU: The default value is 1500. It's recommended to keep this parameter the default value, because improper MTU value will decrease the network performance, even worse resulting the network stop working..

When selecting Dynamic IP, continue to finish the following **5 6 7** settings,



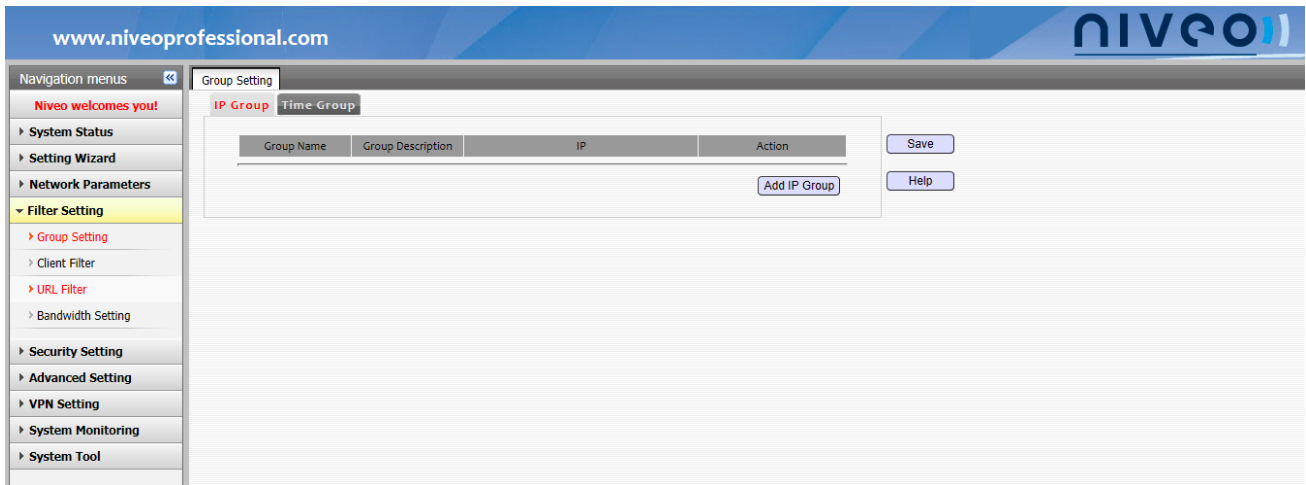
5 User Name, Password: Input the PPPoE user name and password provided by your ISP.

6 Bandwidth: The bandwidth of your user account. Consult the value from the ISP.

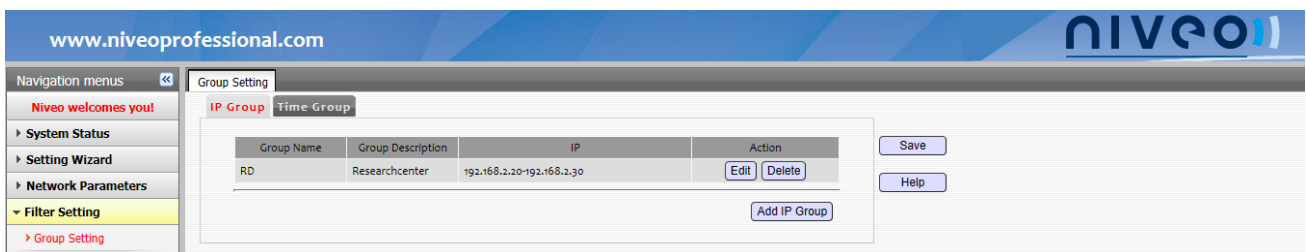
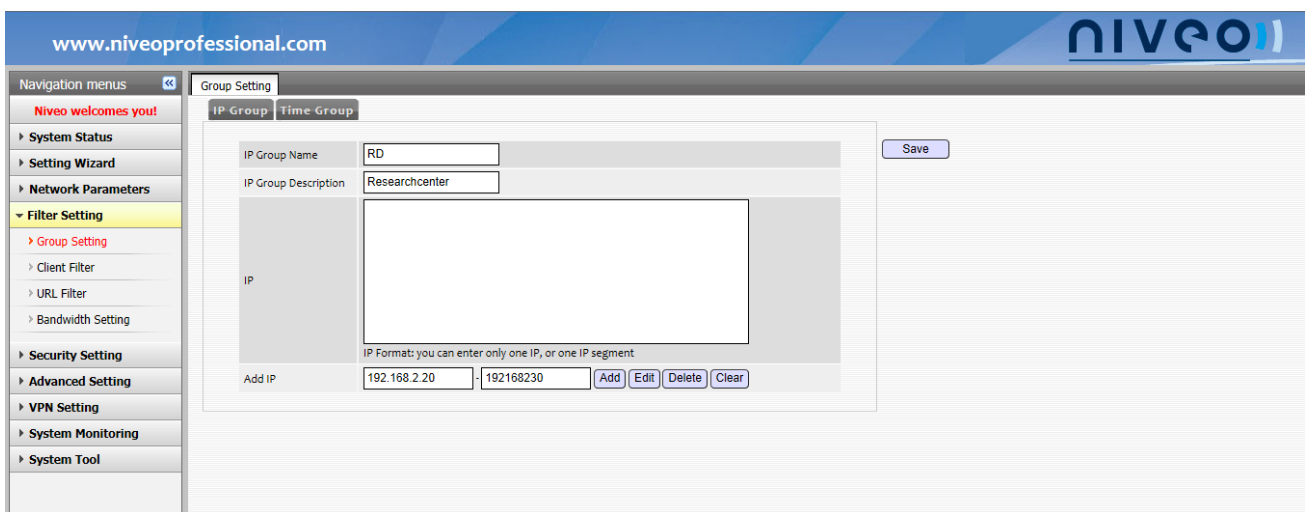
7 MTU: The default value is 1492. It's recommended to keep this parameter the default value, because improper MTU value will decrease the network performance, even worse resulting the network stop working.

2. Multiple WAN Policies

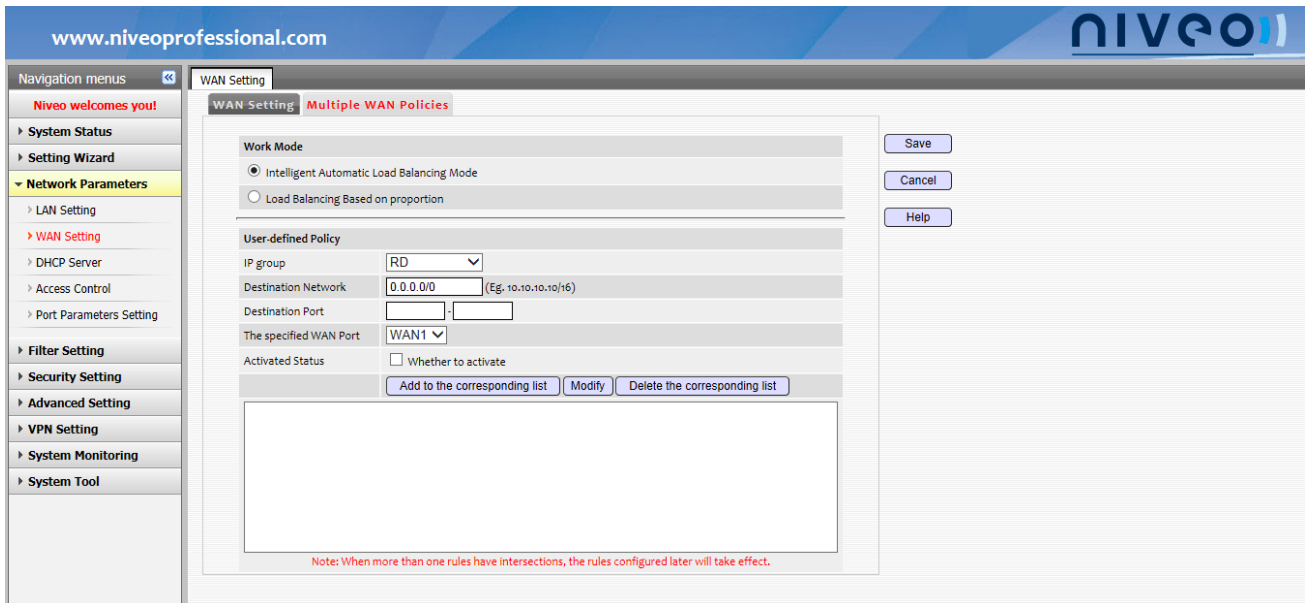
1 Before configuring WAN policies, go to **Filter Setting->Group Setting**, to add IP groups.



For example, add the RD Group as below.



2 Go to **Network Parameters->WAN Setting->Multiple WAN Policies**, to customize the WAN policies.



a. Intelligent Automatic Load Balancing Mode:

The system automatically assigns load according to traffic. It will search the WAN port with the minimum traffic to communicate, and this method is the smartest and the best load pattern. The load balancing policy not involved in manual work at all, will automatically assign traffic and can successfully implement the bandwidths' stack.

This Automatic mode is the default mode here.

b. Load Balancing Based on properties: Assign load according to the set proportion of the WAN ports.

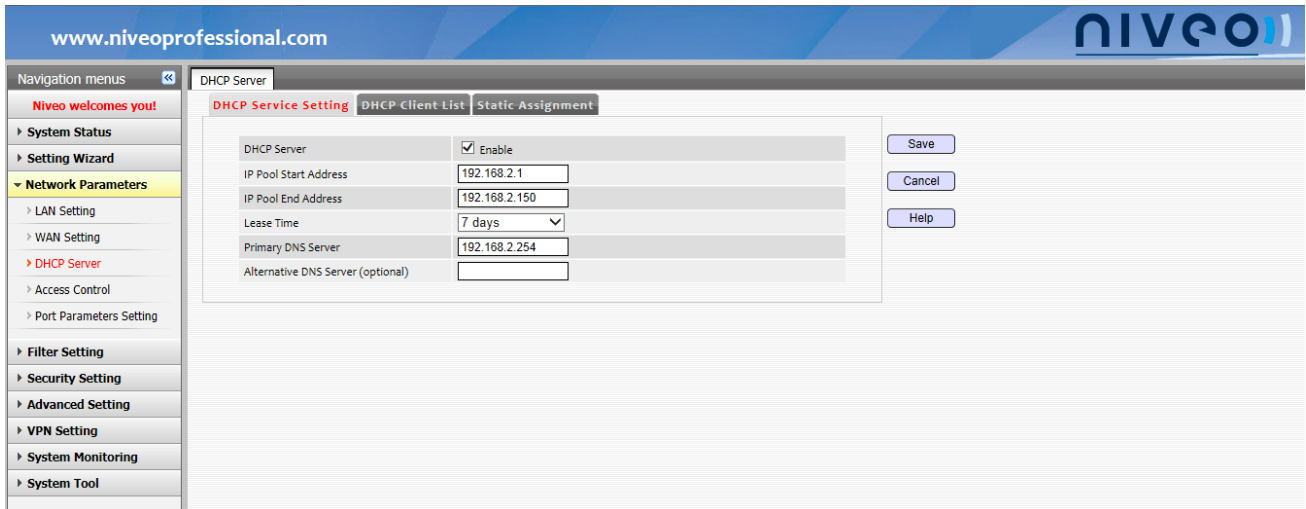
c. User-defined Policy: Users select circuits via the specified destination address and port on the basis of their actual needs.

DHCP Server

1. DHCP Serer

To make it easier for you to configure the TCP/IP of your computer, just enable the DHCP Server of your Router, and the DHCP sever will automatically assign you the IP address, Subnet mask and DNS Server, etc.

① Click **Network Parameters->DHCP Server->DHCP Service Setting**, to enter the setting interface.



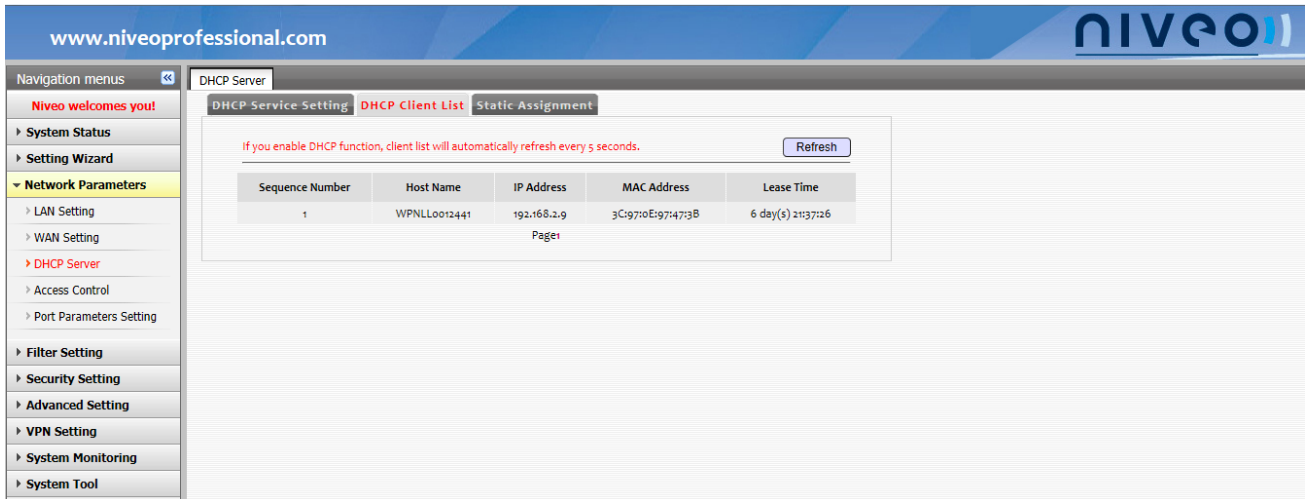
- 2 **DHCP Server:** Check/Uncheck it to enable/disable the DHCP Server.
- 3 **IP Pool Start Address, IP Pool End Address:** Enter the start address and end address, for example 192.168.2.1, 192.168.2.150 on the figure above.
- 4 **Expiration Time:** The available time of the IP address obtained by your Client.
- 5 **Primary DNS Server:** The field is entered automatically with the current LAN IP address of your Router, which can help the devices in the LAN to access the Internet or Intranet. The default LAN IP address is 192.168.2.254.
- 6 **Alternative DNS Server (Optional):** The **Alternative DNS Server** field can be kept blank unless you need one as a second choice.

! Note

Set the LAN setting in the computer to "Obtain an IP address automatically".

2. DHCP Client List

Click **Network Parameters->DHCP Server->DHCP Client List**, to view all the IP hosts with their IP addresses, MAC addresses and Lease time.

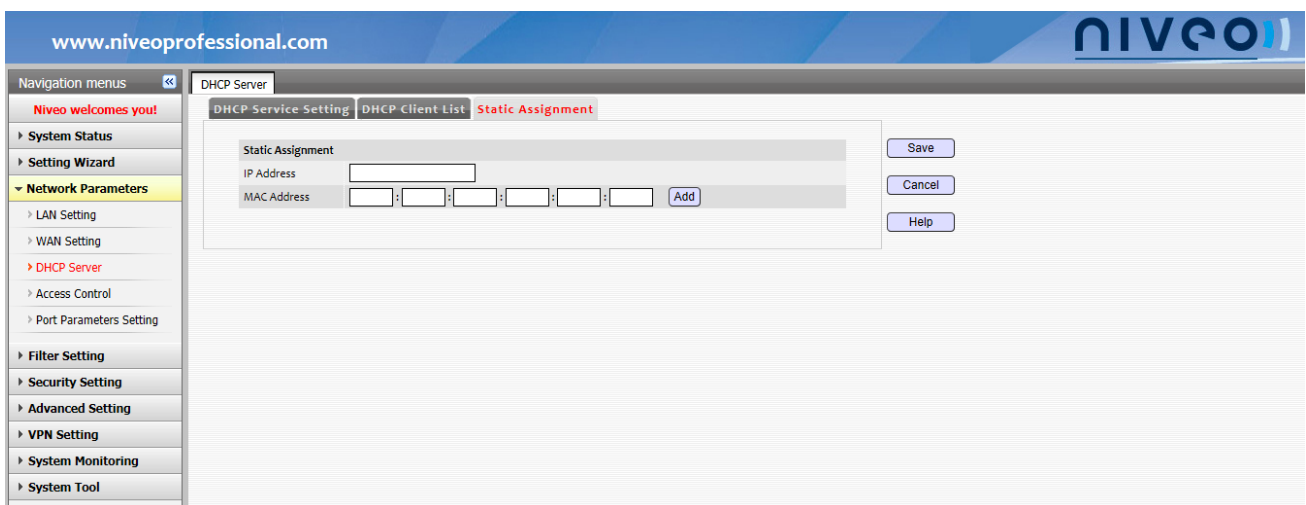


- **Host Name:** The name of the client.
- **IP Address:** The IP address acquired by the client.
- **MAC Address:** The MAC Address of the computer that has been given the IP address.
- **Lease Time:** The available time of the IP you get

3. Static Assignment

If you want some hosts to obtain the same IP address assigned from the DHCP Server every time it starts up, you can configure this feature.

For example, MAC Address of one PC intranet: 22:22:22:22:22:22. You want that after starting up every time, the PC can get the IP 192.168.2.140. In this case, Static Assignment is the perfect solution.



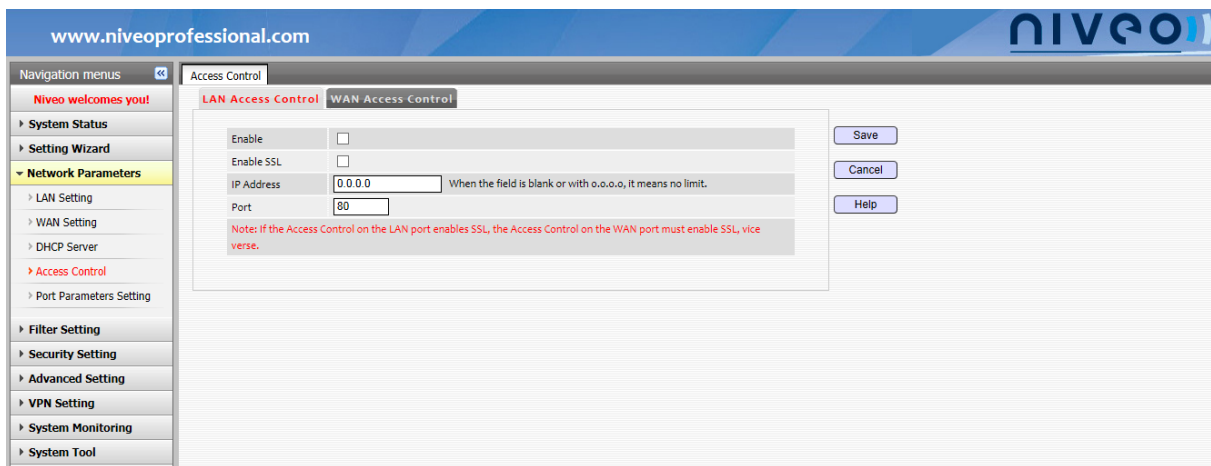
- **IP address:** the reserved IP address.
- **MAC address:** the MAC address of the computer of which the IP address you want to reserve.

- **Add:** add the reserved IP address and MAC address to the list.
- **Edit:** modify the static assigned IP address and MAC address.
- **Refresh:** refresh the edited rules to the list.
- **Delete:** delete the created static allocation information

Access Control

For lowering the router's possibility of being attacked, you can enable the designated host address and ports.

1. LAN Access Control



- **Enable SSL:** if you don't check the box, the HTTP protocol will be adopted to manage the WEB interface; if you check the box, the HTTPS protocol will be adopted to manage the WEB interface. Only the specified port sequence number is adopted, for visiting the router management interface.
- **Enable:** Enable the Web limiting function in accessing the router.
- **IP Address:** Enter the IP address of the computer in the LAN, or 0.0.0.0. Also you can leave this address field blank.
- **Port:** Enter the port ID you use to access the router's Web page. The default port is 80.

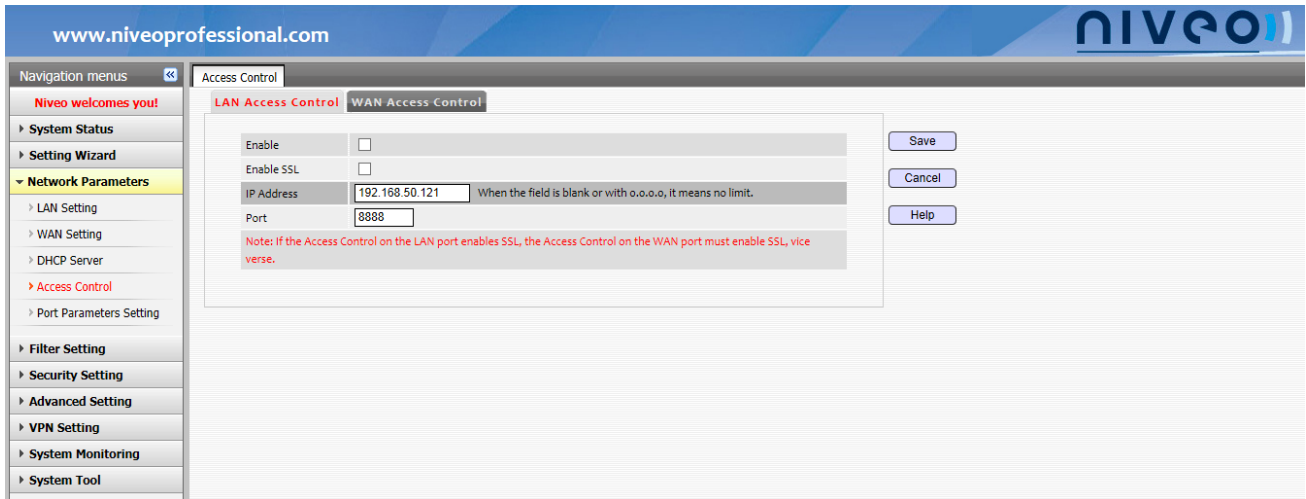
Note:

The IP address 0.0.0.0 or its blank status indicates that every IP is allowed;

The designated IP indicates that only this IP address is allowed to login to the router, while hosts with other addresses cannot.

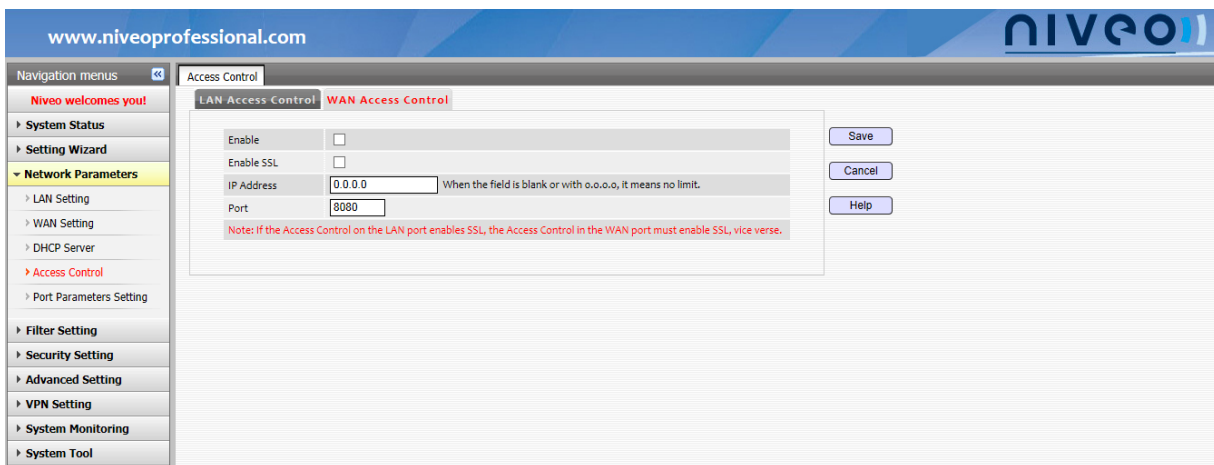
If SSL is enabled, the port will become 443 automatically, and you need to enter <https://192.168.2.254> to login the Router's management interface. And also, WAN Access Control should be using https.

For example, the Router's IP is 192.168.50.1; only the client with IP 192.168.50.121 can access the Router's Web interface via port 8888. In this case, parameters you configure is shown as the following figure. Meanwhile the accessing website is changed into <http://192.168.50.1:8888>.



2. WAN Access Control

Generally speaking, only the users in the LAN can access the router. If there's special necessity, this function can help remotely accessing and controlling the router.



- **Enable:** Enable the WAN Port Accessing and limiting function in accessing the router.
- **Enable SSL:** If you don't check the box, the HTTP protocol will be adopted to manage the WEB interface; if you check the box, the HTTPS protocol will be adopted to manage the WEB interface.

- **IP Address:** Enter the IP address of the WAN port which can access and control the router, or 0.0.0.0. Also you can leave this address field blank.
- **Port:** Enter the port ID you use to access the router's Web page. **The default port is 8080.**

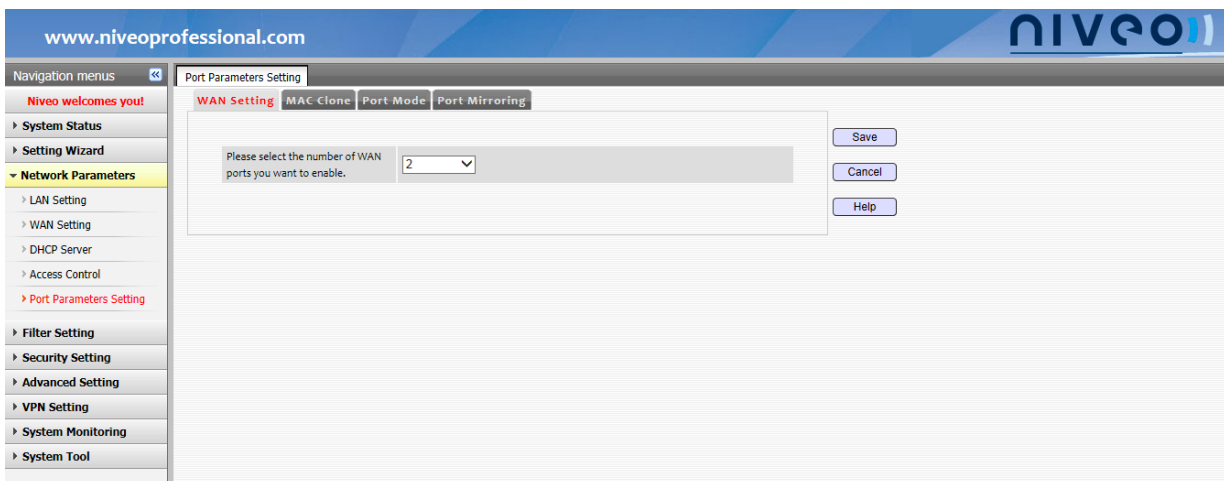
⚠ Note:

1. The IP address 0.0.0.0 or its blank status indicates that every IP is allowed; the designated IP indicates that only this IP address is allowed to login to the router, while hosts with other addresses cannot. You must use the way "IP Address (the router's WAN port IP address): Port ID" to login the router to implement remote management. E.g., if WAN IP of the Router is 211.23.1.2, you need to enter <http://211.23.1.2:8080>
2. If you change the default IP address, say 58.60.111.221, only the computer in the WAN with the designated IP (say, 58.60.111.221) can access the Router's management interface.

Port Parameters Setting

1. WAN Setting

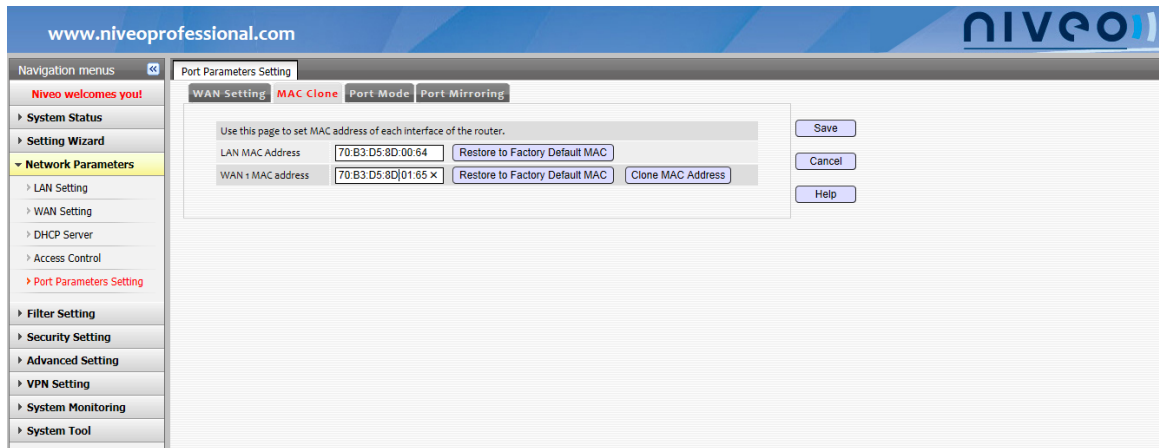
You can select the number of the WAN ports you want to enable: 1, 2, 3, and 4.



2. MAC Clone

You can configure the MAC address of each device connected to the interfaces on the Router.

Note that if your ISP doesn't bind the MAC address of the router, do not enable this function in case of other problems.



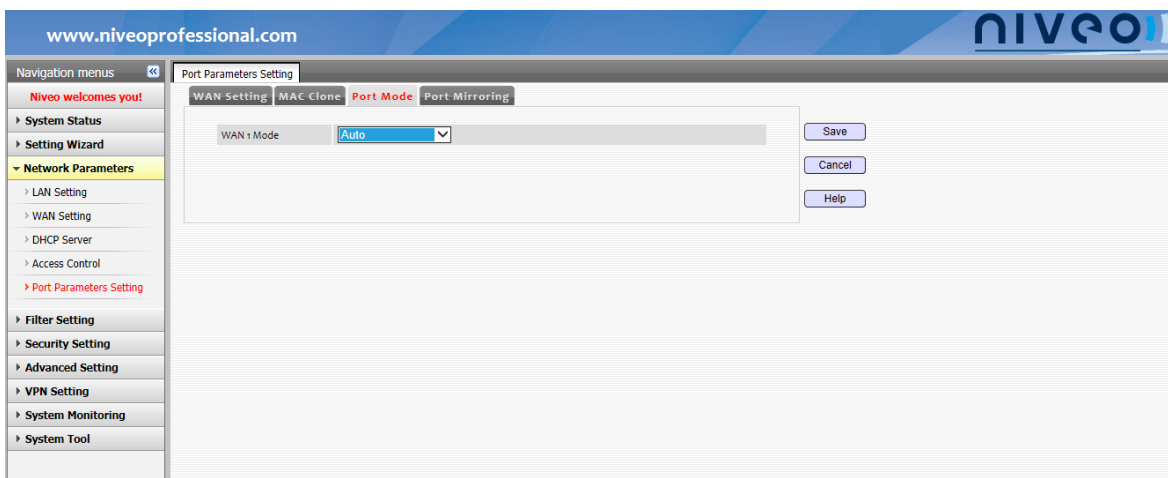
- **LAN MAC Address:** The router’s LAN MAC address. You can enter it manually;
- **WAN1/2/3/4 MAC Address:** The router’s WAN MAC address. You can enter it manually;
- **Restore to Factory Default MAC:** Click this button to restore the devices’ MAC to the factory default;
- **Clone MAC Address:** Click this button to set the MAC address of the device connected to WAN 1/2/3/4.

⚠ Note:

MAC Address refers to the WAN port MAC address of your router, no need to be modified generally. But some ISPs may bind the MAC address, if so, ISP will provide the user with valid MAC address. Fill in the **WAN MAC Address** field on basis of the value provided by the ISPs. Click "Save", and then you can change the WAN MAC address of your Router. Reboot the router to activate the new settings.

3. Port Mode

This feature is to set the data’s transmission mode on the WAN port.



- **Full-duplex:** Allows the signal’s duplex transmission at the same time.
- **Half-duplex:** Allows the signal’s unidirectional transmission within some time.

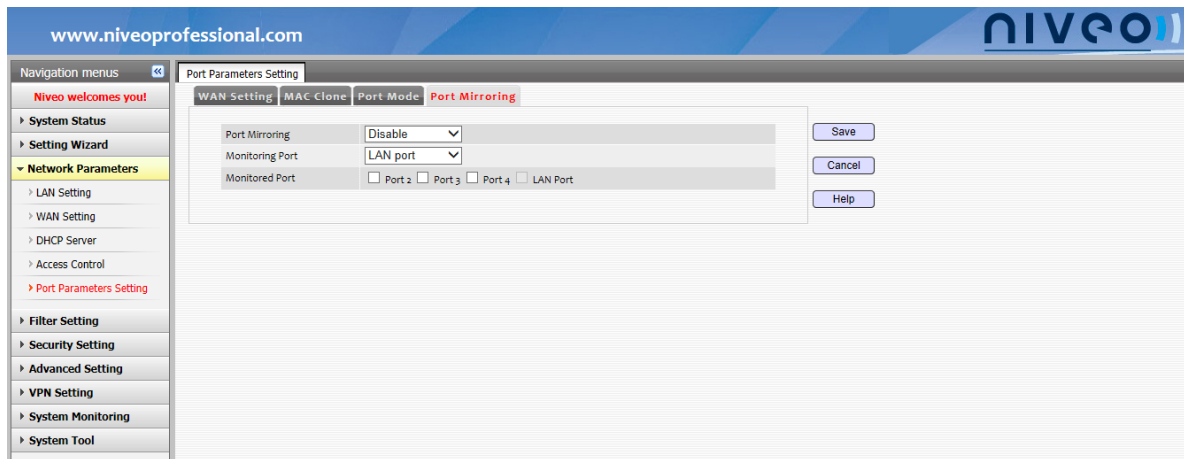
Users can select different negotiation modes on the WAN port as required, Auto, 10M full/half duplex, 100M full/half duplex, 1000M half/full duplex. The default mode is **Auto**.

Note:

The WAN port work mode must be accordance with the remote port of the WAN port, or it may cause that the WAN port cannot receive or send messages properly. If you are not clear about the remote port's working mode, you can select the auto mode.

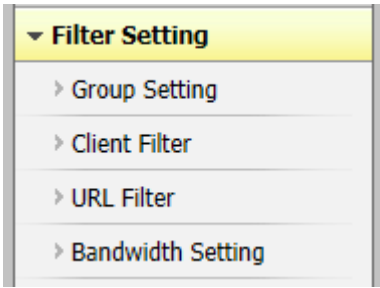
4. Port Mirroring

When this feature is enabled, all packets on the monitored port will be backed up to the monitoring port.



- **Port Mirroring:** Disable/Enable the Port Mirroring feature.
- **Monitoring Port:** Select the physical port to monitor other ports.
- **Monitored Port:** For the router's physical port, you can check the box or just leave it blank to decide whether the port is a member of the VLAN. Interface 2 corresponds to WAN2/LAN4, interface 3 corresponds to WAN3/LAN3, and interface 4 corresponds to WAN4/LAN2.
- **Save:** After you click **Save**, the router will produce a new VLAN list according to the configuration on the current page. And also the settings will take effect.

4 Filter Setting

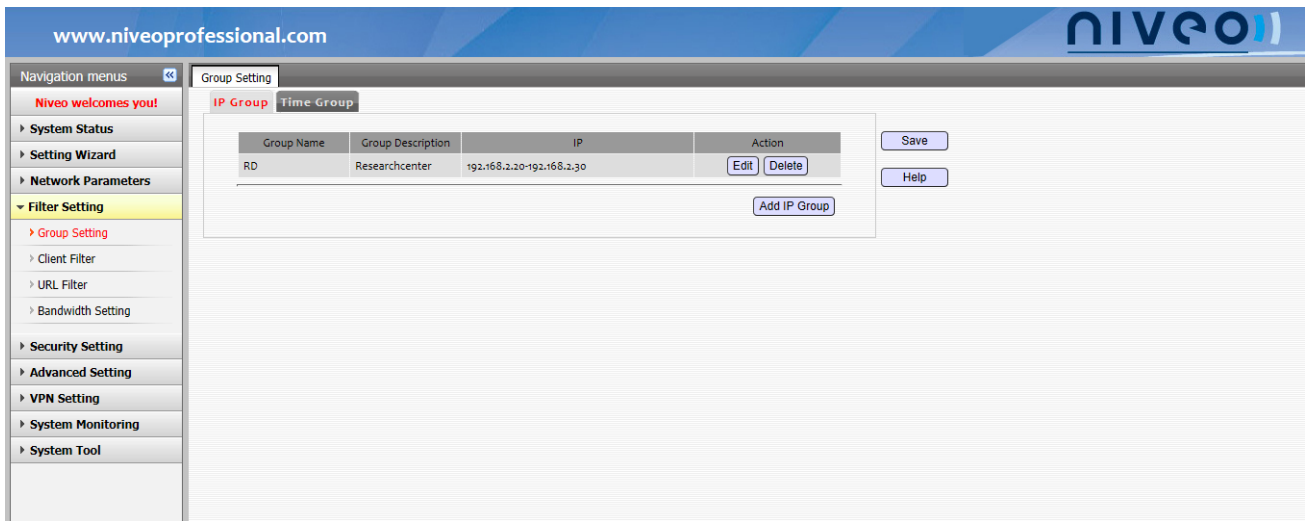


Group Setting

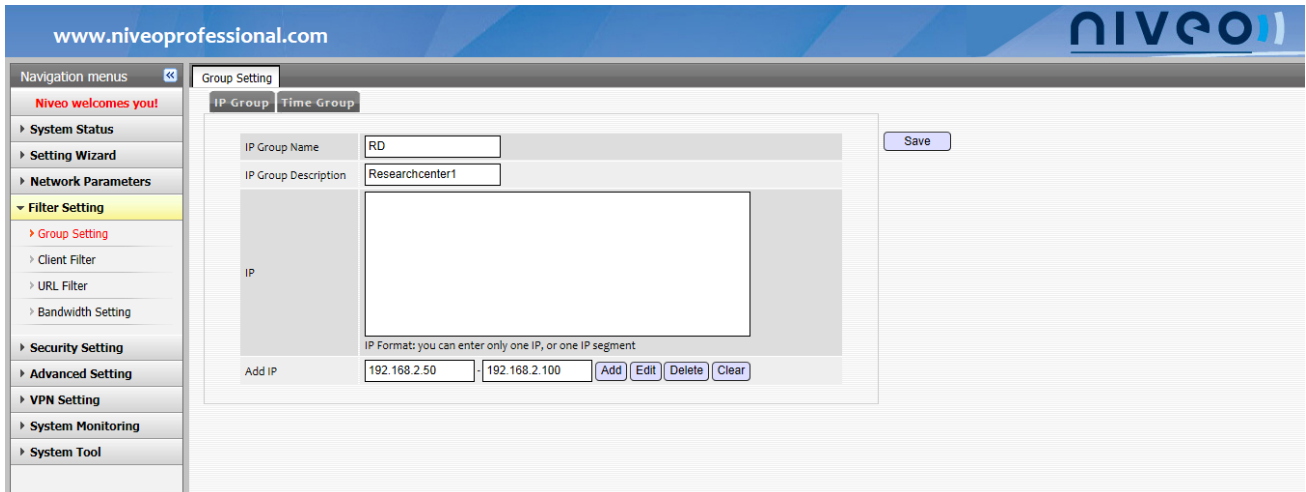
1. IP Group

This function is to group the intranet users using the IP as identifiers, coordinating with other functions to control the user behavior and set security parameters.

Click **Filter Setting->Group Setting->IP Group**, to add an IP group here.

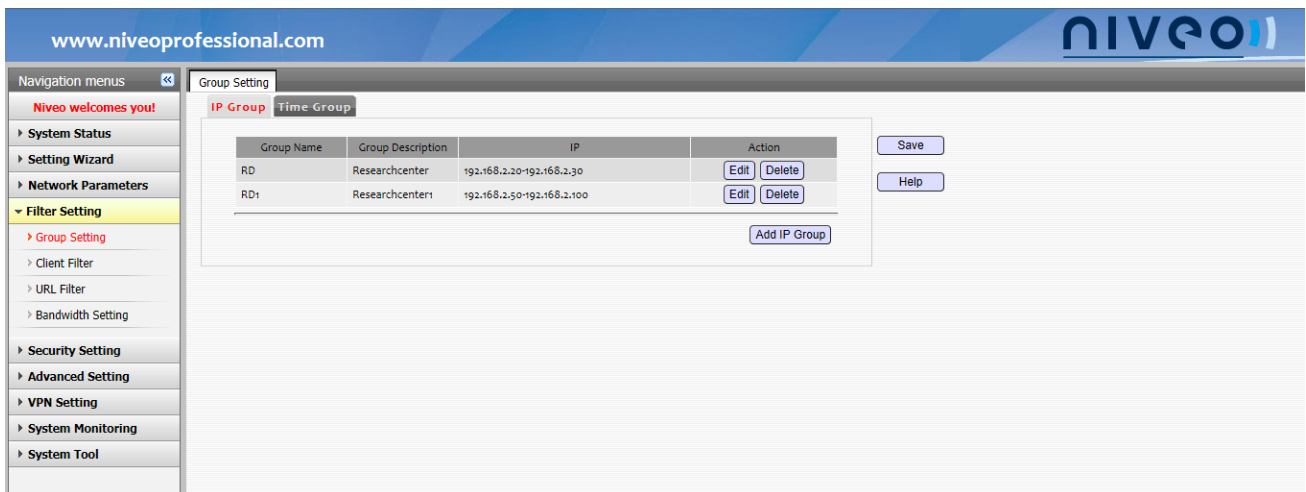


Click **Add IP Group** to enter the following configuration interface. Parameter shown on the figure is example.



- **IP Group Name:** You must enter the content here. It can be the group identifier easy to distinguish, e.g., RD.
- **IP Group Description:** You must fill the comment description in the field, say Research Center.
- **Add:** You need or need not to enter the IP segment, e.g., 192.168.2.50-192.168.2.100; you can also designate one IP, at this moment, the second text field is left blank.

After you click **Save**, you can see the following figure.



- **Add IP Group:** When adding the IP segment, first enter the start IP and end IP of the IP segment, and then click **Add IP Group**. After all the settings, click **Save**.
- **Edit:** When modifying the IP segment, first select the IP segment on the list, and then click **Edit**. After you modify the start and end IP, click **Refresh**. After all the settings, click **Save**.
- **Delete:** When deleting the IP segment, first select the IP segment on the list, and then click **Delete**. After all the settings, click **Save**.

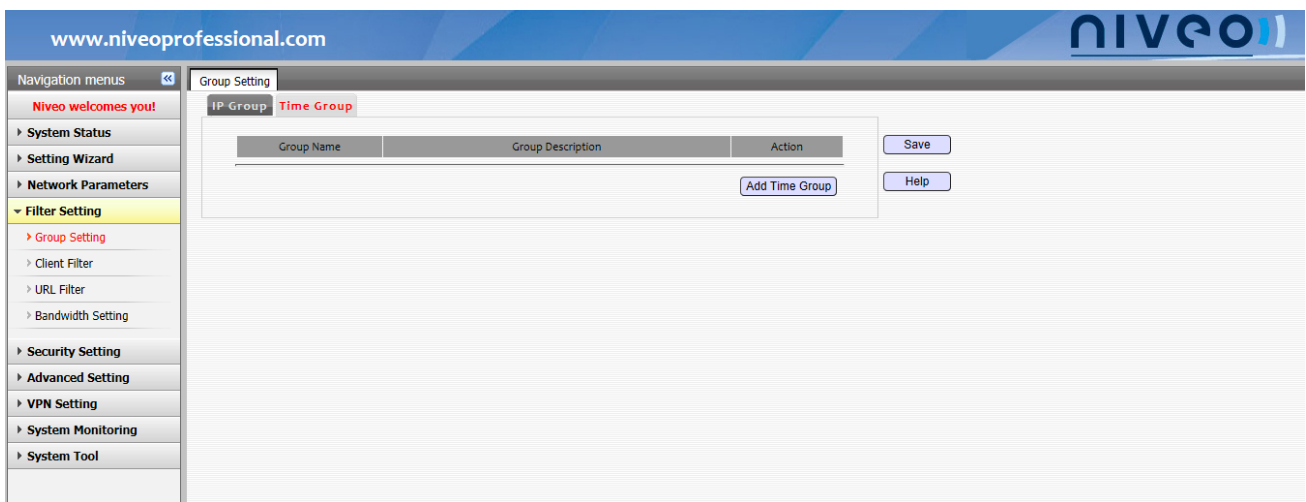
! Note:

This function is used in the port filtering and URL filtering; when one user group is used, you cannot modify its group name or delete the group. If you wish to do that, you need to cancel to use the group.

In addition, when the LAN IP of the router changes, all the IP segment in the user group will be automatically modified to have the same network ID with the LAN IP, but the host ID stays.

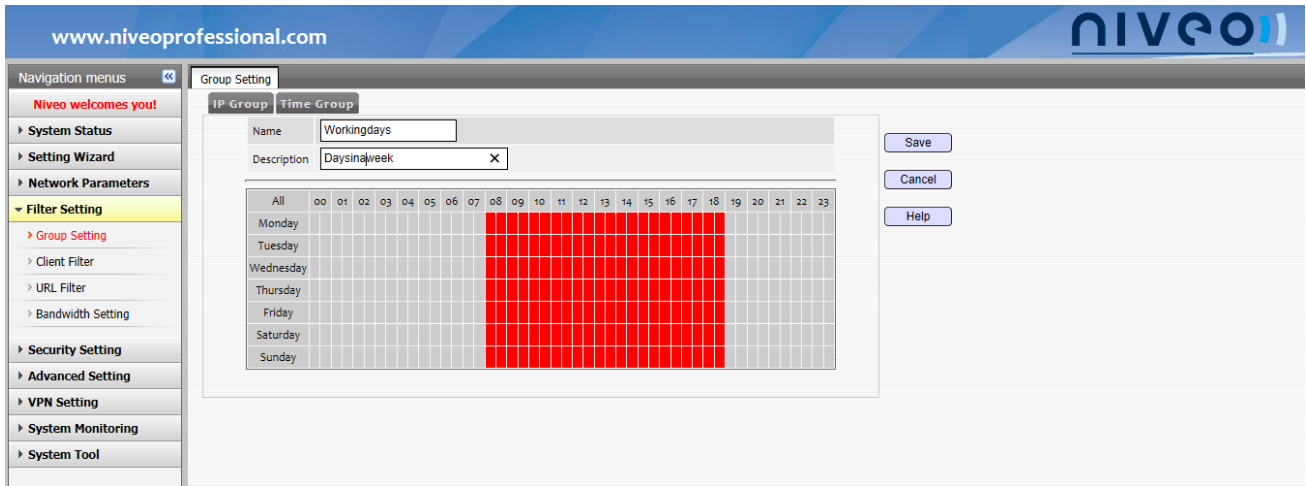
2. Time Group

Click **Filter Setting->Group Setting->Time Group** to configure the time segments.

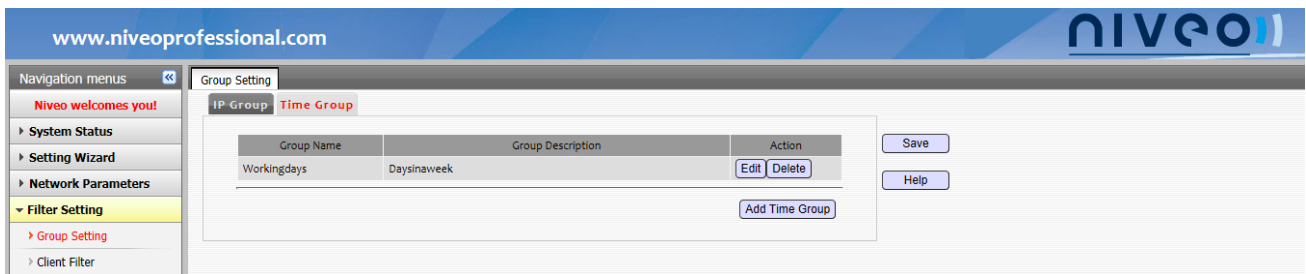


One time group is the collection of some time-segment, e.g., "work time" is set from Monday to Friday, 9 a.m. to 5 p.m. This function should coordinate with other functions to control the user behavior and set security parameters.

Enter the group name in the Name bar; select and enter the comment description in the description bar; in the time box, select the time range that needs to be set within one week. When you're selecting the time, click one time and the box will turn, indicating it's selected, if you click it again, it will turn gray, indicating it's not selected. You can press and hold the left click of your mouse and drag it to consecutively select some time segments. You can also click to select or cancel one day from Monday to Sunday

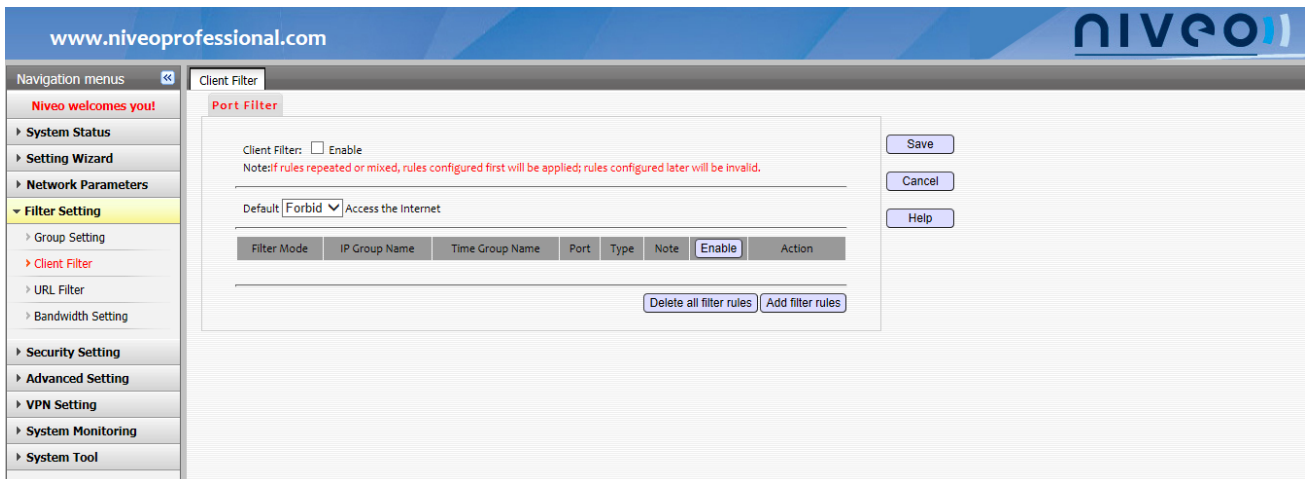


Clicking **Save** will show the screen as below.

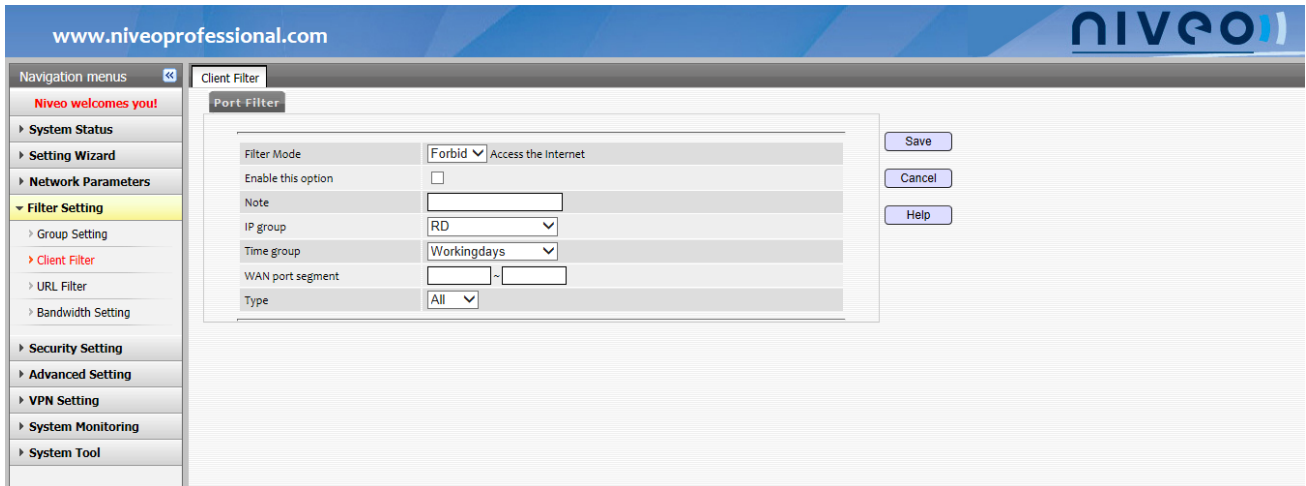


Port Filter

To make it more convenient for you to manage the computers in the LAN, you can enable Port Filtering function to control these computers in the LAN to accessing the Internet.

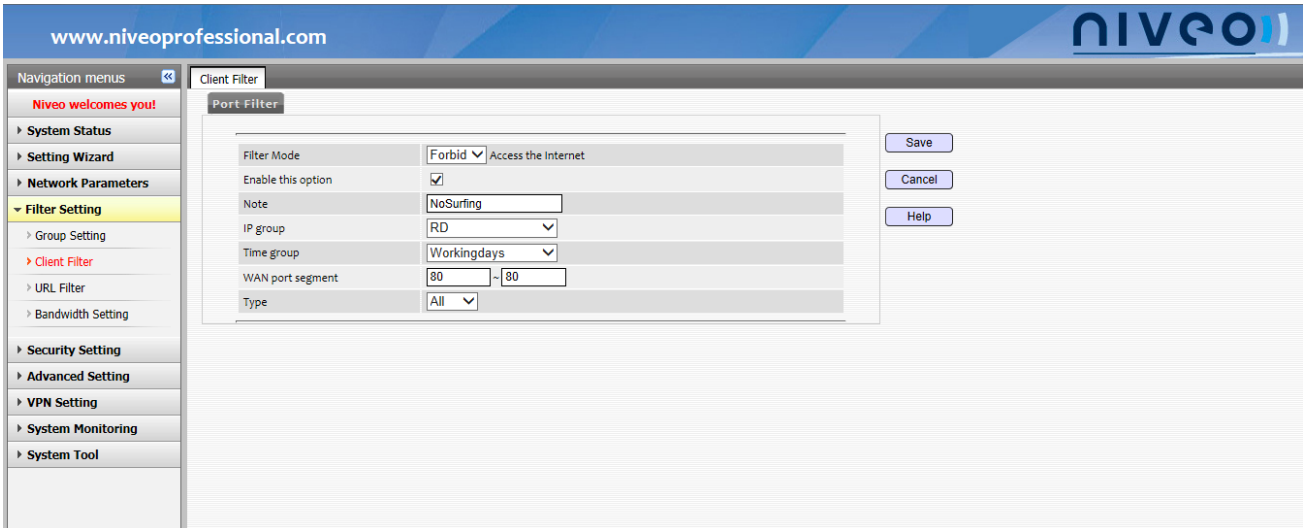


Click **Add filter rules**, and the following figure will be displayed.

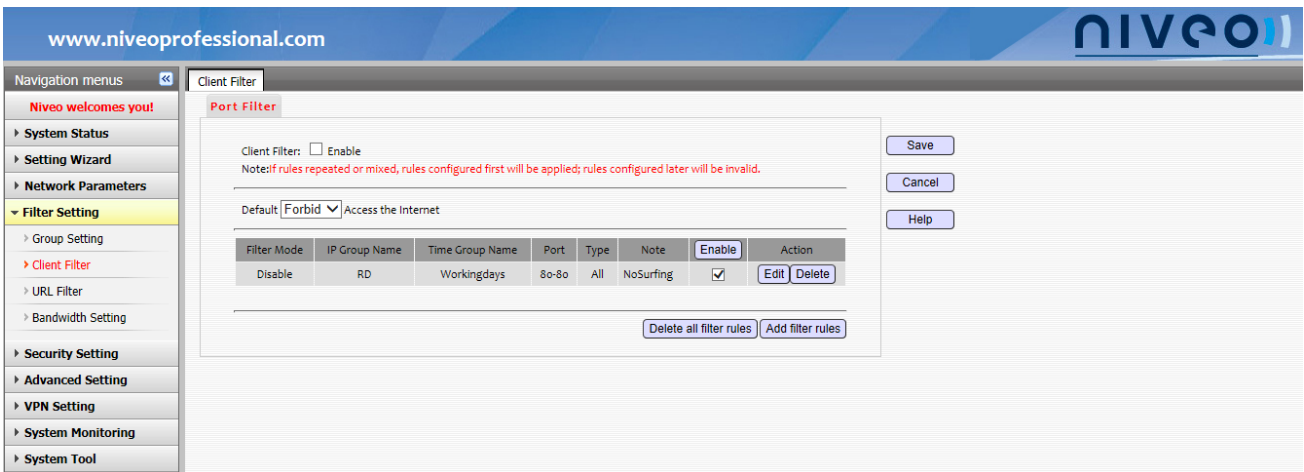


- **Filter Mode:** Select the client filter mode. There are two valid modes: **Allow** and **Forbid**.
Forbid: Forbid the data packets which are matching with the port filter rules passing through the router. And the unrestricted data packets are processed according to default rule.
Allow: Allow the data packets which are matching with the port filter rules to pass through the router. And the unrestricted data packets are processed according to default rule.
- **Enable this option:** Check this box to enable current filter rule.
- **Note:** Edit a brief description about the filter rule.
- **IP Group:** Select an IP group.
- **Time Group:** Select a time group.
- **WAN Port Segment:** Specify a port range. The valid range is 1-65535.
- **Type:** Select the protocol that the filtering data using. There are three selections: **All**, **TCP** and **UDP**.

For example, if you hope computers of IP addresses from 192.168.2.20 to 192.168.2.30 (Time Group-Working day) cannot access Websites from 8:00~18:00, Monday to Friday. Just do the following configurations on the interface.



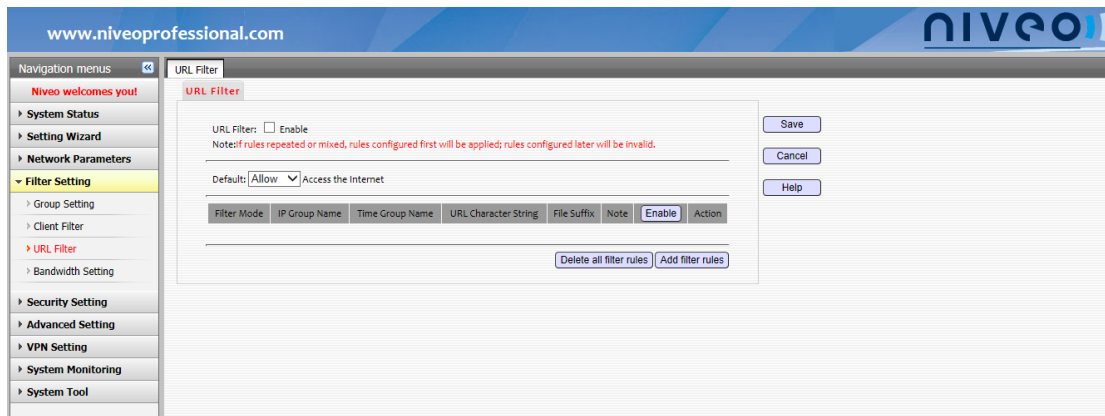
Click **Save** and you will see the figure below



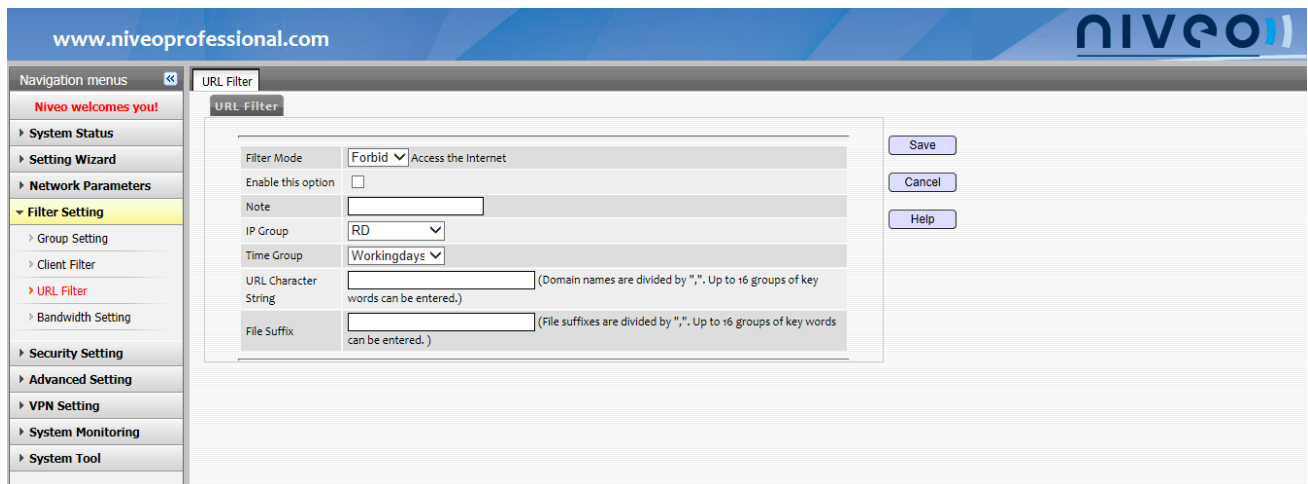
Set the **Forbid to access the Internet** as the default rule, check **Enable** to enable the Clients Filtering feature and save it.

URL Filter

To limit some websites via URL Filtering

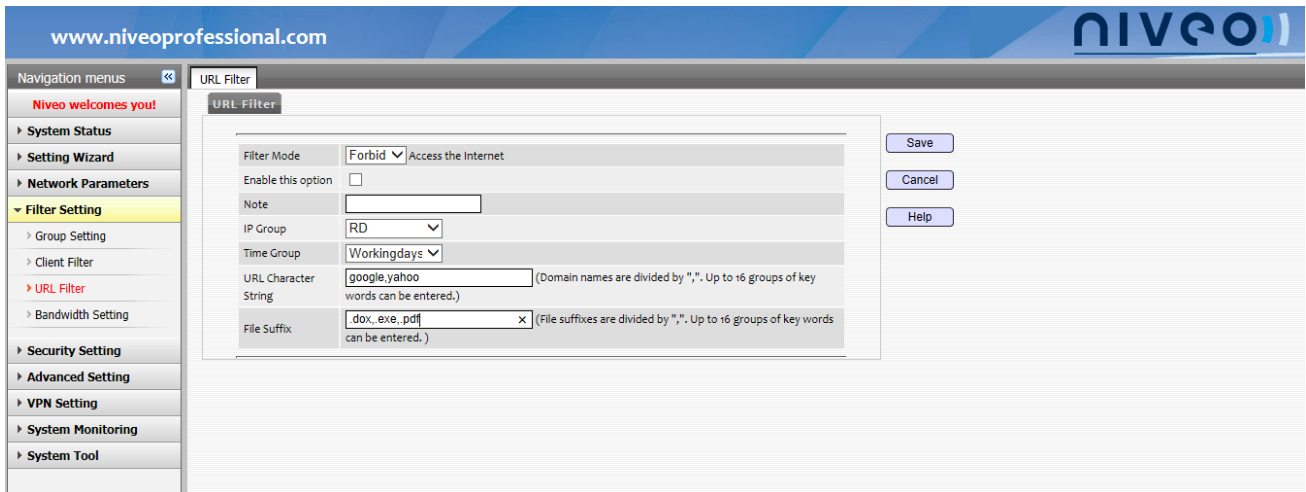


Click **Add filter rules**, and you will see the interface below.

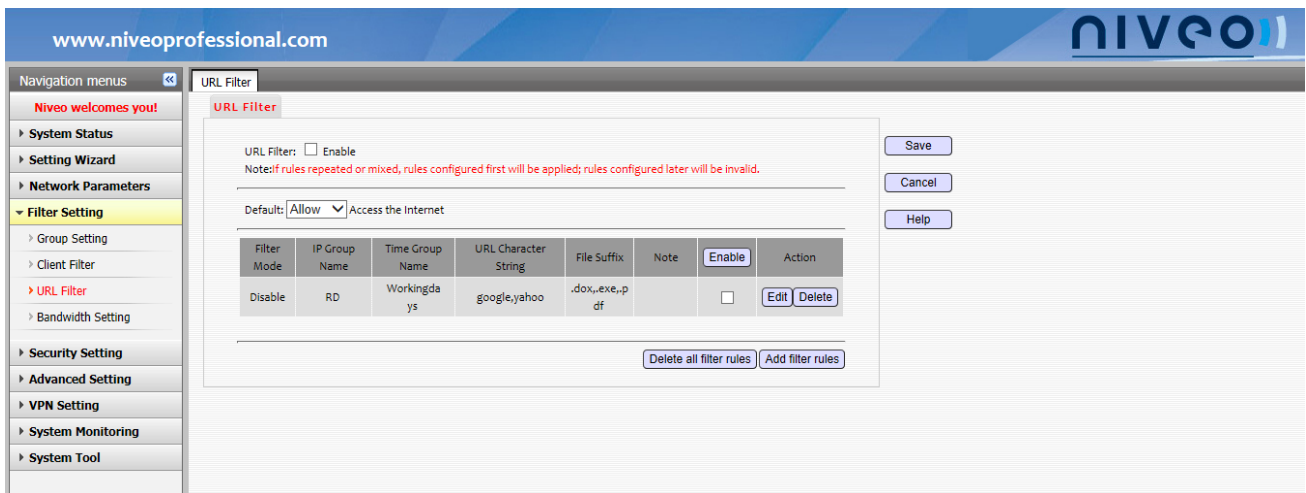


- **Filter Mode:** Select the URL filter mode. There are two valid modes: **Allow** and **Forbid**.
 - Forbid:** Forbid the data packets which are matching with the URL filter rules passing through the router. And the unrestricted data packets are processed according to default rule.
 - Allow:** Allow the data packets which are matching with the URL filter rules passing through the router. And the unrestricted data packets are processed according to default rule.
- **Enable this option:** Check this box to enable this filter rule.
- **Description:** Edit a brief description about the URL filter rule.
- **IP Group:** Select an IP group.
- **Time Group:** Select a time group.
- **URL:** Specify the domain name you want to filter. Up to 16 entries can be filtered at one time. Multiple URLs should be separated by commas.
- **File Suffix:** Specify the extension of file allowed to be downloaded, such as .html, .exe, .pdf. Up to 16 entries can be filtered at one time. Multiple extensions should be separated by commas.

For example, if you hope that computers of IP addresses from 192.168.2.20 to 192.168.2.30 (IP Group-RD) from 8:00~18:00, Monday to Friday can access all Websites except the ones with characters **google** and **yahoo**, and cannot download files with the appendix **.doc**, **.exe**, **.pdf**. But computers in other IP segment can browse all websites. What you need to do is to set as the figure below.



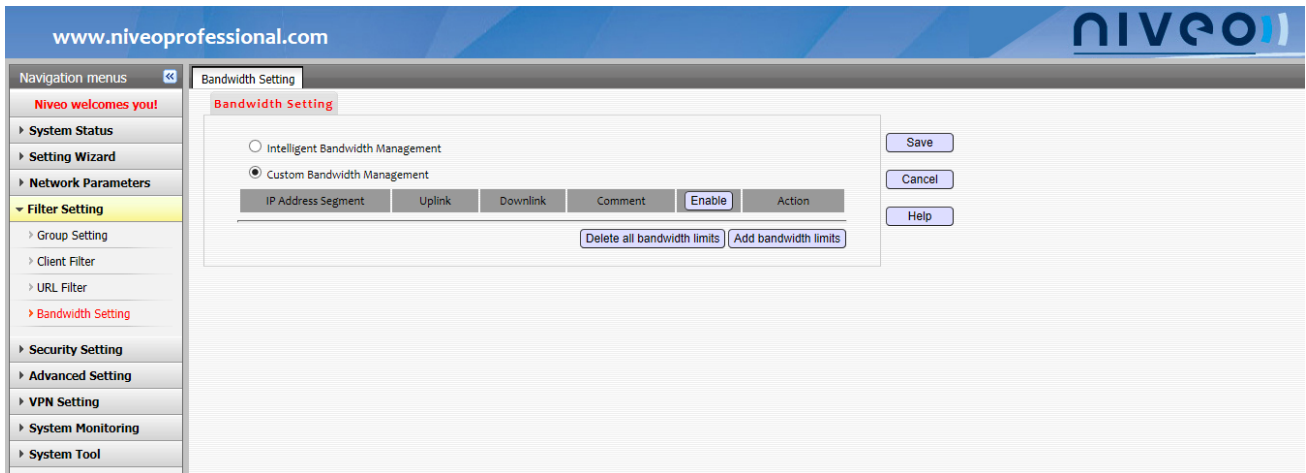
Click **Add filter rules (Save)**, and you will see the interface below.



Set **Allow to access the Internet** as the default rule, check **Enable** to enable the Clients Filtering feature and save it.

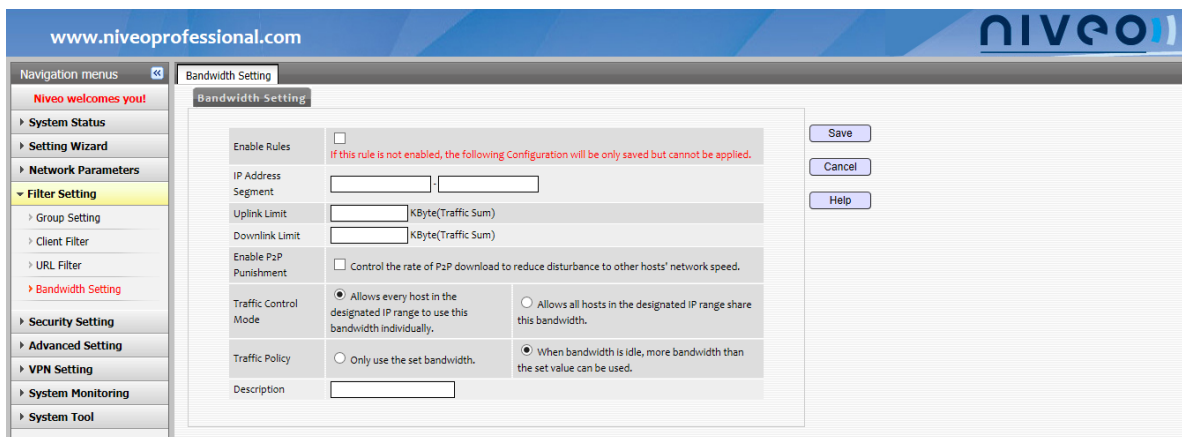
Bandwidth Setting

To select a work mode you need from Intelligent Bandwidth Management and Custom Bandwidth Management.



- **Intelligent Bandwidth Management:** The router allocates bandwidth intelligently according to the real-time data traffic. Aims to making full use of bandwidth in an idle time; to assigning bandwidth reasonably in a busy time.
- **Custom Bandwidth Management:** You can set bandwidth control for a host according to your needs manually.

The data traffic of the host in the LAN can be controlled by configuring bandwidth manually. It supports configuring according to host IP address segment. Click **Add bandwidth limits**, the configuration screen will be displayed as below.



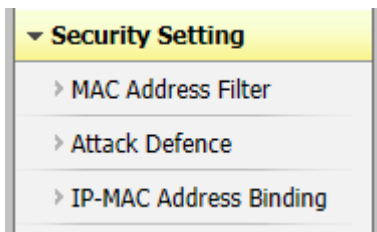
- **Enable Rules:** Check this box to enable this bandwidth rule.
- **IP Address Segment:** The traffic control host IP address range. It is a single IP address when you fill two same IP addresses in the field; or it is an IP range when you fill two different IP addresses in the field.
- **Uplink Limit:** The maximum traffic sum that the controlled hosts allowed to upload.
- **Downlink Limit:** The maximum traffic sum that the controlled hosts are allowed to download.
- **P2P Punishment:** Control the rate of P2P download to reduce disturbance to other host's network speed.

- **Traffic Control Mode:** Allows every host in the designated IP range to use this bandwidth individually.
Allows all host in the designated IP range to share this bandwidth.
- **Traffic Policy:** Only use the set bandwidth.
When bandwidth is idle, more bandwidth than the set value can be used.
- **Description:** Edit a brief description about the rule.

Note:

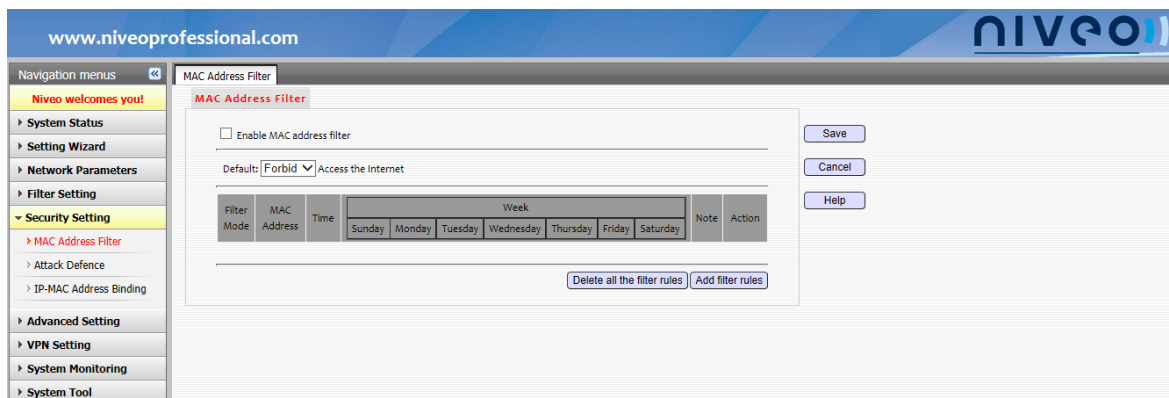
1. Please note the unit of data traffic when configure the upload/download limit.
2. If you select “When bandwidth is idle, more bandwidth than the set value can be used”, the bandwidth will be assigned flexibly and intelligently. That means when there is available bandwidth, more bandwidth than the set value can be used; when there is no available bandwidth, only the set bandwidth can be used.

5 Security Setting

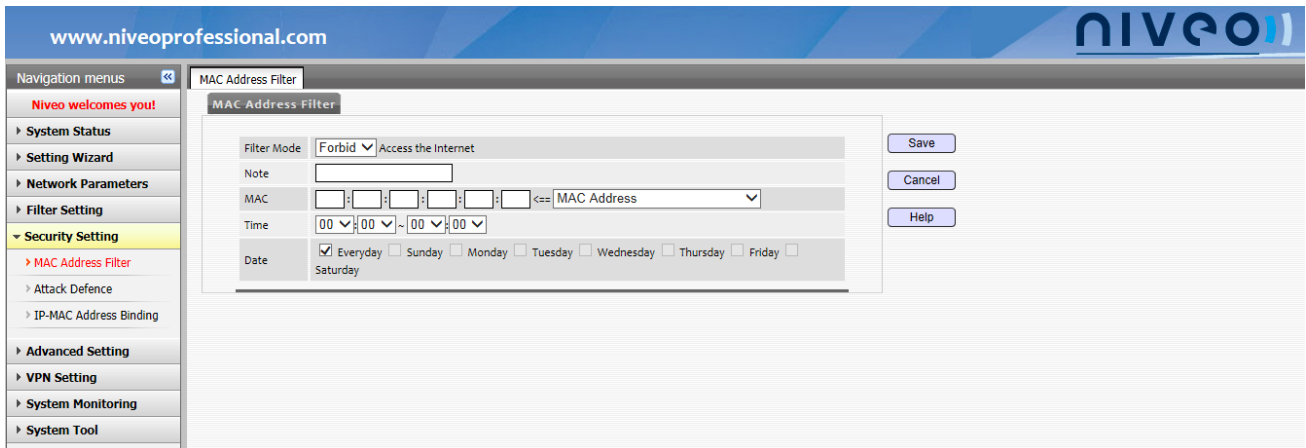


MAC Address Filter

For managing computers in the LAN to access the Internet via MAC Address Filter.



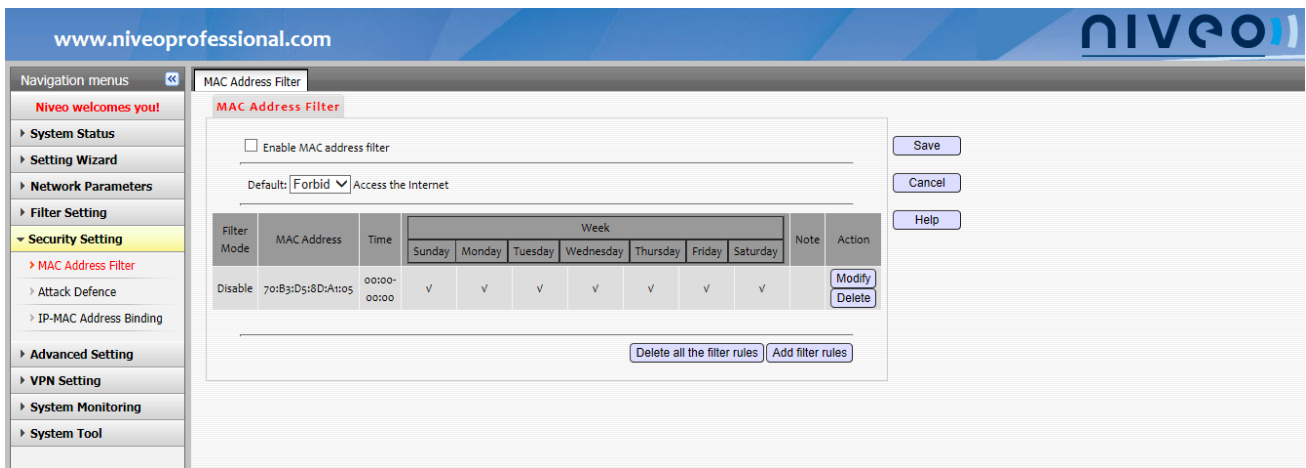
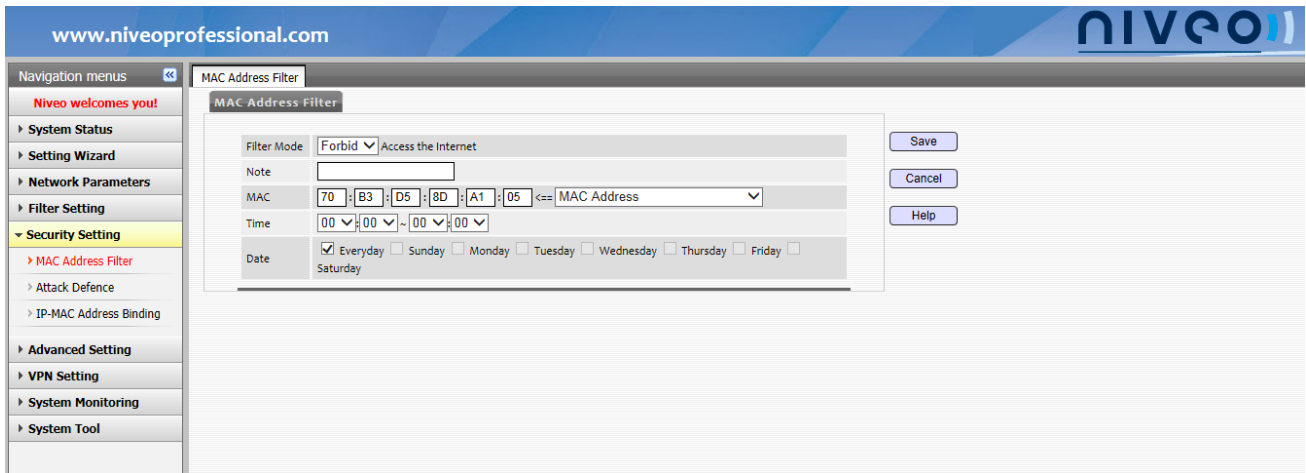
Click **Add filter rules**, and you will see the interface below.



- **Filter Mode:** Configure the filter rule of MAC address.
 - Forbid:** Forbid the data packets which are matching with the MAC address filter rules passing through the router. And the unrestricted data packets are processed according to default rule.
 - Allow:** Allow the data packets which are matching with the MAC address filter rules passing through the router. And the unrestricted data packets are processed according to default rule.
- **Note:** Edit a brief description about the filter rule.
- **MAC:** Enter a MAC address you want to filter into the MAC field, or you can select one from the MAC address list.
- **Time:** Specify the time when the rule works (including start time and end time). If you keep it default configurations (00:00~00:00), it means the rule works all day 24 hours.
- **Date:** Specify the date when the rule works.

For example

Forbid the host whose MAC address is “70:B3:D5:8D:A1:05” in the LAN accessing the Internet from 00:00~00:00 every day, and no restriction on other hosts in the LAN. You need to set parameters as below shown.



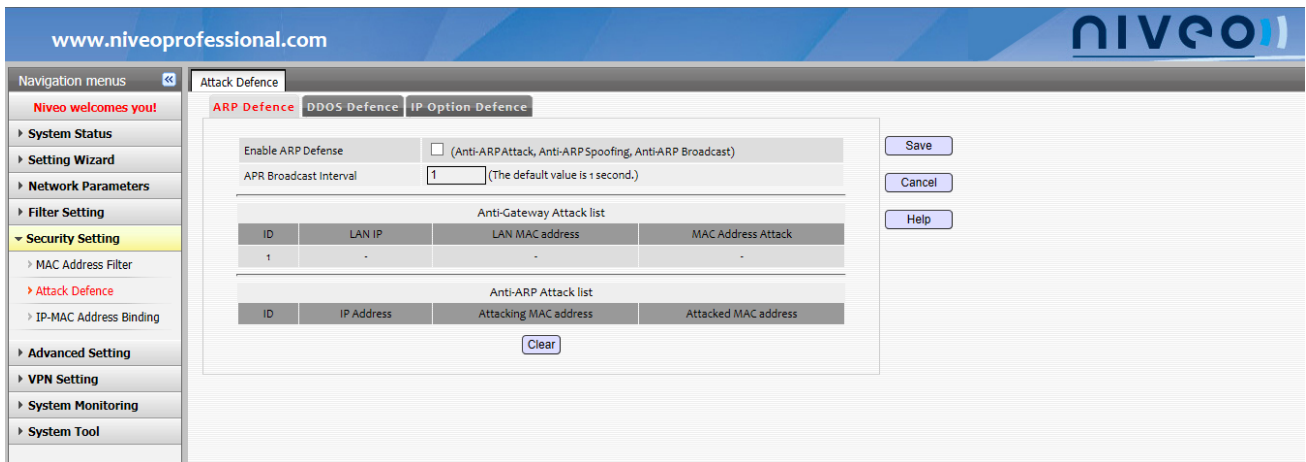
Set **Forbid to access the Internet** as the default rule, check **Enable MAC address filter** to enable the Clients Filtering feature and save it.

Attack Defence

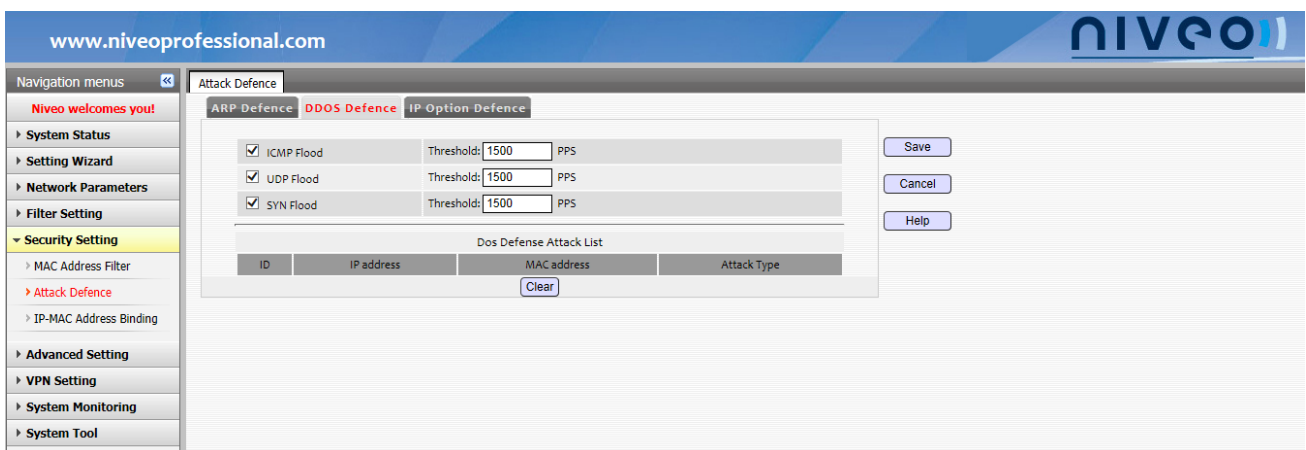
1. ARP Defence

Enabling this feature to prevent ARP attacks/disguising from happening in the LAN, for better network security.

ARP broadcast frequency is 1 second, the setting range is 1~60 seconds.

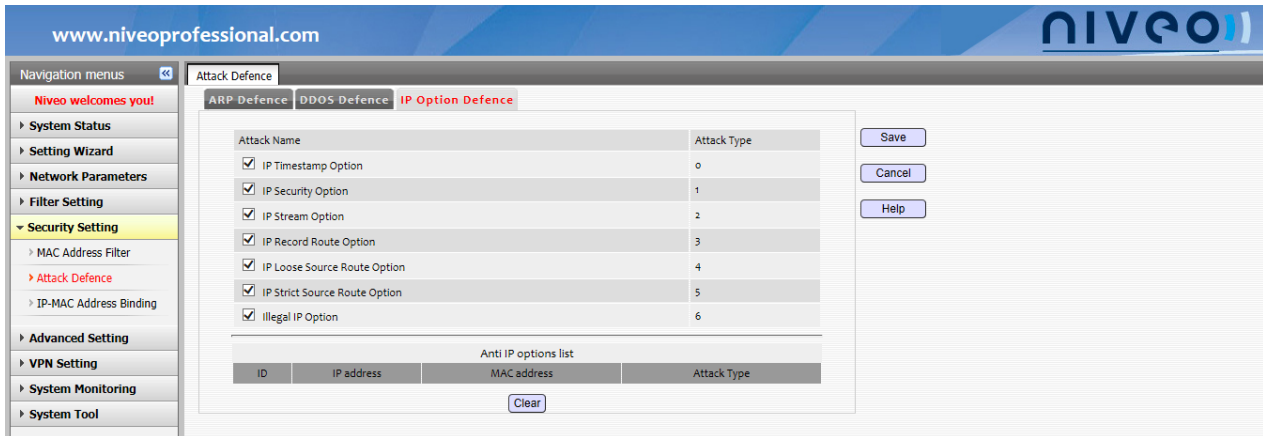


2. DDOS Defence



- **ICMP Flood:** If a destination host receives ICMP request packets in one second which exceeds the specified value, it means that the destination IP is under the attack of ICMP Flood.
- **UDP Flood:** If a certain port on a destination host receives UDP packets in one second which exceeds the specified value, it means that the port is under the attack of UDP Flood.
- **SYN Flood:** if a certain port on a destination host receives TCP SYN packets in one seconds which exceeds the specified the value, it means that the port is under the attack of SYN Flood.

3. IP Option Defence

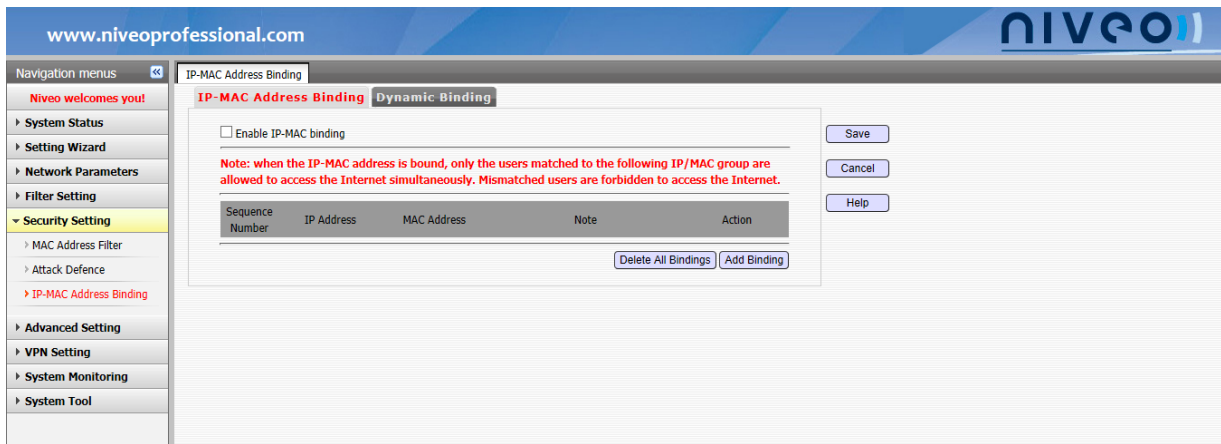


- **IP Timestamp Option:** Indicates whether to check the IP from the designated area contains the Internet Timestamp option.
- **IP Security Option:** Indicate whether to check the IP from the designated area contains the Security option.
- **IP Stream Option:** Indicate whether to check the IP from the designated area contains the Stream ID option.
- **IP Record Route Option:** Indicate whether to check the IP from the designated area contains the Record Route option.
- **IP Loose Source Route Option:** Indicate whether to check the IP from the designated area contains the Loose Source Route option.
- **IP Strict Source Route Option:** Indicate whether to check the IP from the designated area contains the Strict Source Route option.
- **Illegal IP Option:** Indicate whether to check the integrity or correctness of the IP from the designated area.

IP-MAC Binding

1. IP-MAC Address Binding

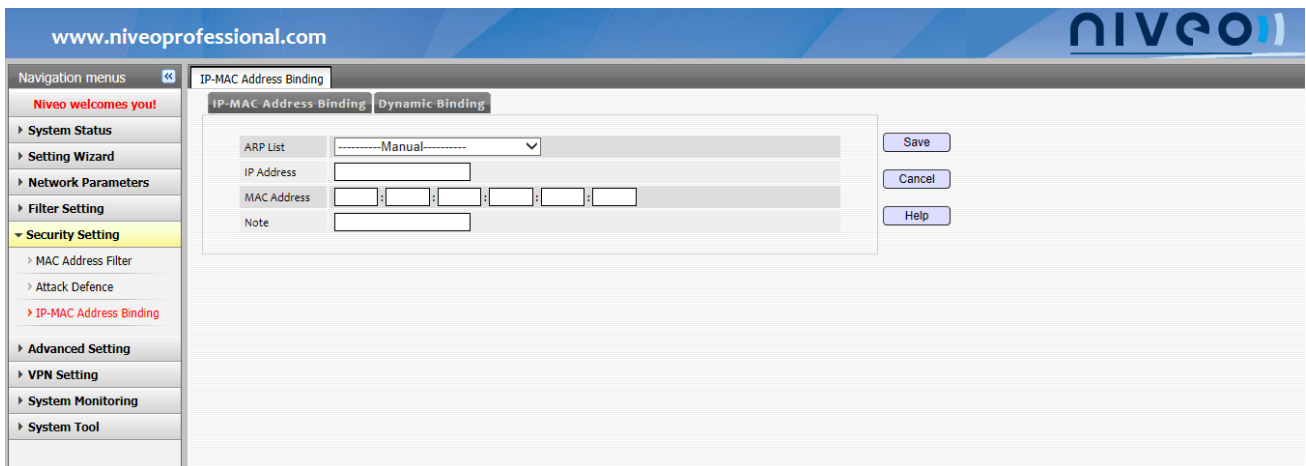
This feature is applied to bind the IP addresses and MAC addresses in the LAN. Once the address binding is configured, the specified IP address can just be used by the specified IP address. In this case, IP address in the LAN cannot be modified randomly and IP address conflicts will disappear.



Click **IP-MAC Address Binding**.

Enable IP-MAC binding: check to enable it.

Click **Add Binding**, and the following Binding figure will be displayed.

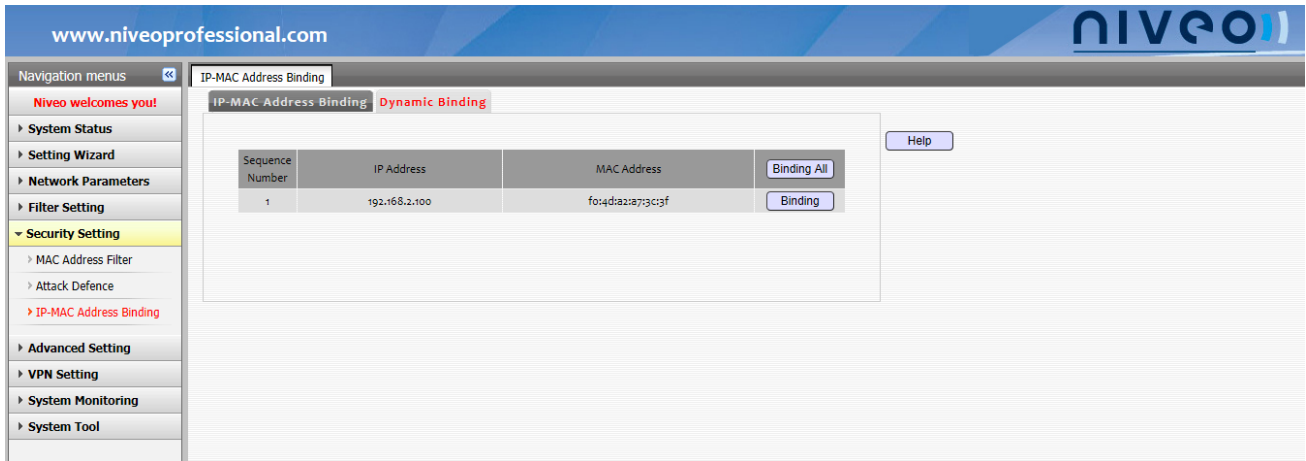


- **ARP List:** From the pull-down menu of the ARP list field, you can select the IP-MAC pair of the host which is already connected to the router. Or you can select “Manual” to add IP-MAC pair manually.
- **IP Address:** Enter the IP address you need to bind.
- **MAC Address:** Enter the MAC address you need to bind.
- **Note:** Edit a brief description about the IP-MAC pair binding rule.

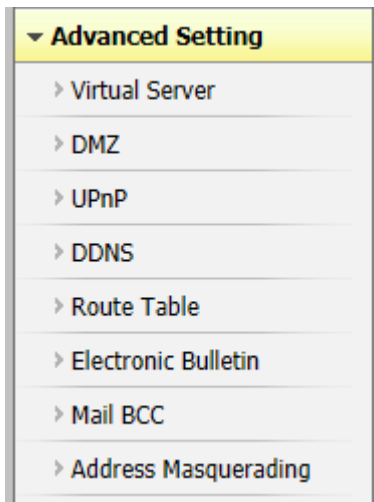
2. Dynamic Binding

Click **Dynamic Binding** to view the binding list. You will see the accessing information: IP address and MAC address.

You can also bind the single one or all to quickly enable Dynamic Binding feature.

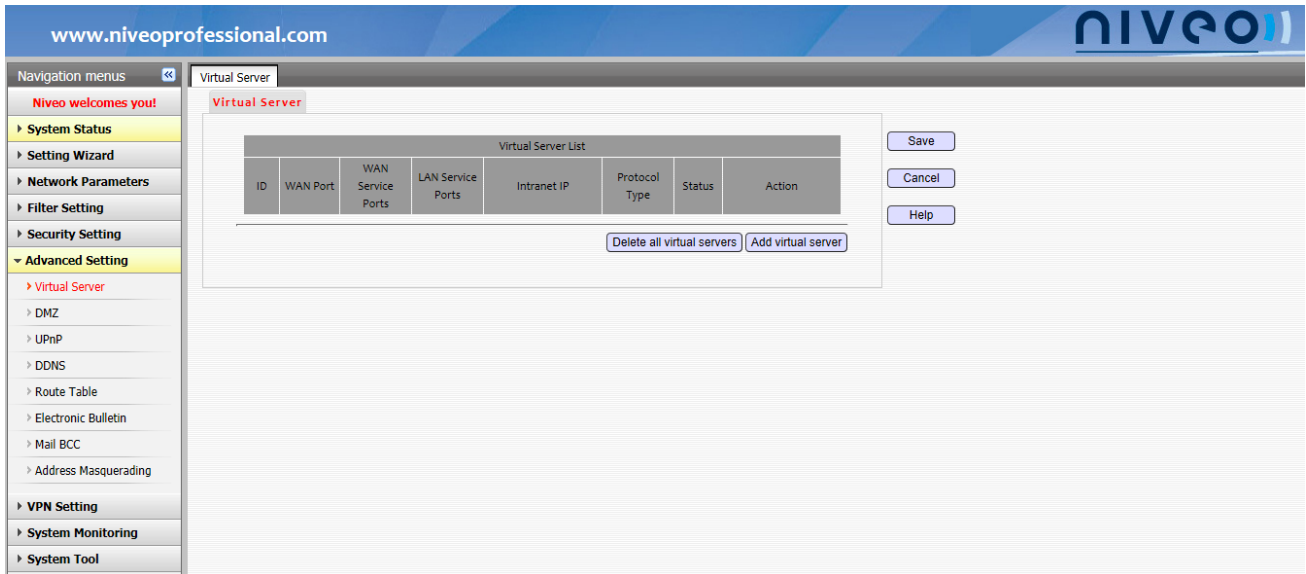


6 Advanced

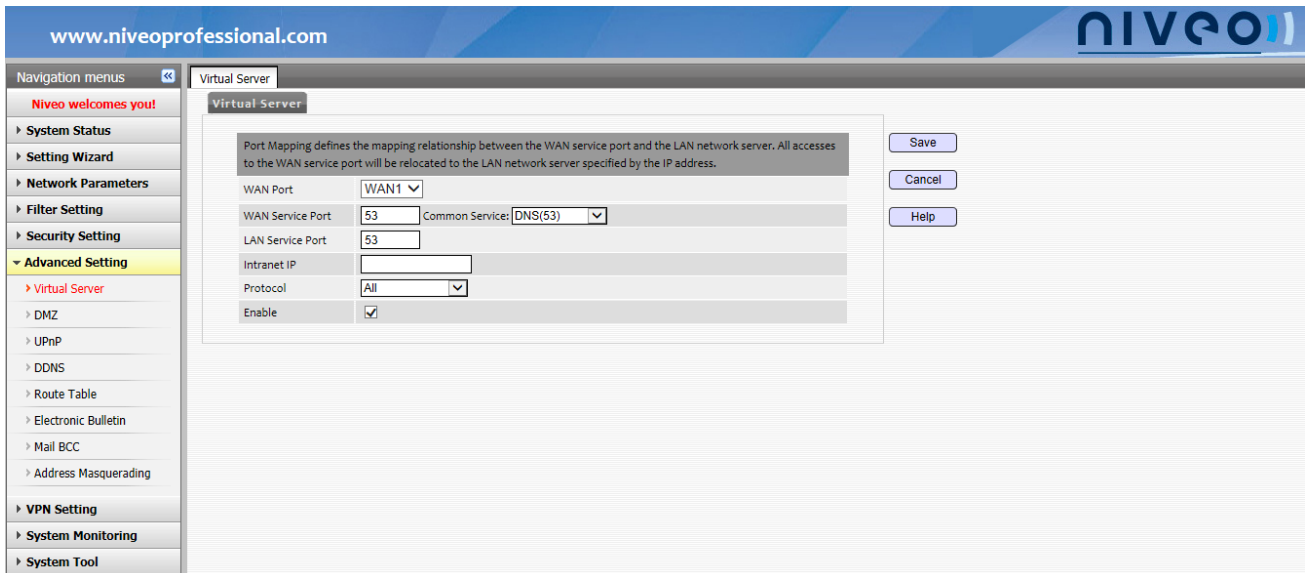


Virtual Server

Virtual Server is to set the mapping between the WAN service ports and LAN server, enabling all access to the WAN service ports to be re-specified to the LAN server via IP address.



Click **Add virtual server** to set it.



- **WAN Port:** Select a WAN port to be a mapping port.
- **WAN Service Port:** It is the port that the PC in LAN mapping to WAN.
- **Common Service:** Contain some common service ports, such as DNS(53), FTP(21), GOPHER(70), HTTP(80), NNTP(1190), POP3(110), PPTP(1723), SMTP(25), SOCK(1080), TELNET(23). For the service ports not covered here, you can add manually.
- **LAN Service Port:** It is the port of the PC in LAN.
- **Intranet IP:** Specify a host IP in the LAN to be Server.
- **Protocol:** There are three types of protocol: **TCP**, **UDP** and **All**. If you are not sure about which one to use, "All" is the best choice.
- **Enable:** Check this box to enable the rule.

For example, you create a Web server in the LAN (IP:192.168.2.10/80), if you hope that you can use <http://x.x.x.x:40> (x.x.x.x is the WAN2 IP address of your Router)to access the Web server, you can configure it as the following:

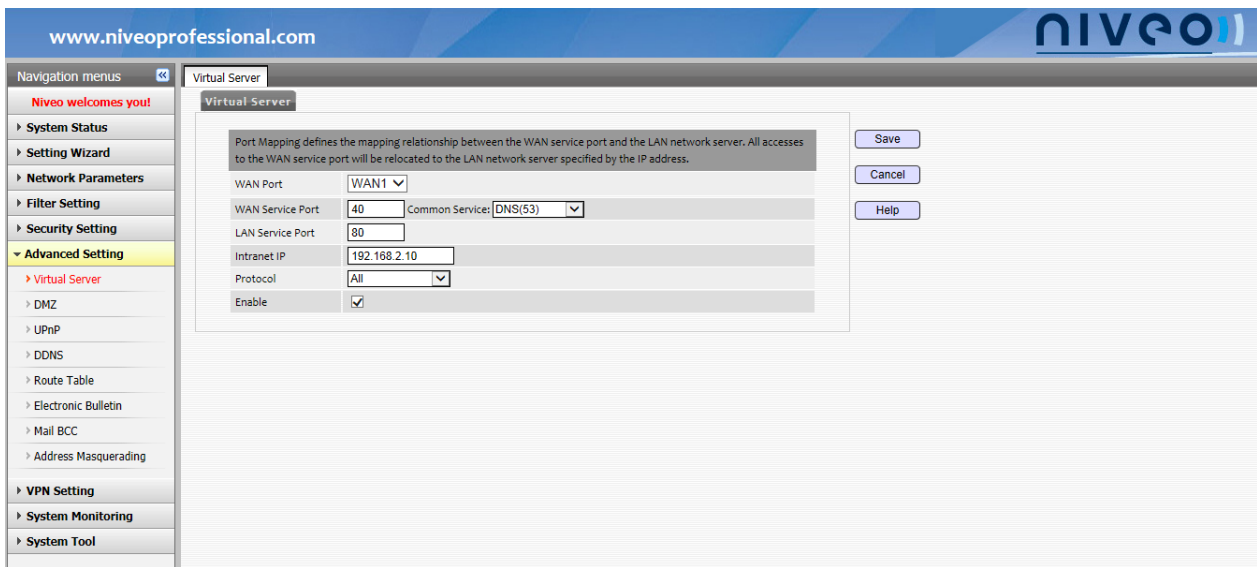
WAN port: Enter **40**,

LAN port: Enter **80**,

Intranet IP: Enter **192.168.2.10**

Protocol: Select **All, Enable**

Click **Save** to take the settings into effect.

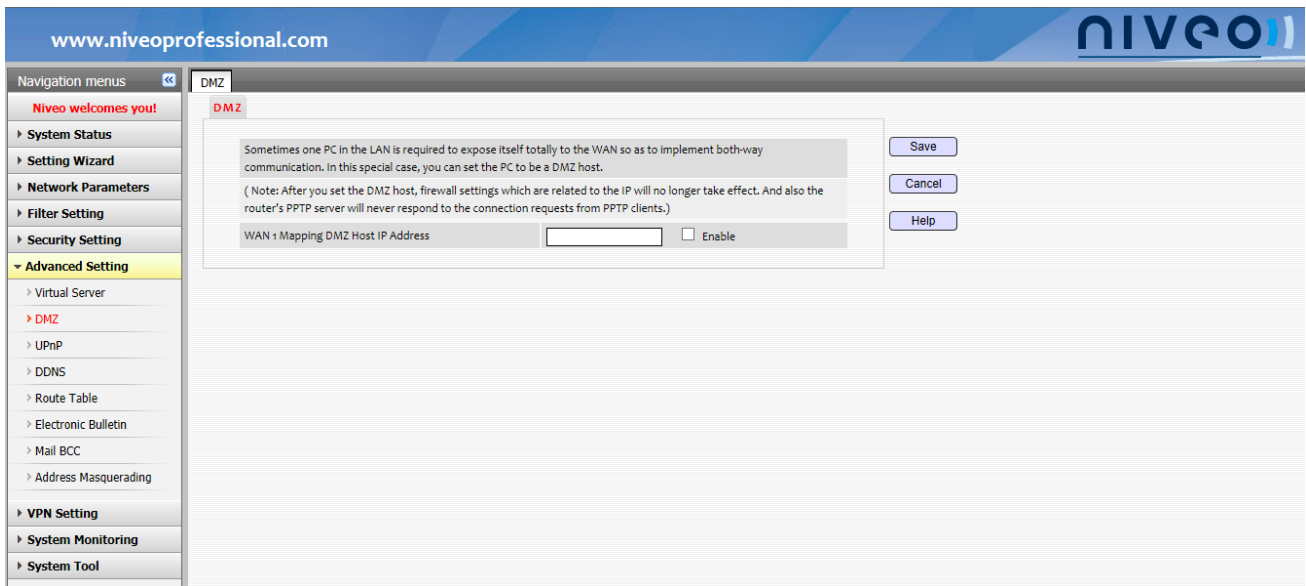


Note:

If you enter 80 as the WAN port of the Virtual Server, you need to set a value except 80 in the WAN Access Control in Network, for example the default value 8080, or there will be conflicts, and the virtual server will take no effect.

DMZ

In some special applications, it's necessary for a computer in the LAN to expose itself to the WAN in order to achieve dual-communication. In this case, you can configure this computer as a DMZ host.



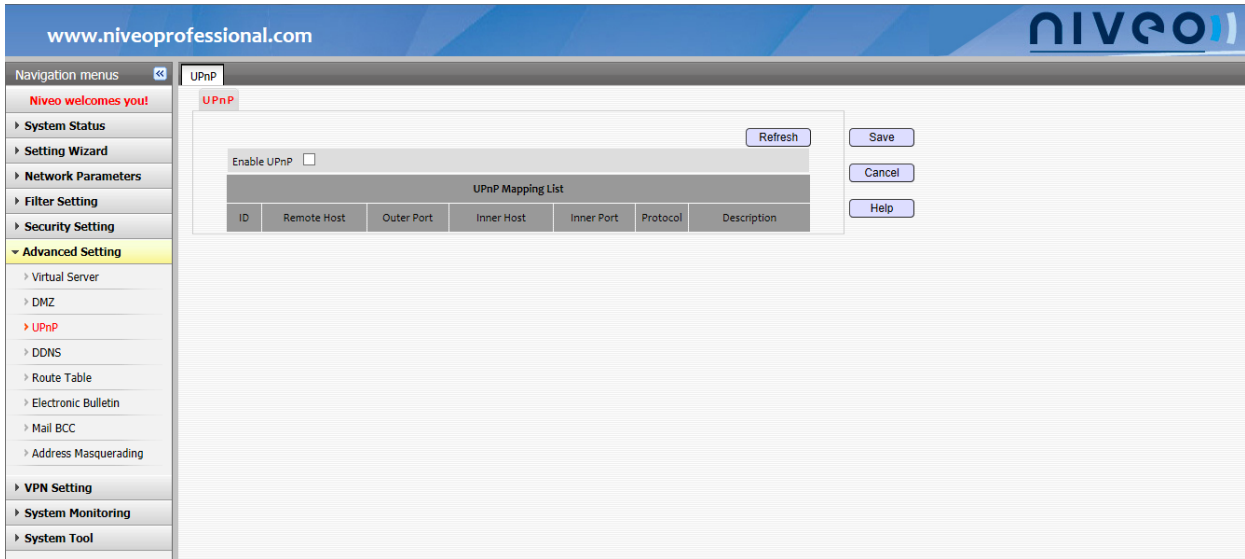
- **WAN Mapping DMZ IP Address:** Enter the address into this field.
- **Enable:** Click Enable to save the DMZ settings.

⚠ Note:

1. After DMZ is set, Firewall settings relevant to the IP address are not effective anymore.
2. When hosts in the WAN access the DMZ host, the IP address they access is the WAN IP address.

UPnP

The Router supports Universal Plug and Play, applied to Windows ME/Windows XP or higher (Note: system should be integrated, and installed with Directx9.0 or higher) or UPnP-supported application software support. For example, if you install one P2P software in your Windows XP, when uploading and downloading, you can use the UPnP protocol. Enable UPnP, and you will find that when you start up your P2P software, you can see the port switchover information, which is provided when the P2P software send requests.

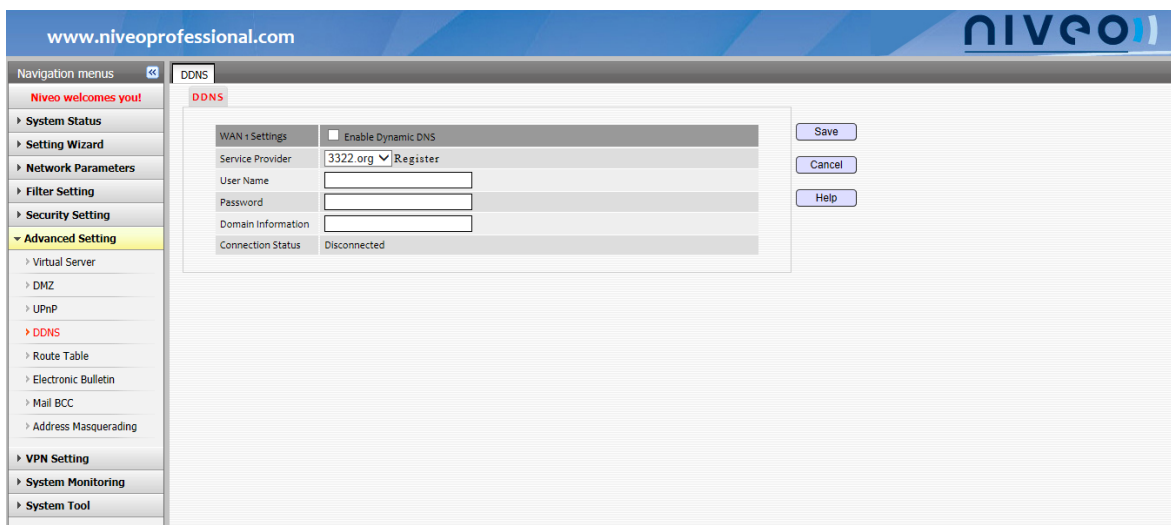


- **ID:** The UPnP mapping **NO**.
- **Remote Host:** The address of remote host to receive and send responds.
- **Outer Port:** The port set on the router is used to map to the outer.
- **Inner Host:** The address of inner host to receive and send responds.
- **Inner Port:** The host port which needs to be mapped.
- **Protocol:** Indicates the mapping protocol.
- **Description:** Displays information of mapped software.

DDNS

Setting DDNS to allow hosts use a domain to access your Router or Virtual server.

4 WAN interfaces on the Router can be set with the DDNS feature, of which configuration methods are the same. Here takes WAN 1 as an example.

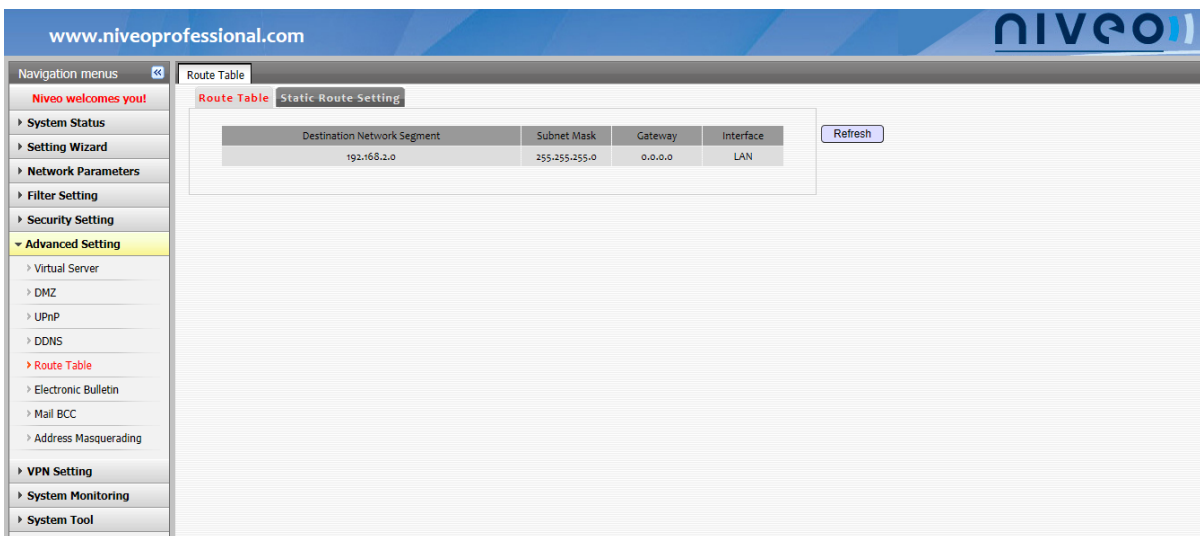


- **Enable Dynamic DNS:** Check the box to enable dynamic DNS.
- **Service Provider:** Select a DDNS service provider. It supports three types of DDNS service: 3322.org, 88ip.cn and gwnway.
- **User Name:** The username you registered on the DDNS server.
- **Password:** The password to login to the DDNS server.
- **Domain Information:** The host name you registered on the DDNS server.
- **Connection Status:** Displays the current status of connection to DDNS.

Route Table

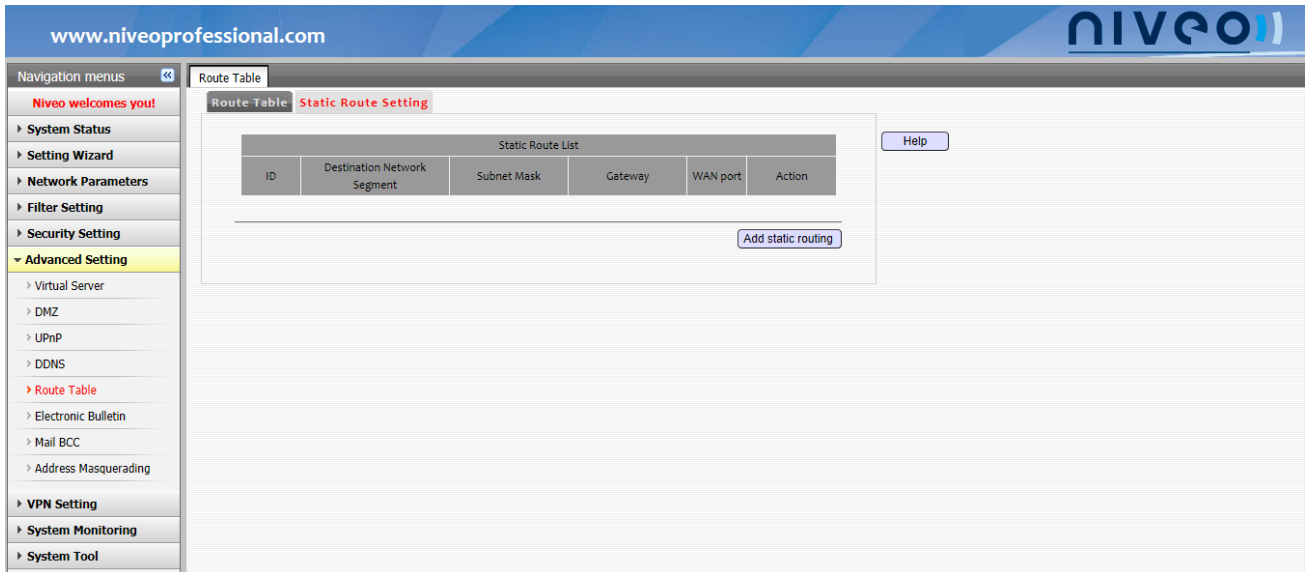
1. Route Table

To view the content of the Router.



2. Static Route Setting

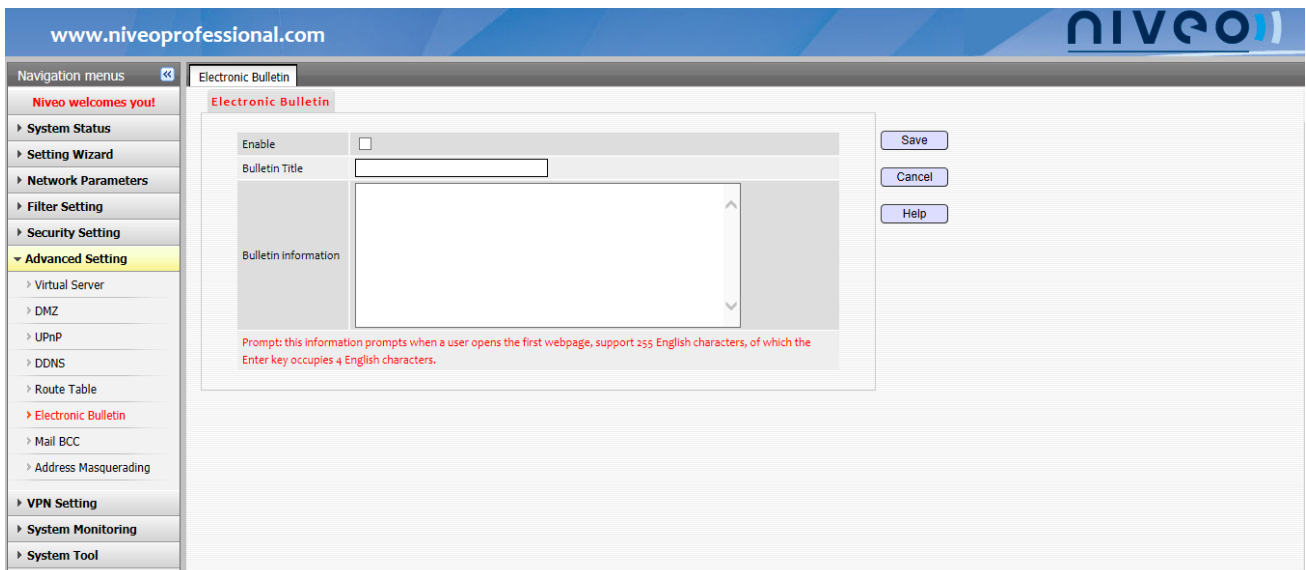
Click **Add static routing** to specify the static route rules.



- **Destination Network Segment:** Displays the IP address segment of the destination network.
- **Subnet Mask:** Displays the mask of the destination IP address.
- **Gateway:** Displays the IP address of the next pop router entry.
- **WAN Port:** Specify the corresponding LAN port or WAN port.

E-bulletin

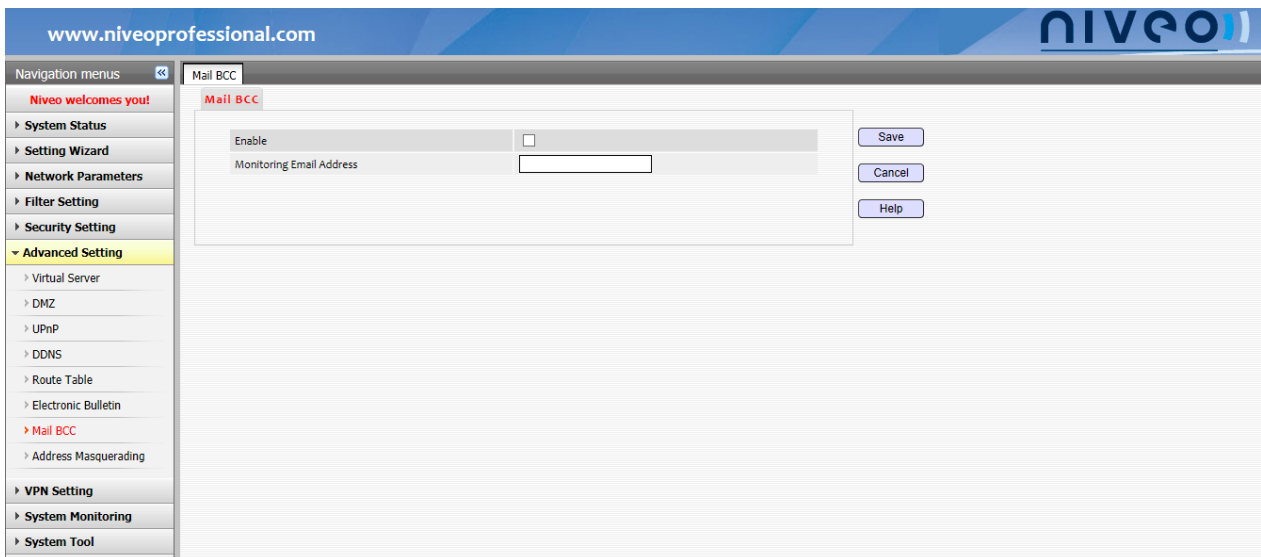
The E-bulletin information will prompt when you open the first Intranet websites.



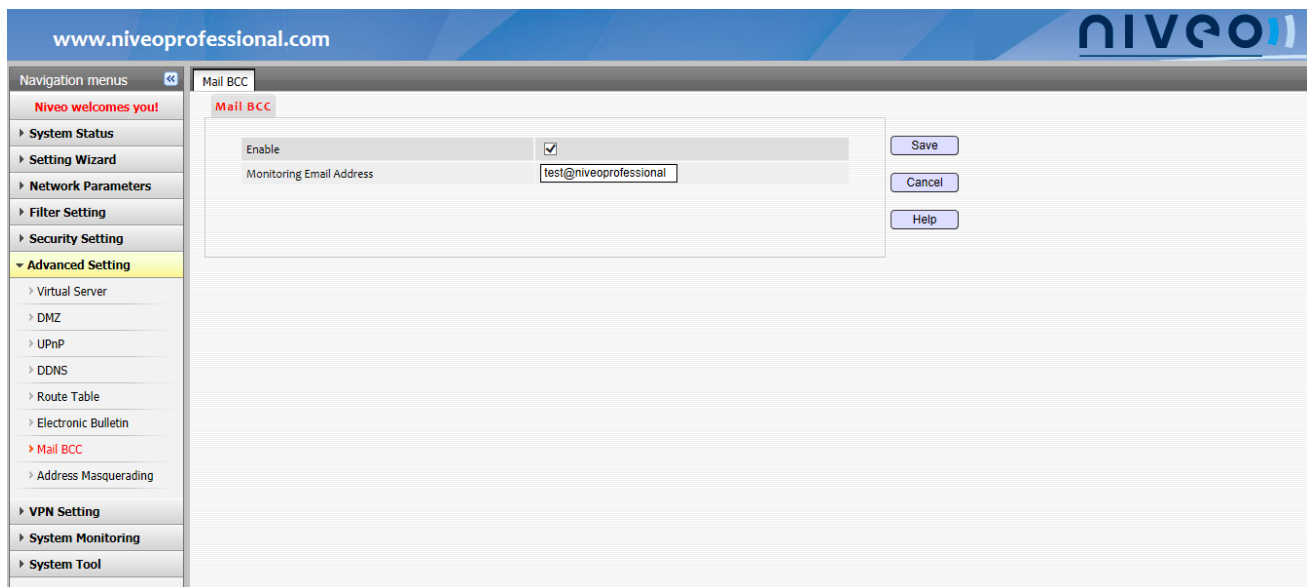
- **Enable:** Check this box to enable E-bulletin feature.
- **Bulletin Title:** Display the title of the E-bulletin.
- **Bulletin Information:** Display the details info of the bulletin.

Mail BCC

Enable this function, to monitor emails of all the mail clients (Outlook, Foxmail, etc.) of all hosts on the Router's downlink side, effectively improve the safety and secrecy. All the emails will be received by the monitoring address you set on the following interface.



- **Enable:** Check this box to enable mail monitoring feature.
- **Monitoring Email Address:** Specify a mail address to be monitored. The mail address must be registered legally on the Internet. Only one mail address can be monitored.



For example: when you send an email in any email client on any computer in the LAN, if your source address is test01@niveoprofessional.com, your destination address is test@niveoprofessional.com, and you enter

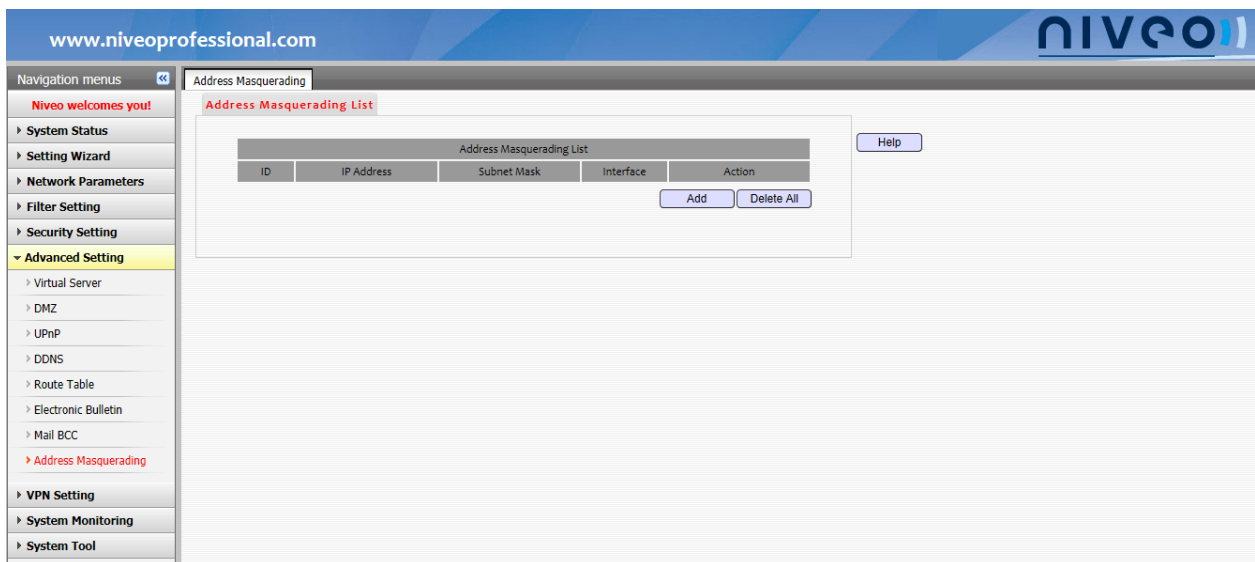
test@niveoprofessional.com in the Monitoring Email Address, after you send an email, you monitoring email client can also receive an email from test01.

Note:

The email software can be only the client email software, such as foxmail and outlook. Emails sent via any other email client software or web email ways cannot be monitored.

Address Masquerading

This feature is to implement NAT on the selected interface with the specified IP address or network. In addition, if you set the static Routing LAN interface, computers in the LAN in different network segments can access the Internet.



- **IP Address:** Means the IP or its IP segment of the Client PC.
- **Subnet Mask:** The subnet mask of the host IP.
- **Interface:** Configure a WAN port, WAN1, WAN2, WAN3, WAN4 or All.

For example: The LAN IP is 192.168.2.1.

Network configuration of one computer in the LAN:

IP: 192.168.20.100

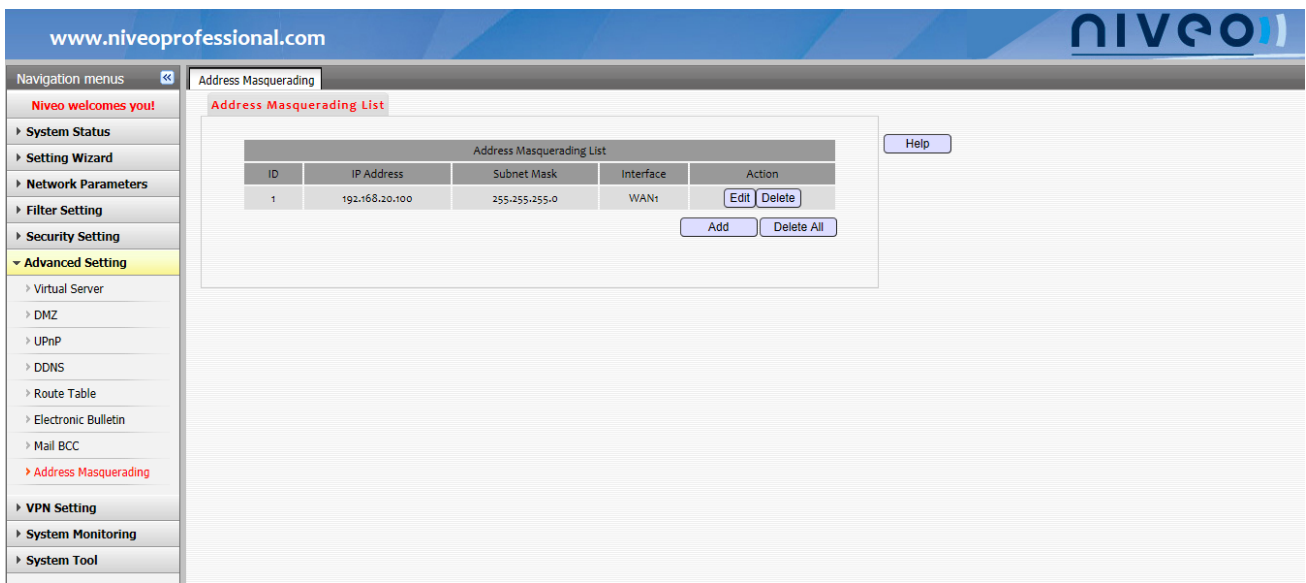
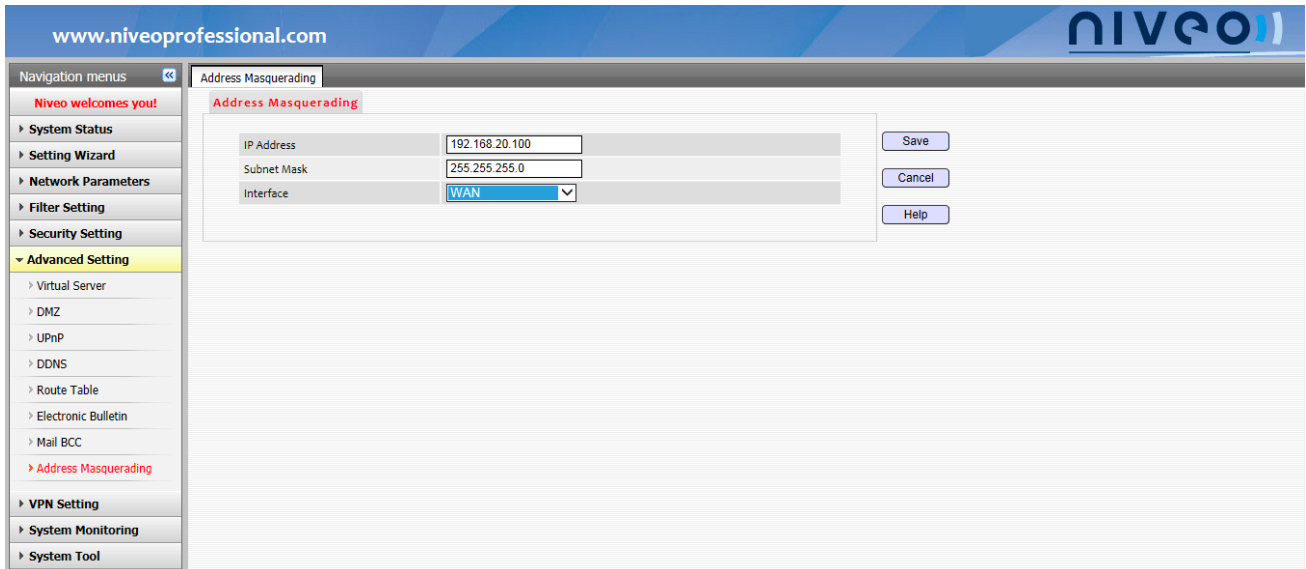
Subnet mask: 255.255.255.0

You need to set the Gateway and DNS as the Router's LAN IP as the following.

Gateway: 192.168.2.1

DNS: 192.168.0.1

If you need to connect WAN 1 to the Internet, you need to configure the Address Masquerading shown as the figure below.

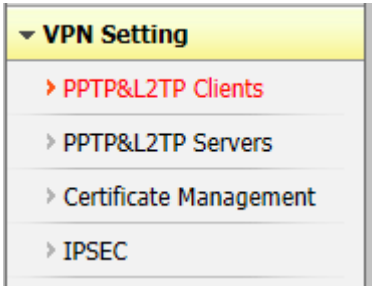


Note:

Before enabling this feature, you must disable Attack Defence to take the Address Masquerading into effect.

7 VPN Setting

VPN is short for virtual private network. This Router has 3 modes to create a VPN: PPTP, L2TP and IPSEC. To enter the configuration interface of a certain feature, simply click a corresponding tab. Features are detailed below.



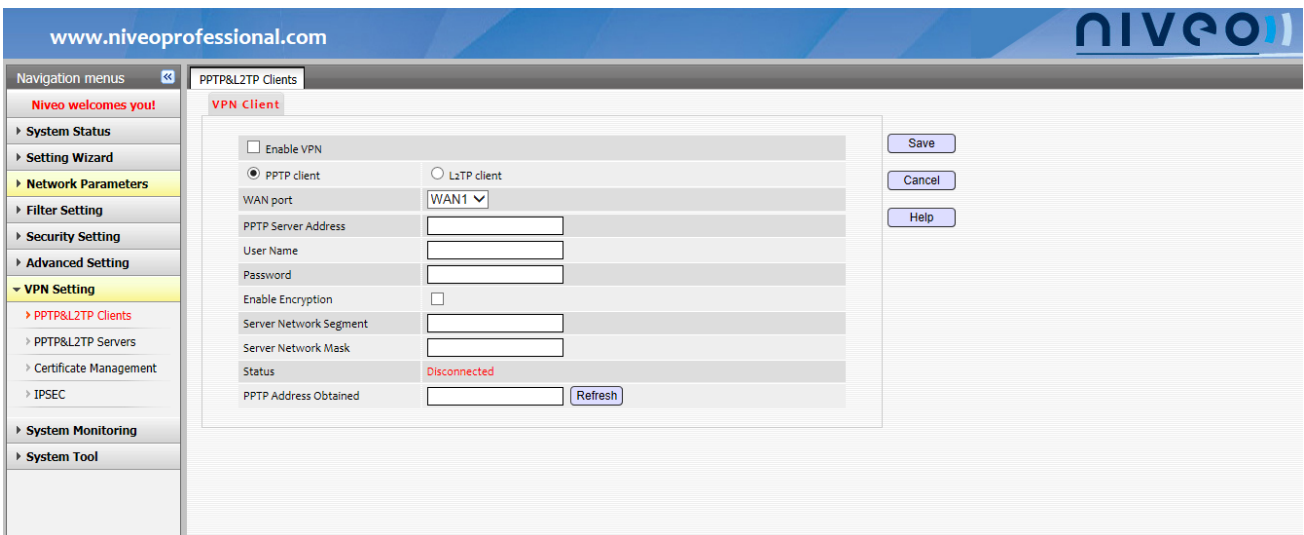
PPTP & L2TP Clients

This section includes PPTP client and L2TP client, which allows a VPN router client to connect to a VPN router server. For example: A corporate branch and its headquarter, or a can use this connection type to implement mutual and secure access to each other’s resources.

Note:

PPTP client and L2TP client cannot be enabled concurrently. Enabling either one, the other will be disabled automatically.

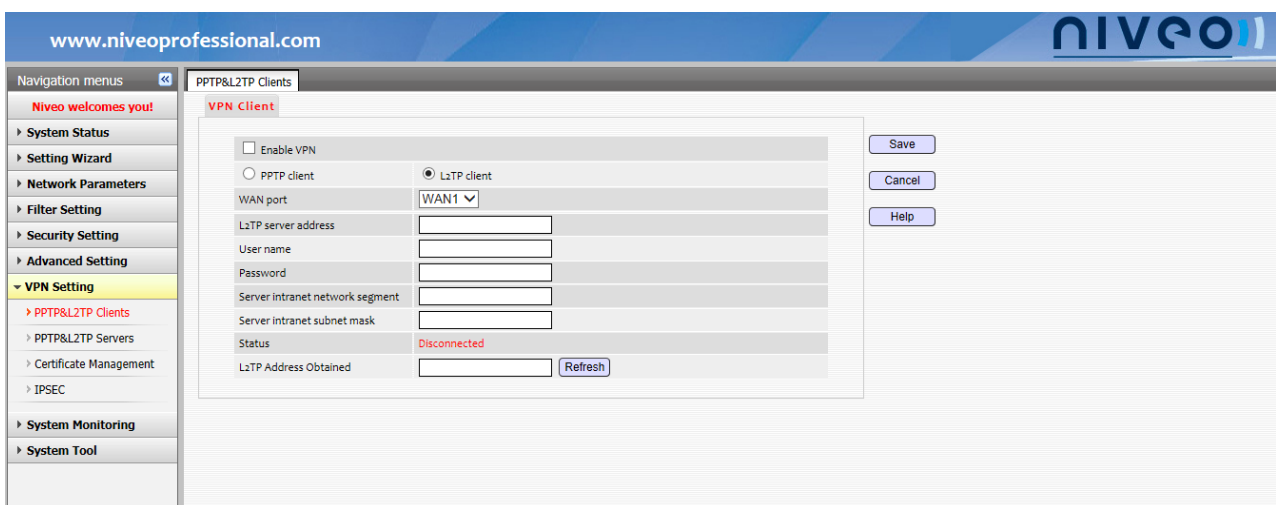
1. PPTP Client



- **VPN Client:** PPTP client and L2TP client can only be enabled separately. If you select **PPTP Client**, all configurations apply to the PPTP Client feature.
- **Enable VPN:** Enable/disable the VPN client feature. To enable PPTP client feature, check **Enable VPN** and select **PPTP Client**.
- **WAN Port:** Specify a WAN port for PPTP dialup.

- **PPTP Server Address:** Enter the IP address or domain name of the PPTP server you want to connect.
- **User Name/Password:** Enter the user name and password assigned by the PPTP server.
- **Enable Encryption:** Enable/disable data encryption. Note that this setting must exactly match the server.
- **Server Network Segment/Mask:** Specify the local network segment and mask of the PPTP server.
- **Status:** Displays connection status of PPTP client.
- **PPTP Address Obtained:** Display the IP address obtained from the PPTP server.

2. L2TP Client

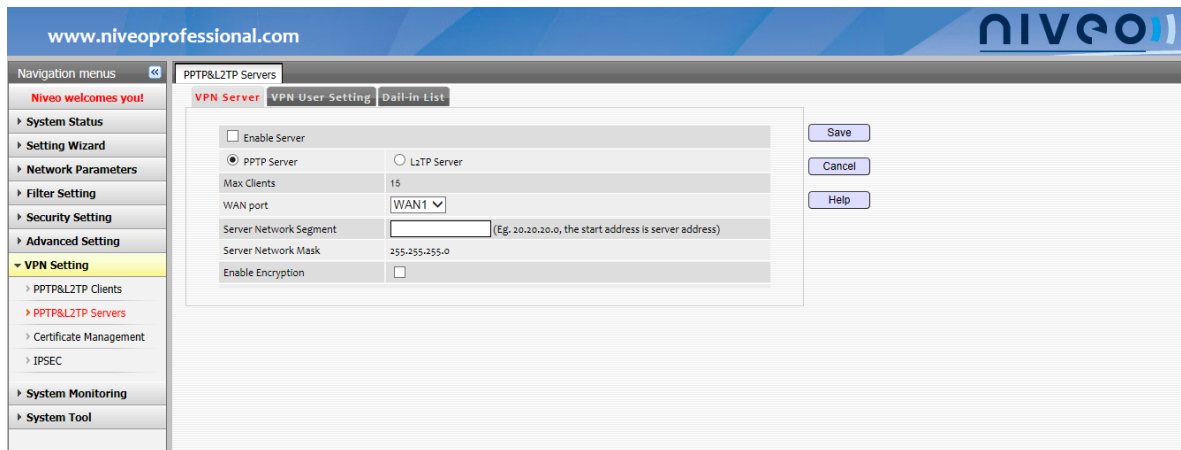


- **VPN Client:** PPTP client and L2TP client can only be enabled separately. If you select **L2TP Client**, all configurations apply to the L2TP Client feature.
- **Enable VPN:** Enable/disable the client feature. To enable L2TP client feature, check **Enable VPN** and select **L2TP Client**. PPTP Client feature will be disabled automatically.
- **WAN Port:** Specify a WAN port for L2TP dialup.
- **L2TP Server Address:** Enter the IP address of the L2TP server you want to connect.
- **User Name/Password:** Enter the user name and password assigned by the L2TP server.
- **Server Network Segment/Mask:** Specify the local network segment and mask of the L2TP server.
- **Status:** Displays connection status of L2TP client.
- **L2TP Address Obtained:** Display the IP address obtained from the L2TP server.

PPTP & L2TP Servers

1. VPN Server

Here you can configure the PPTP server and L2TP server.

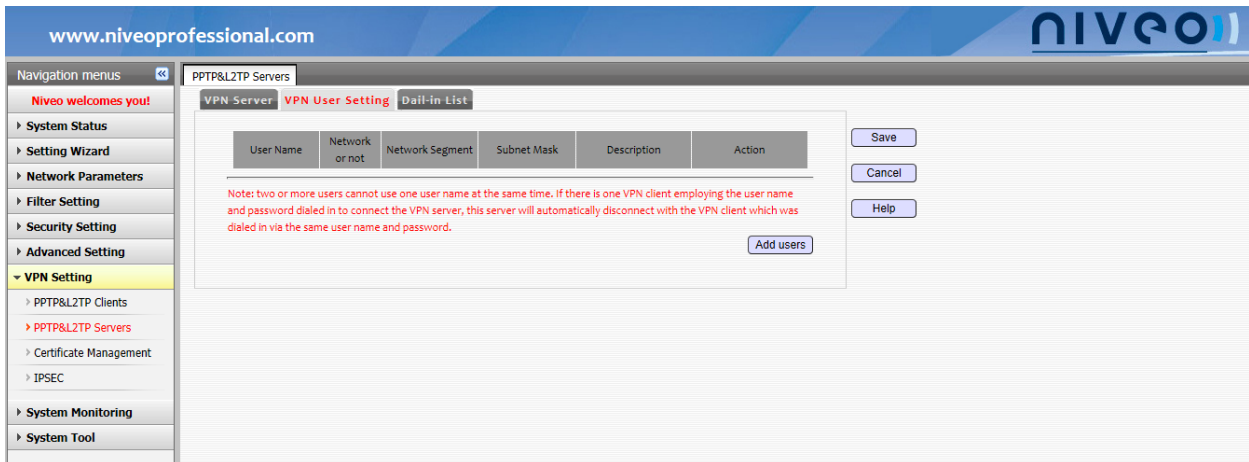


PPTP server and L2TP server cannot be enabled concurrently. Enabling either one, the other will be disabled automatically. All configurations apply to the L2TP server feature if you select **L2TP Server**, and PPTP server if you select **PPTP Server**.

- **Enable Server:** Enable/disable the server feature. To enable PPTP server feature, check **Enable Server** and select **PPTP Server**. To enable L2TP server feature, check **Enable Server** and select **L2TP Server**.
- **Max Clients:** Maximum PPTP/L2TP clients allowed by the server.
- **WAN Port:** Specify a WAN port used by the server to listen for PPTP/L2TP clients.
- **Server Network Segment:** Specify the IP address segment to assign to clients. The start IP address in the segment serves as the server's IP address and the others will be assigned to clients. For example, if you enable the PPTP server and the client's network segment is 20.20.20.0, then the IP address of the PPTP server is 20.20.20.1 and the IP address of the first connected client is 20.20.20.2.
- **Enable encryption:** Only PPTP sever needs to set whether to enable PPTP communication data. PPTP sever and PPTP client must keep accordance, or they cannot communicate with each other. If you select to enable encryption, client also needs to be enabled encryption in order to access the Internet. If you don't enable the encryption, encryption of the client cannot be enabled as well.

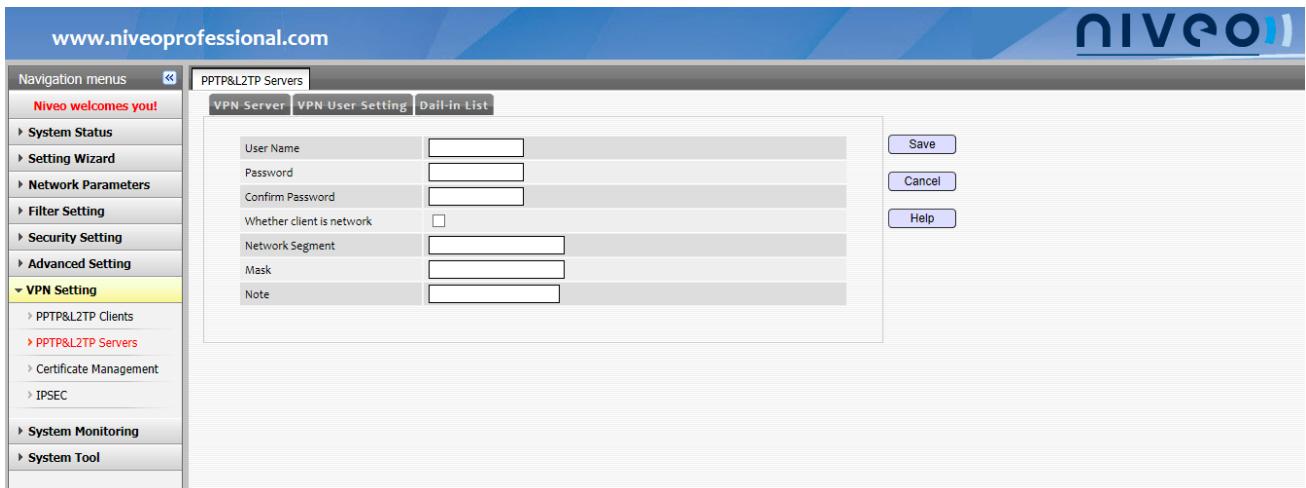
2. VPN User Setup

Here you can see the configured VPN accounts for PPTP/L2TP client dialup.



- **Add Users:** Click to add a user account for PPTP/L2TP client dialup. Up to 15 accounts can be added.
- **Edit:** Click to modify a corresponding account.
- **Delete:** Click to delete a corresponding account.

Click **Add Users**, and enter the following figure to start configure the user.

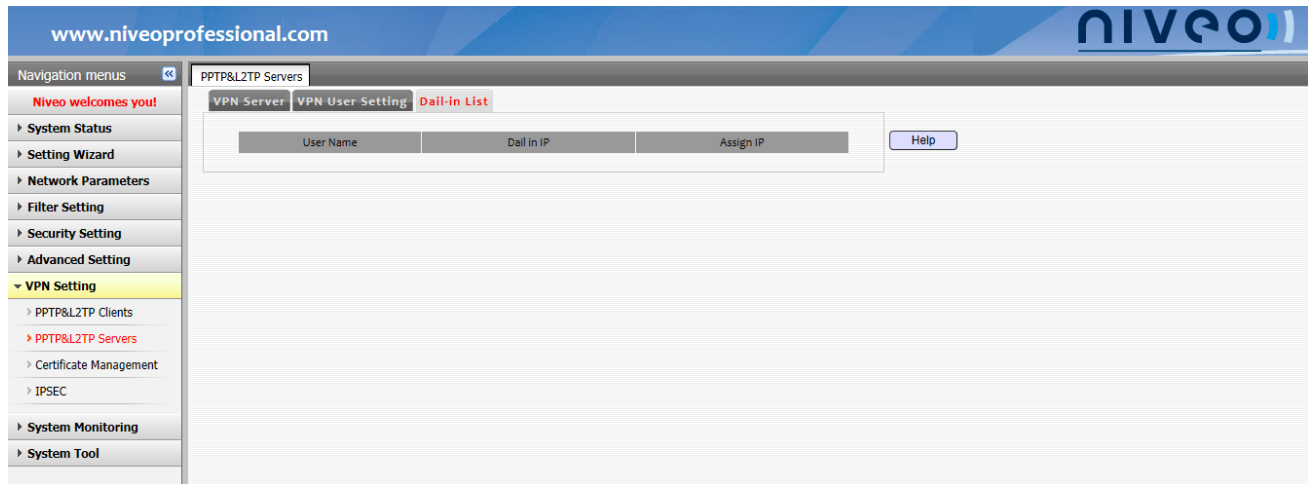


- **User Name/Password/Confirm Password:** The user name and password used by client to connect to the VPN server.
- **Whether client is network:** If the client is a computer, unchecked. If the client is a router. It must be checked, or the PC in the client router's intranet cannot communicate with another PC in this sever router's intranet.

- **Network Segment/mask:** If you check the client to be network. You need to set the client's LAN segment and subnet mask, i.e., the client sever router's intranet segment.
- **Note:** Briefly describes the configuration. This field is optional.

3. Dial-in List

Here you can view clients that have connected to this VPN server.



- **User Name:** Displays the user name(s) used by the connected client(s) for dialup.
- **Dial-in IP:** Displays the IP address(es) of the connected client(s).
- **Assigned IP:** Displays the IP address(es) assigned by the VPN server to connected client(s).

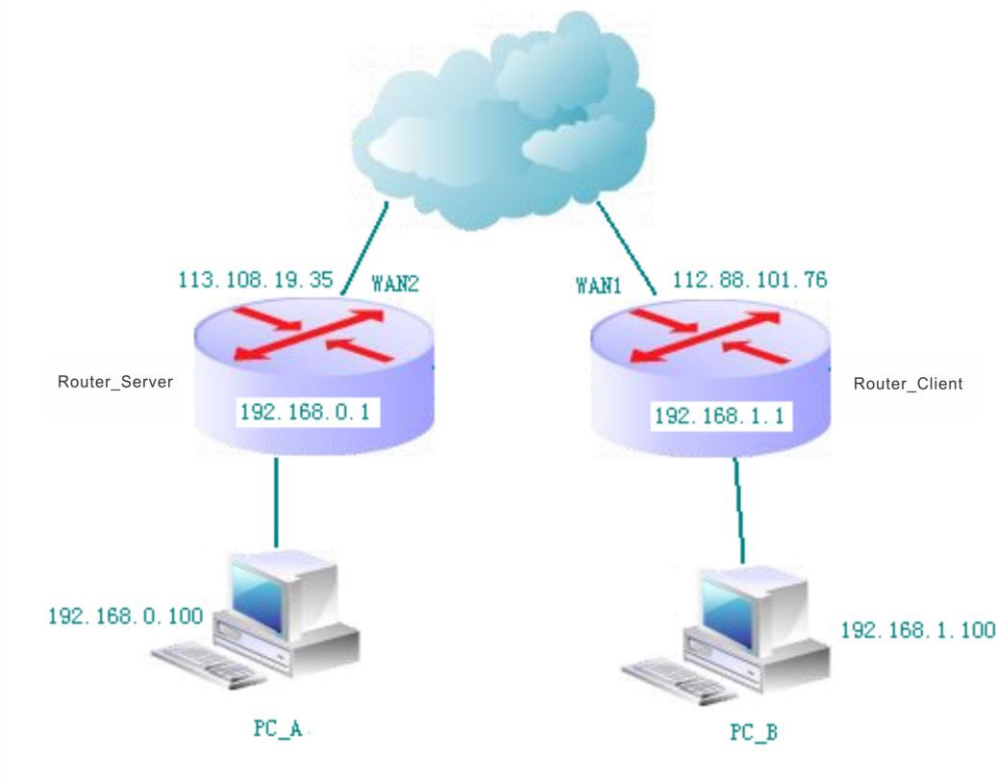
Note:

Note below when configuring VPN server and client.

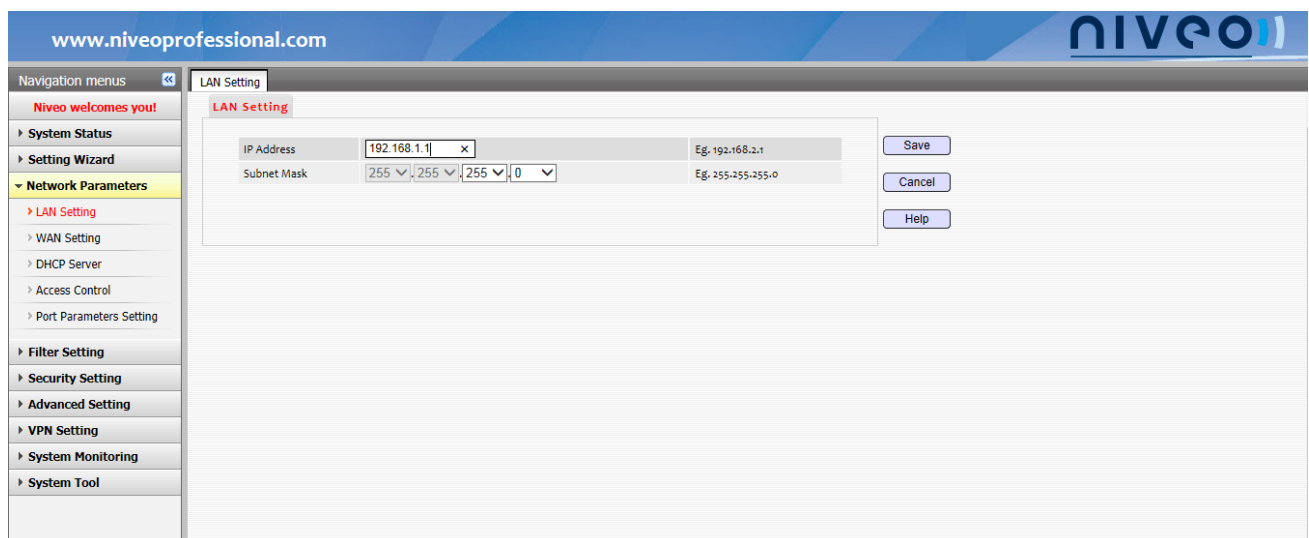
1. PPTP client and L2TP client cannot be enabled concurrently. Enabling either one, the other will be disabled automatically. PPTP server and L2TP server cannot be enabled concurrently. Enabling either one, the other will be disabled automatically.
2. Before creating a VPN, make sure the involved server router and client router can intercommunicate properly. For example, both directly dial in to access the Internet.
3. When configuring PPTP or L2TP client, enter the WAN IP address of the PPTP or L2TP server side instead of the IP address you configure in the PPTP & L2TP Server interface in the PPTP/L2TP Server Address field.
4. Encryption settings must be the same on both PPTP server side and client side.
5. To let a VPN server and client, either of which has its own subnet work, can access each other, you must configure the corresponding subnet works correctly.

4. Application

Steps of two Routers building up VPNs via PPTP. (Router_Client and Router_Server)

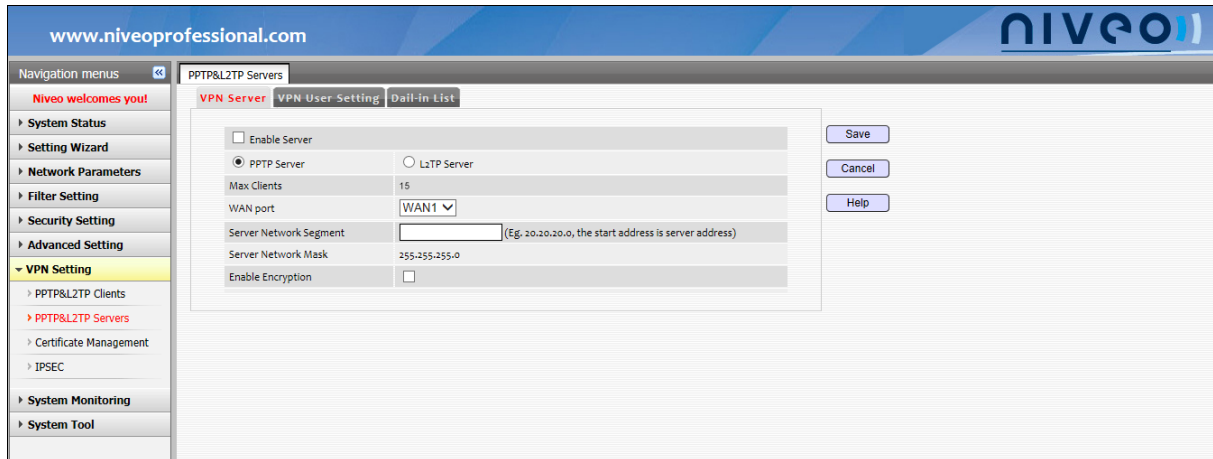


Step 1: LAN IPs of Router_Client and Router_Server can not be in the same network segment. The default LAN IP of these two Routers are both 192.168.0.1, so you need to change one Router’s LAN IP. Here we change the Router_Client LAN IP into 192.168.1.1

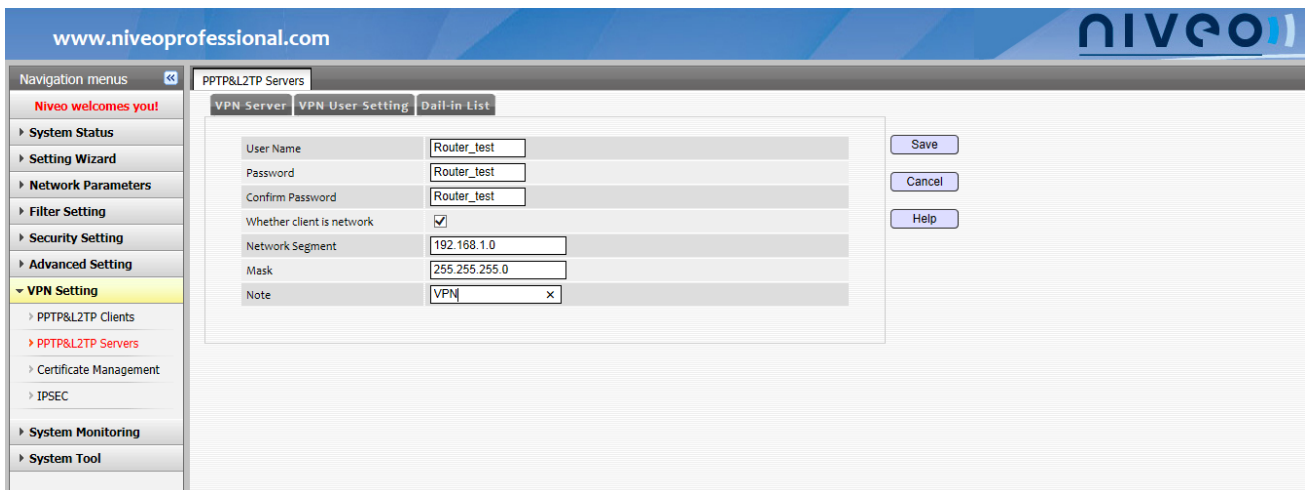


Step 2: Router_Server WAN2 obtains IP: 113.108.19.35 via PPPoE; Router_Client WAN1 obtains 112.88.101.76 via PPPoE. PC_A can ping 112.88.101.76 successfully, and PC_B can ping 113.108.19.35 successfully.

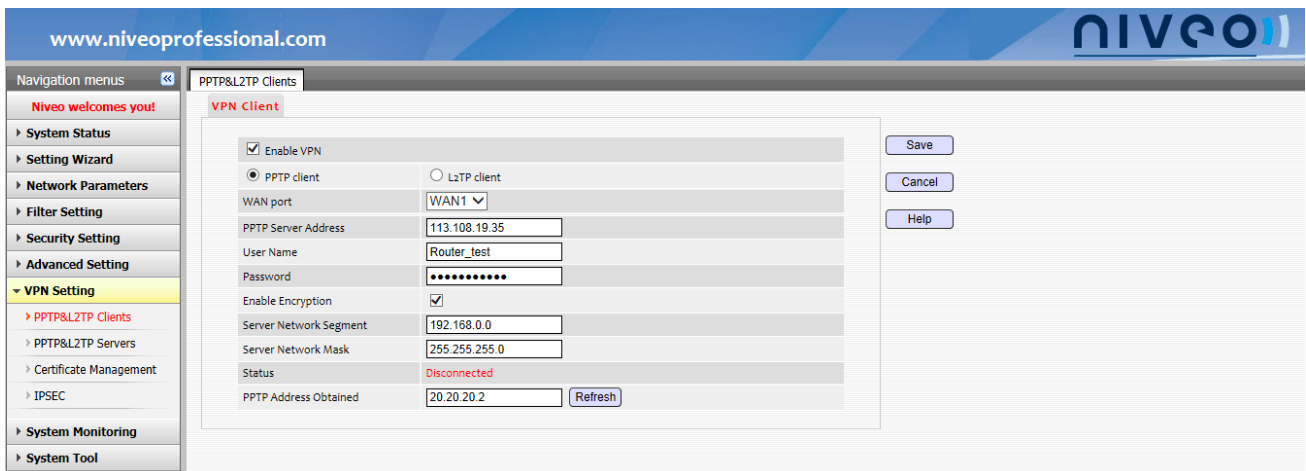
Step 3: Enable PPTP server on Router_Server, detailed configuration shown below.



Step 4: Add a user Router_test on Router_Server, detailed configuration shown below.



Step 5: Enable PPTP server on Router_Client as the following figure shows.

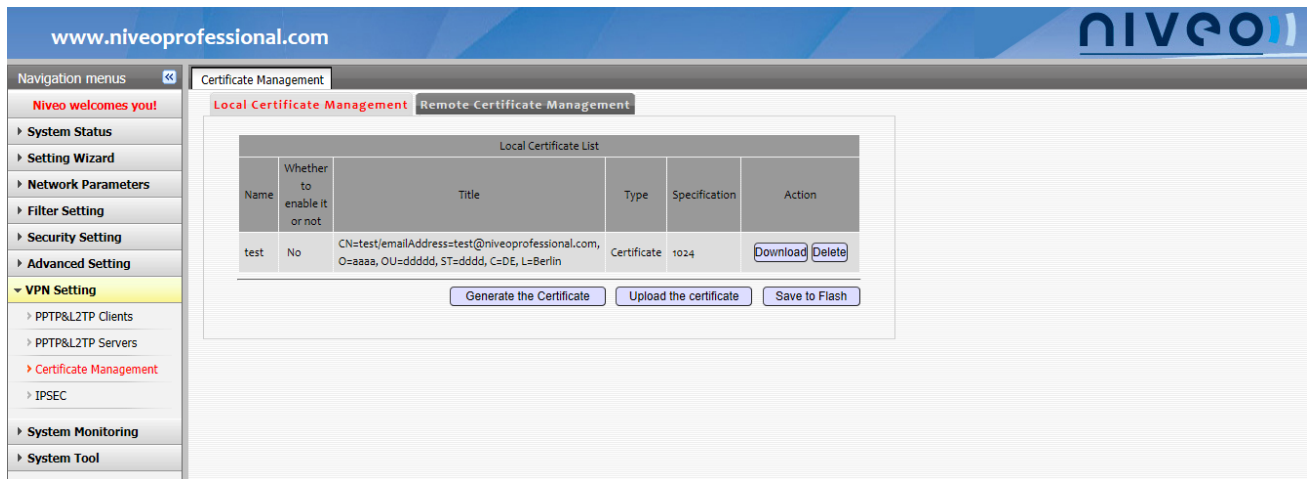


When PPTP server obtains the IP, between these two routers are built up PPTP VPN. PCs on the router's downlink side can communicate with each other directly. PC_A can straightly ping PC_B IP 192.168.1.100 successfully, PC_B can directly ping PC_A IP 192.168.0.100 successfully.

Certificate Management

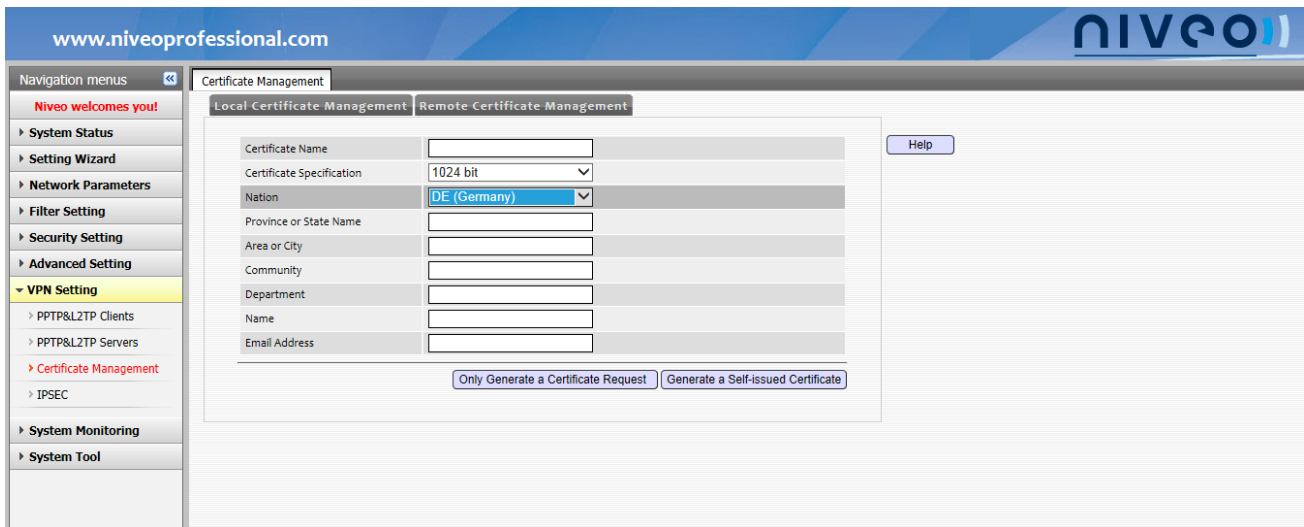
This is used to manage the digital certificates of local and remote routers for ID certification when IPSEC VPN created.

1. Local Certificate Management



- **Local Certificate List:** Displays all certificates of the local router.
- **Download:** Download the requests of .cer-certificates and .csr-certificates to the local disk.
- **Delete:** Delete the current digital certificate from the Router. You cannot delete a certificate in use.
- **Import the Certificate:** When the certificate request is generated, click this button to import the issued digital certificate. After you lead it successfully, this button will disappear.
- **Generate the Certificate:** Generate the digital certificate or certificate requests.
- **Upload the Certificate:** Upload the digital certificate and secret key on the local disk to the system.
- **Save to Flash:** Save all the certificates of the Router to Flash. If you do not save them, when the Router restarts up, all certificates will be deleted. Although they are still displayed on the list, actually they are not saved in the system. So, every time there's one certificate generated, please click **Save to Flash**.

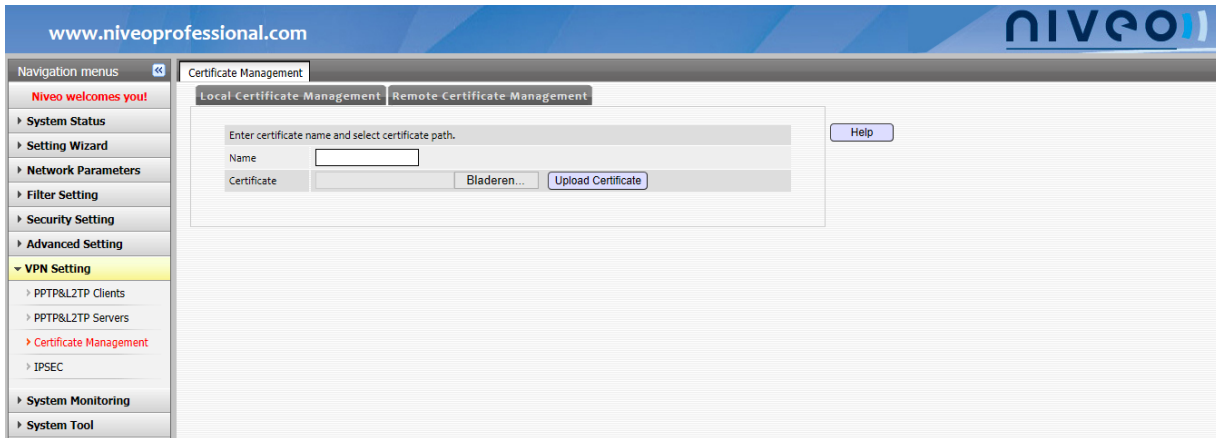
✧ How to Generate a Certificate



- **Certificate Name:** Name the digital certificate that you want to generate. Note that do not use a same name with the existing certificates.
- **Certificate Specification:** Generate 1024-bit digital certificate.
- **Nation:** Select your Nation.
- **Province or State Name:** Enter the province or state name, only up to 16 English characters are allowed.
- **Area or City:** Enter the area or city name, only up to 16 English characters are allowed.
- **Community:** Enter the Community name, which can only consist of letters, numbers and underscores, up to 16 English characters.
- **Department:** Enter the department name, which can only consist of letters, numbers and underscores, up to 16 English characters.
- **Name:** Enter the name, which can only consist of letters, numbers and underscores, up to 16 English characters.
- **Email Address:** Enter the email address here, which can only consist of letters, numbers and “-_@”, up to 40 English characters.
- **Only Generate a Certificate Request:** Only generate a secret key and certificate request, but not digital certificate. After the request is generated, you can download it on the management interface, and request to CA server to apply for a certificate. After verified and assigned, it will be issued a certificate. After you get the assigned certificate, you can import the certificate to the Router.
- **Generate a Self-issued Certificate:** Generate the secret key, certificate requests, and the digital certificate assigned by the Router. It's strongly recommended that it can generate a self-assigned certificate.

✧ How to Import a Certificate

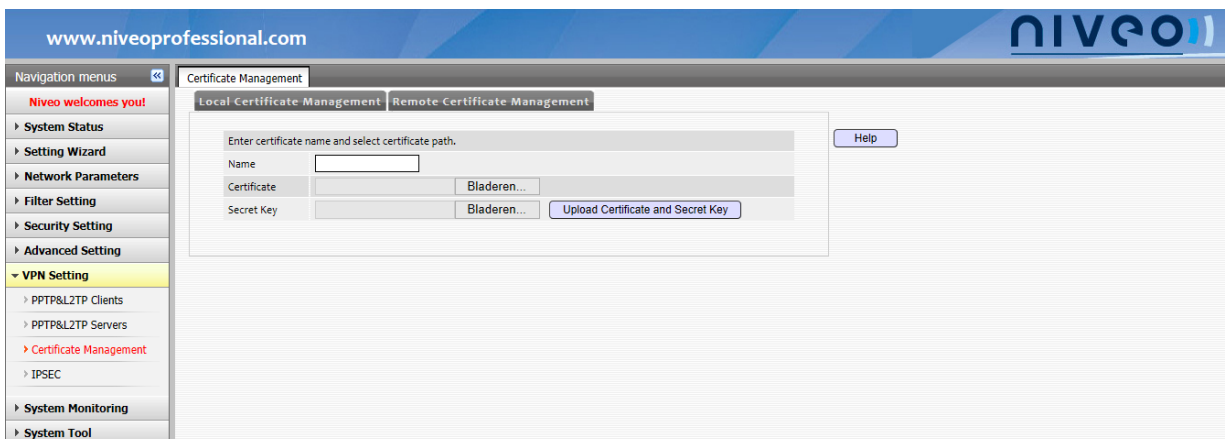
Import the certificate from the CA server and import it into the Router.



- **Name:** the name when “Only allow to generate the certificate request”; After the certificate is imported, i.e. the name of the certificate name.
- **Certificate:** Select the designated certificate.
- **Browse:** Click it to find the digital certificate applied from the CA server on the local disk.
- **Import Certificate:** Import the digital certificate on the local disk to the Router. Only the digital certificate on the disk matches with the certificate request of the Router can the digital certificate successfully be imported to the Router.

✧ How to Upload a Local Certificate

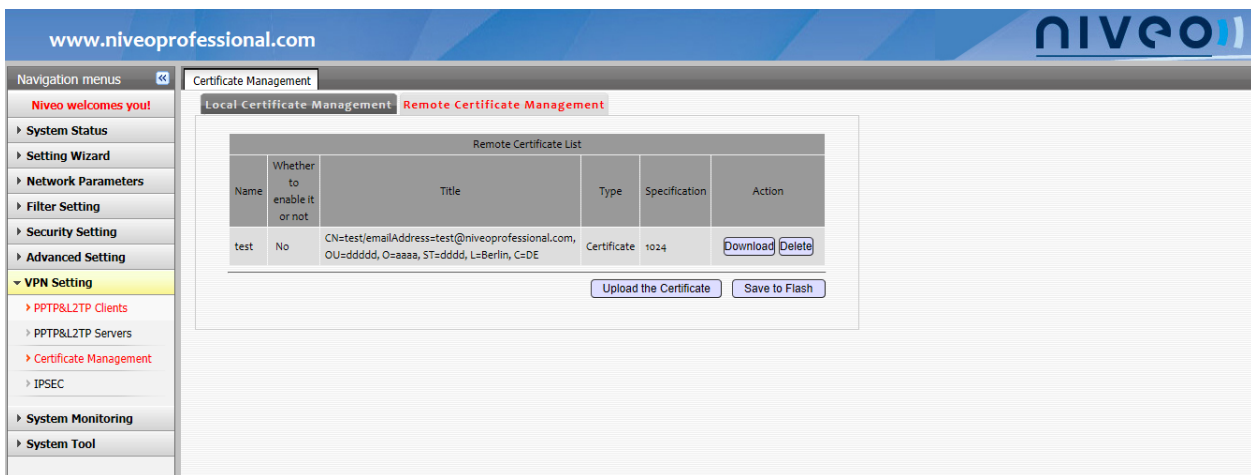
Upload the current digital certificate and secret key to the Router.



- **Name:** name the digital certificate you want to upload. Note that the name should be different with the existing names.
- **Certificate:** the digital certificate, i.e., the public secret key.

- **Secret Key:** the secret key of the digital certificate, i.e., the private key. The certificate and secret key should be used together. Use the public key to encrypt and the private key to unlock/decode.
- **Browse:** select the corresponding file saved on the local disk.
- **Upload Certificate and Secret Key:** Import the digital certificate and secret key to the Router. Only the selected certificate and secret are matched can they be imported successfully.

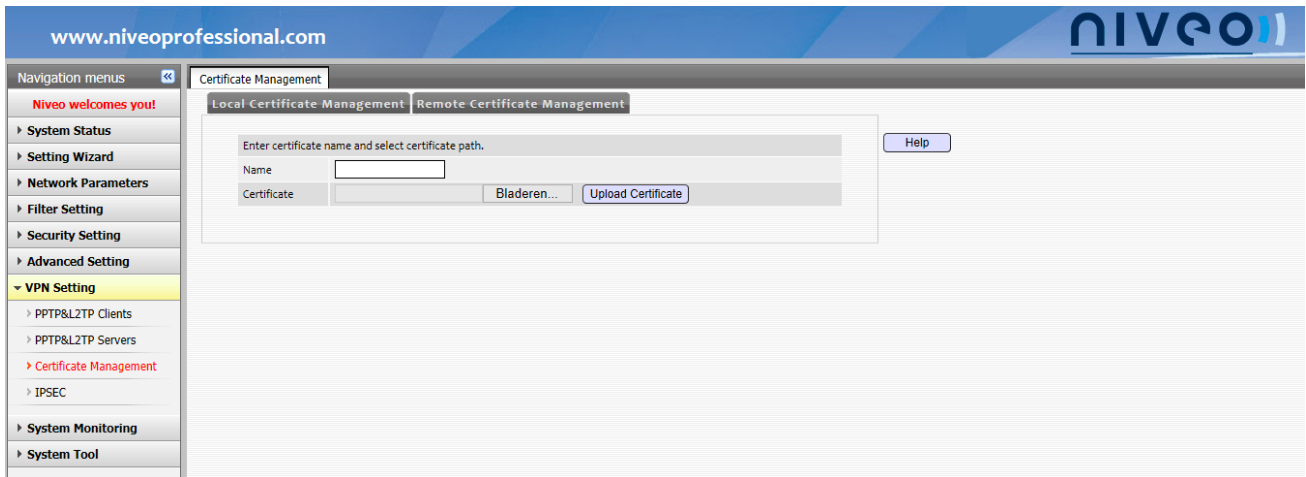
2. Remote Certificate Management



- **Remote Certificate List:** Show the list of the certificates that already have been uploaded to the Router.
- **Download:** Download the .cer-digital certificate to the local disk.
- **Delete:** Delete the digital certificate from the Router. There's no Delete button for the certificate in use.
- **Upload the Certificate:** Upload the digital certificate to the remote router. As for the digital certificate, i.e., the remote digital one, it's from the remote and located on the local router.
- **Save to Flash:** save all the certificates of the router to Flash. If you do not save them, when the Router restart up, all certificates will be deleted. Although they are still displayed on the list, actually they are not saved in the system. So, every time there's one certificate generated, please click **Save to Flash**.

✧ How to Upload a Remote Certificate

Import the remote router's digital certificate to the local digital certificate.

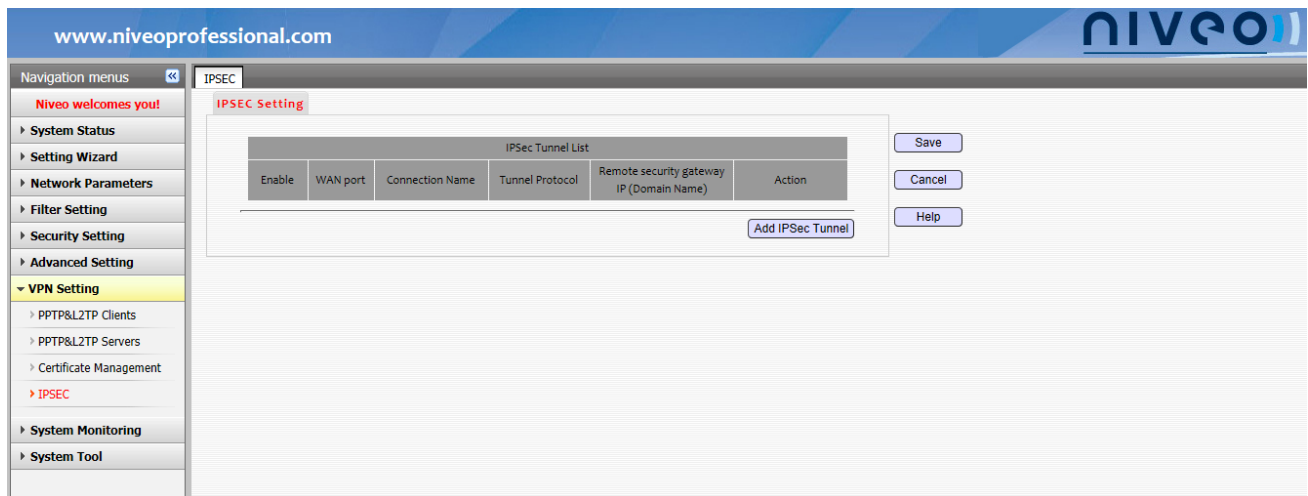


- **Name:** Name the digital certificate you want to upload. Note that the name should be different with the existing names.
- **Certificate:** the remote digital certificate, i.e., the remote router's public secret key.
- **Browse:** Select the digital certificate of the remote router.
- **Upload Certificate:** Import the remote digital certificate to the Router. Only the .cer-digital certificate can be imported successfully.

IPSEC

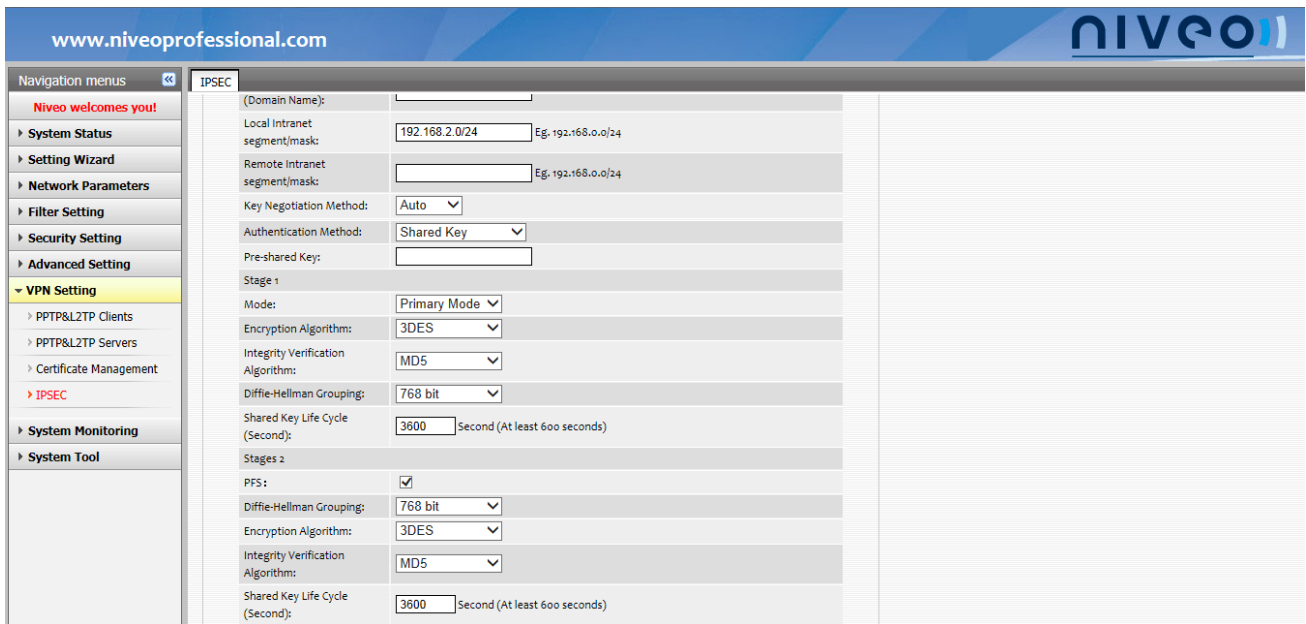
1. Create VPN via IPSEC Setting

The default mode of this Router is tunnel mode. In this mode, the overall packet is encapsulated as effective load, with new IP header attached outside. "Inner" IP header (Original IP header) specifies the final information source and information destination address; while "Outer" IP header (New IP header) includes security gateway address which does the middle processing.



- **IPSec Tunnel List:** Show the existing IPSEC tunnels.
- **Enable:** Enable/Disable the IPSEC tunnel.
- **WAN Port:** Display which WAN interface the IPSEC tunnel is created.
- **Connection Name:** Name the IPSEC tunnel. The name should be different from other names.
- **Tunnel Protocol:** Show the security protocol adopted by the tunnel.
- **Remote security gateway IP (Domain Name):** Display the WAN IP of the remote router on which IPSEC tunnel created.
- **Edit:** Modify IPSEC tunnel configuration.
- **Delete:** Delete the IPSEC tunnel.
- **Add IPsec Tunnel:** Add one IPSEC tunnel. Up to 15 entries can be added.

✧ How to Add IPSEC Tunnel



- **Enable:** Whether to enable the IPSEC tunnel.
- **WAN Port:** Select the local interface. Bind the IPSEC configuration to the designated interface, then packets through this interface will be checked by IPSEC, to verify whether to encrypt and decode the packets.
- **Connection Name:** Name the IPSEC tunnel. The name should be different from other names.
- **Tunnel Protocol:**

ESP (Encapsulating Security Payload): In end-to-end tunnel communication, this protocol will encrypt the overall packets. Clients can select a keyed hash algorithm to guarantee the integrity and authenticity (With high compatibility, this protocol is used widely in different gateway products.).

AH (Authentication Header): the protocol will detect the overall packet's integrity, including the outer IP header. If the data is not encrypted, and the packet is modified in processing, the packet will be discarded.

ESP+AH: Function with ESP and AH two protocols encryption and integrity detection.

- **Remote Security Gateway IP (Domain name):** IP address (or domain name) of the tunnel remote gateway, generally the WAN IP of the remote router.
- **Local Intranet IP/Mask:** Any IP address and subnet mask in local protected intranet.
- **Remote Intranet IP/Mask:** Any IP address and subnet mask in the tunnel remote protected intranet. If the remote end is a single host, the parameters will be the IP address of the device/32.
- **Key Negotiation Method:**

Manual: the establishment of SA needs clients to set encryption/authentication algorithm. SA established manually has no life cycle limit, never out of date, unless deleted manually, thus this way has potential risk. It is always used in debugging state.

Auto: SA's auto-establishment, dynamic maintenance and deletion can be achieved via IKE (Internet Key Exchange). SA established automatically has life cycle. If SP demands secure and encrypted connection, but there's no corresponding SA connected, IPSEC core will enable IKE immediately to negotiate SA.

Auto negotiation Parameters

➤ **Authentication Method:**

Shared key: The character string shared by both sides negotiated via some method in advance.

- **X.509 Authentication:** Both sides use digital certificate to indicate identity, and use the Digital Signature Algorithm (DSA) to count a signature to authenticate identity.
- **Pre-shared Secret Key:** Negotiate pre-shared secret key you want to use. When the authentication is shared key, the local router and remote router need to be set with the same pre-shared secret key. The key range is 3~128 characters.
- **Local Certificate:** Local digital certificate, can generate self-signed certificate on the certificate management interface; it can also acquire your own digital certificate. Before communication, you need to share local certificate with remote end.
- **Remote Certificate:** Remote digital certificate. Before communication, you need to acquire digital certificate via remote end.
- **Negotiation mode (the first stage):** The Primary mode, active mode (wild mode). The modes on both sides must use the same encryption algorithm.
- **Encryption Authentication Algorithm (the first stage):** It provides preferred encryption and authentication algorithm which is negotiated and used in the first stage. Supporting DES, 3DES, AES-128, AES-192 and AES-256, both sides should use the same encryption algorithm.
- **Integrity Authentication Algorithm (the first stage):** MD5 or SHA1 algorithm takes integrity algorithm on the first stage.
- **Diffie-Hellman Group (the first stage):** Parameters in Diffie-Hellman public secret key algorithm, should be kept the same with the remote.

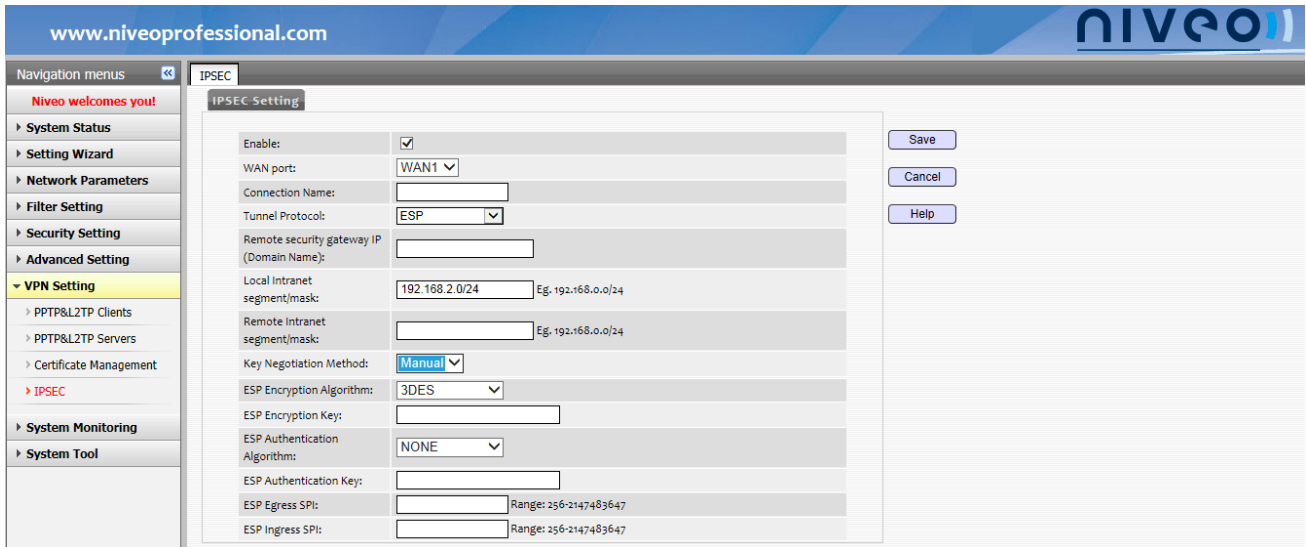
- **Life Time (the first stage):** IKE SA life time, at least 600 seconds. When time is left 540 seconds, IKE SA will be renegotiated.
 - **PFS (Perfect Forwarding Security):** PFS is the attribute that proposer suggests to receiver. If it's negotiation, it will be supported; if it's not, it won't be supported.
 - **Diffie-Hellman Group (the second stage):** parameters in Diffie-Hellman public secret key algorithm, should be kept the same with the remote.
 - **Encryption Authentication Algorithm (the second stage):** It provides preferred encryption and authentication algorithm which is negotiated and used in the second stage.
 - **Integrity Authentication Algorithm (the first stage):** prepare for the integrity authentication on the second stage.
 - **Secret Life Cycle (the second stage):** IPSEC SA life time, at least 600 seconds. When time is left 540 seconds, IPsec SA will be renegotiated.
-

 **Note:**

Configurations on stage1 and stage 2 must be kept accordant. It's recommended to keep the default configuration.

✧ How to Set Parameters Manually.

Set parameters manually on both routers. As for auto-negotiation mode, its secret key is negotiated by the designated algorithm of the two routers, and every some time, both sides will re-negotiate a new secret key. Auto-negotiation mode is easy to set and with high security, which is strongly recommended to use.



➤ ESP encryption algorithm:

3DES: when the encryption algorithm is 3DES, the key length is 24 ASCII numbers or 48 hexadecimal numbers.

DES: when the encryption algorithm is DES, the key length is 8 ASCII numbers or 32 hexadecimal numbers.

AES-128: when the encryption algorithm is AES-128, the key length is 16 ASCII numbers or 32 hexadecimal numbers.

AES-192: When the encryption algorithm is AES-192, the key length is 24 ASCII numbers or 48 hexadecimal numbers.

AES-256: When the encryption algorithm is AES-256, the key length is 32 ASCII numbers or 64 hexadecimal numbers.

➤ ESP Authentication Algorithm: (optional, provide packets integrity and guarantee service)

NONE: ESP authentication algorithm is blank. You do not need to fill in the authentication secret key field.

ESP authentication algorithm is MD5, the authentication length is 16 ASCII numbers or 32 hexadecimal numbers.

SHA1: ESP authentication algorithm is SHA1, the authentication length is 20 ASCII numbers or 40 hexadecimal numbers.

➤ **AH authentication algorithm:**

MD5: AH authentication algorithm is MD5, the authentication length is 16 ASCII numbers or 32 hexadecimal numbers.

SHA1: AH authentication algorithm is SHA1, the authentication length is 20 ASCII numbers or 40 hexadecimal numbers.

➤ **SPI (Security Parameter Index):**

A 32-bit security parameter index, used to identify different SA which have the same IP address and security protocol. To guarantee SA's uniqueness, it's advisable to employ different SPI to configure SA; when the IKE negotiation is employed to produce SA, SPI will be generated randomly.

ESP Egress SPI: Be in the same with remote ESP Ingress SPI.

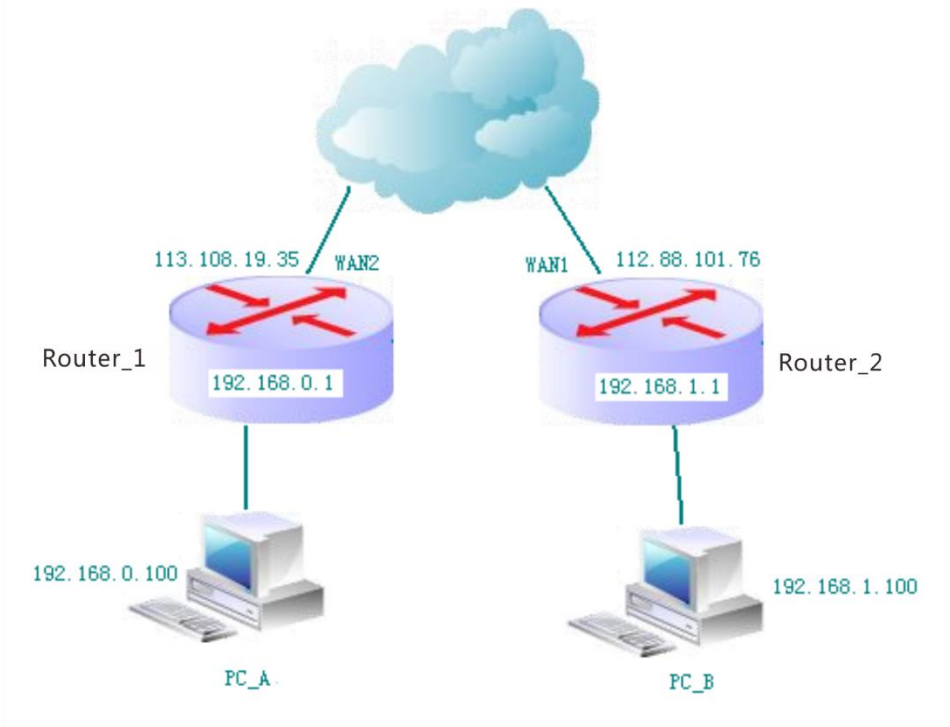
ESP Ingress SPI: Be in the same with remote ESP Egress SPI.

AH Egress SPI: Be in the same with remote AH Ingress SPI.

AH Ingress SPI: Be in the same with remote AH Egress SPI.

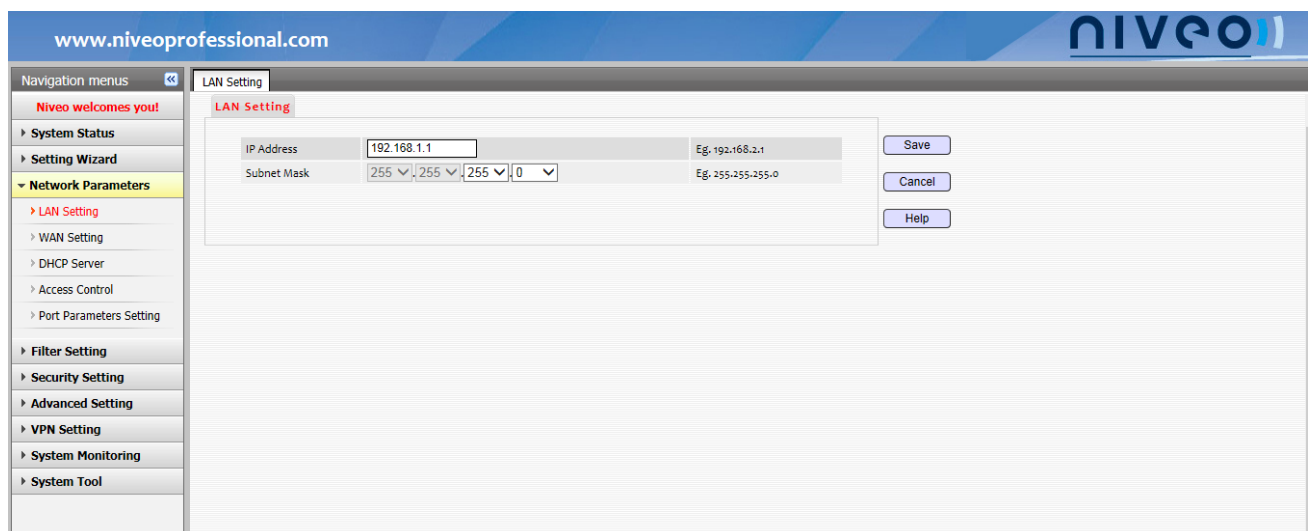
2. Application

Steps of two Routers building up VPN'S via PPTP. Router_1 and Router_2



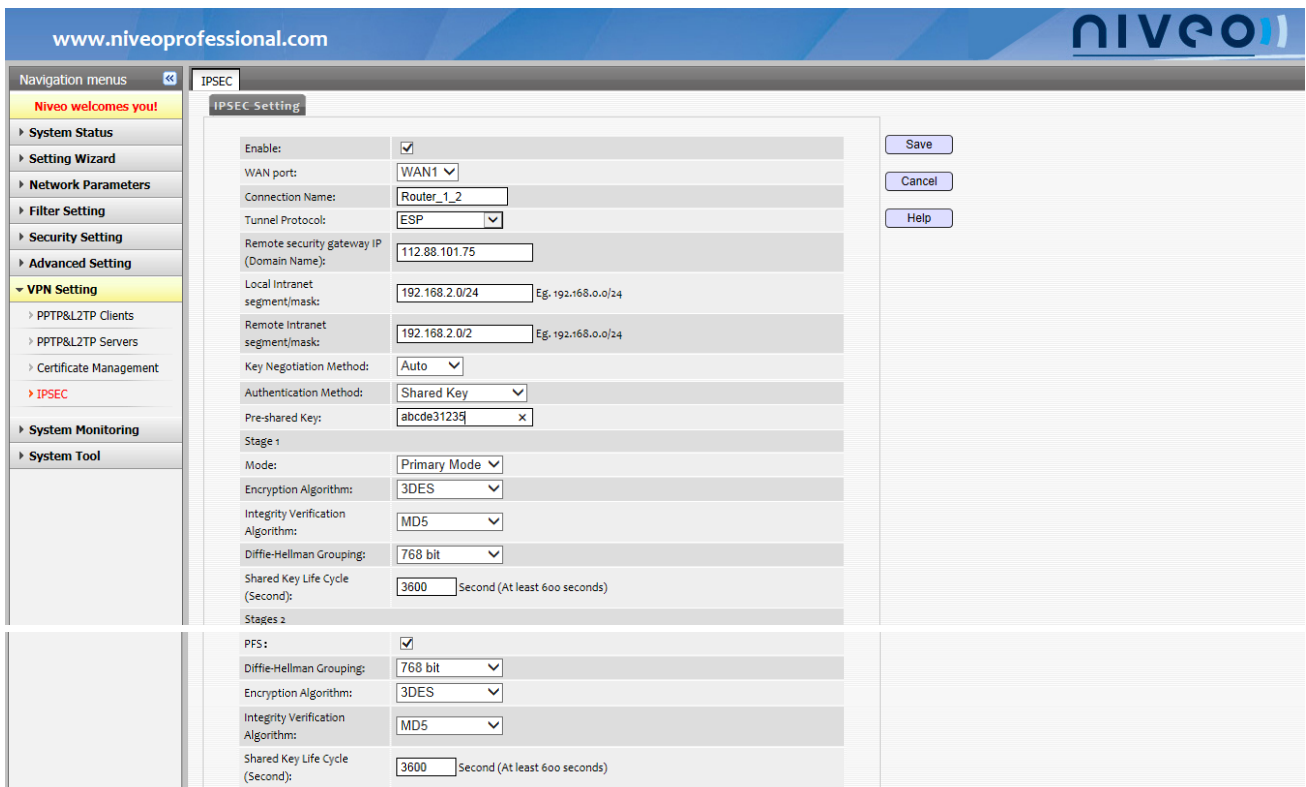
✧ How to Create IPSEC VPN via Pre-shared Secret Key

Step 1: LAN IPs of Router_1 and Router_2 cannot be in the same network segment. The default LAN IP of these two Routers are both 192.168.0.1, so you need to change one Router's LAN IP. Here we change the Router_2 LAN IP into 192.168.1.1



Step 2: Router_2 WAN2 obtains IP: 113.108.19.35 via PPPoE; Router_1 WAN1 obtains 112.88.101.76 via PPPoE. PC_A can ping 112.88.101.76 successfully, and PC_B can ping 113.108.19.35 successfully.

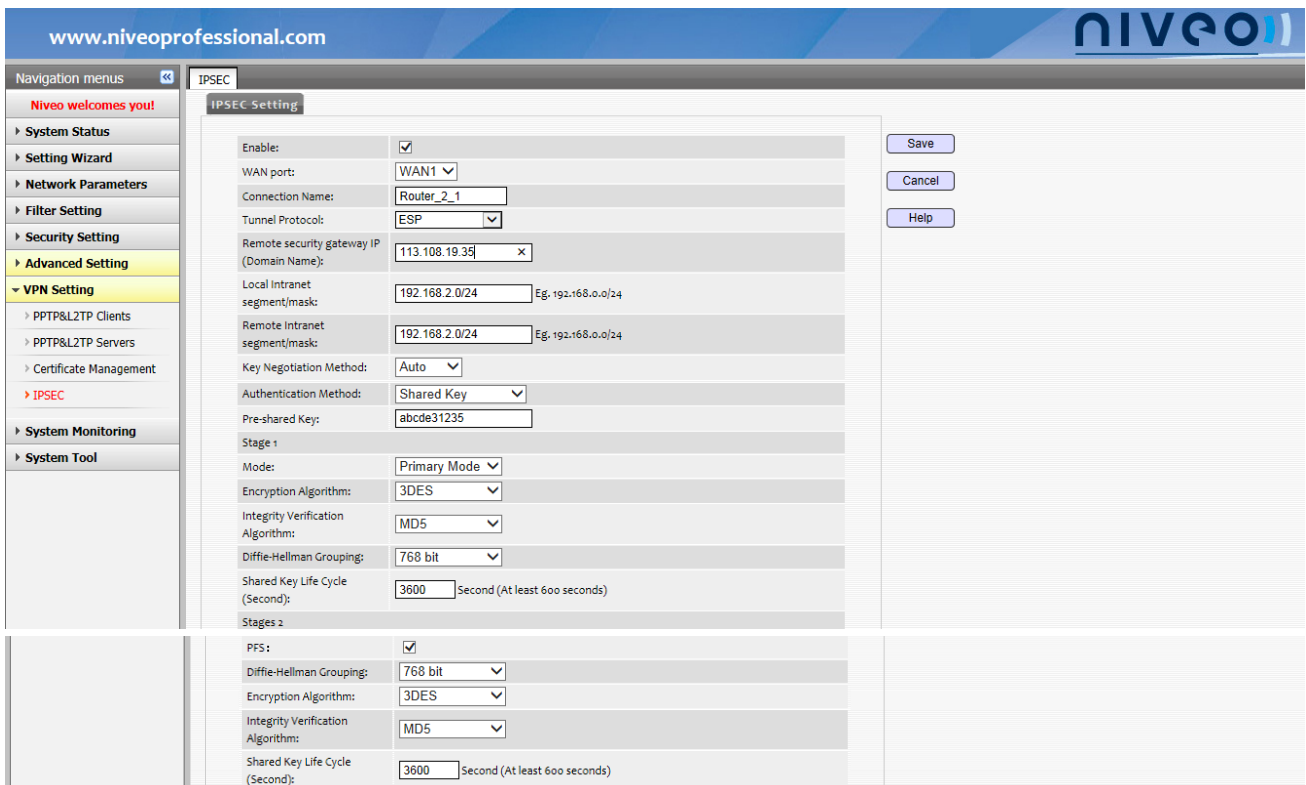
Step 3: Add an IPSEC tunnel on Router_1, detailed configuration shown below.



The screenshot shows the IPSEC configuration page for Router_1. The configuration is as follows:

Field	Value
Enable:	<input checked="" type="checkbox"/>
WAN port:	WAN1
Connection Name:	Router_1_2
Tunnel Protocol:	ESP
Remote security gateway IP (Domain Name):	112.88.101.75
Local Intranet segment/mask:	192.168.2.0/24
Remote Intranet segment/mask:	192.168.2.0/2
Key Negotiation Method:	Auto
Authentication Method:	Shared Key
Pre-shared Key:	abcde31235
Stage 1	
Mode:	Primary Mode
Encryption Algorithm:	3DES
Integrity Verification Algorithm:	MD5
Diffie-Hellman Grouping:	768 bit
Shared Key Life Cycle (Second):	3600
Stages 2	
PFS:	<input checked="" type="checkbox"/>
Diffie-Hellman Grouping:	768 bit
Encryption Algorithm:	3DES
Integrity Verification Algorithm:	MD5
Shared Key Life Cycle (Second):	3600

Step 4: Add another IPSEC tunnel on Router_2, detailed configuration shown below.



The screenshot shows the IPSEC configuration page for Router_2. The configuration is as follows:

Field	Value
Enable:	<input checked="" type="checkbox"/>
WAN port:	WAN1
Connection Name:	Router_2_1
Tunnel Protocol:	ESP
Remote security gateway IP (Domain Name):	113.108.19.35
Local Intranet segment/mask:	192.168.2.0/24
Remote Intranet segment/mask:	192.168.2.0/24
Key Negotiation Method:	Auto
Authentication Method:	Shared Key
Pre-shared Key:	abcde31235
Stage 1	
Mode:	Primary Mode
Encryption Algorithm:	3DES
Integrity Verification Algorithm:	MD5
Diffie-Hellman Grouping:	768 bit
Shared Key Life Cycle (Second):	3600
Stages 2	
PFS:	<input checked="" type="checkbox"/>
Diffie-Hellman Grouping:	768 bit
Encryption Algorithm:	3DES
Integrity Verification Algorithm:	MD5
Shared Key Life Cycle (Second):	3600

When PPTP server obtains the IP, between these two routers are built up PPTP VPN. PCs on the routers downlink side can communicate with each other directly. PC_A can straightly ping PC_B IP 192.168.1.100 successfully, PC_B can directly ping PC_A IP 192.168.0.100 successfully.

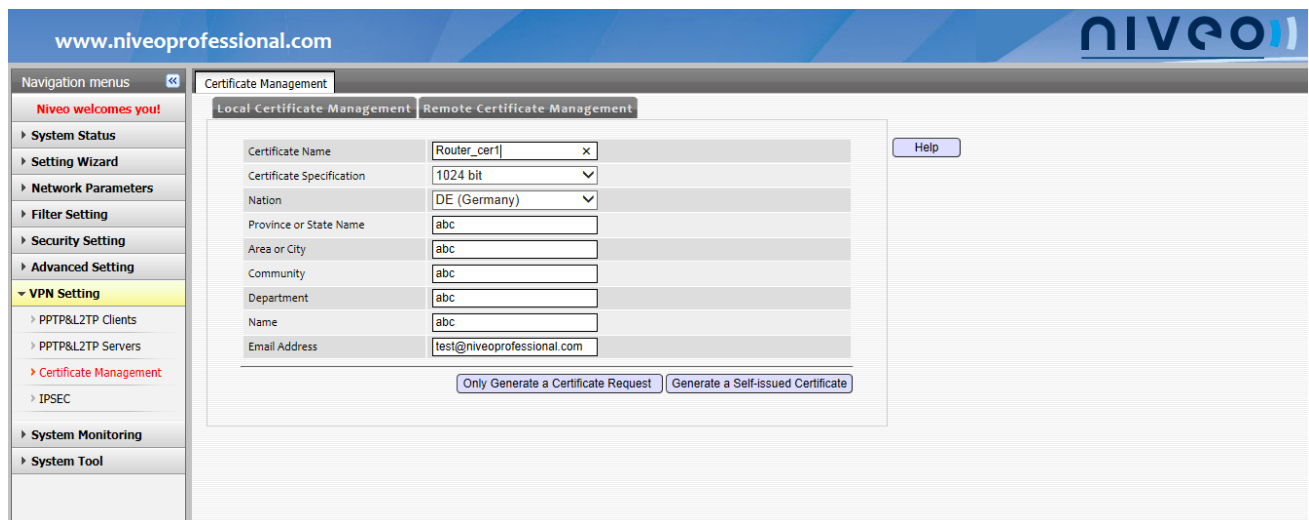
After these two routers are added to the IPSEC tunnels, IPSEC progress started up. But actually IPSEC VPN isn't created yet, which has only been configured with the security policy SP, the security Association-SA hasn't been negotiated and created. Only when one intranet PC of the router can send packets to another router's intranet, the SA starts negotiating. When SA negotiates, IPSEC tunnel is created.

1. PC_A pings 192.168.1.100, when Router_1 receives the first ping packets, IPSEC progress will find that the packets are send to the other side with security policy, then it will start IKE to negotiate SA with Router_2.
2. For the configuration of both sides match, SA can finish the negotiation within several seconds. The negotiation speed is up to the algorithm, generally 2~5 seconds. Thus, when PC_A pings 192.168.1.100, if the former one or two packets Time out, the following packets will ping successfully, namely, the IPSEC VPN is created successfully.

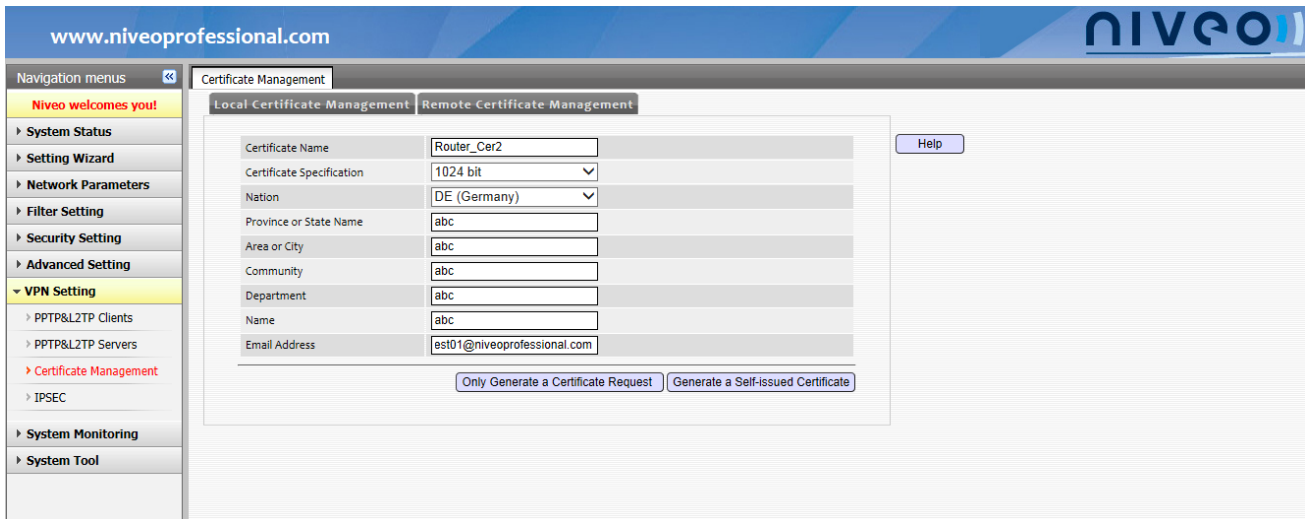
✧ How to Use digital certificate to create IPSEC VPN

Follow steps of the last example, continue the steps bellow.

Step 5: Router_1 generates a self-issued certificate, the name is Router_cer1.



Step 6: Router_2 generated a self-issued certificate, the name is Router_cer2.



Step 7: PC_A downloads certificate Router_cer1 to the local PC, while PC_B downloads Router_2.

Router_cer1	No	CN=abc/emailAddress=test@niveoprofessional.com, O=abc, OU=abc, ST=abc, C=DE, L=abc	Certificate	1024	Download Delete
-------------	----	---	-------------	------	---

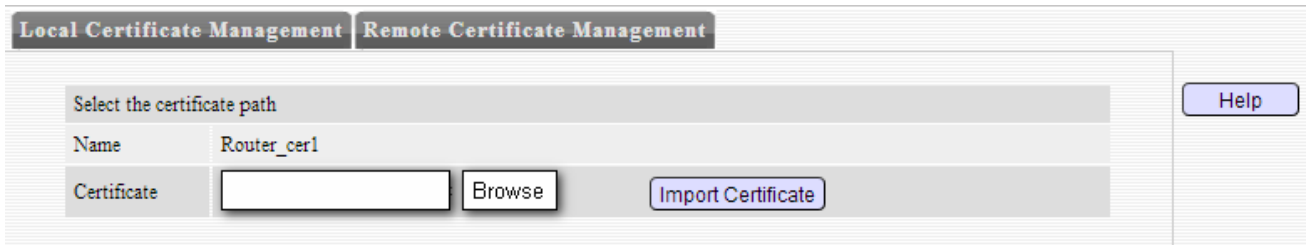
Router_Cer2	No	CN=abc/emailAddress=test01@niveoprofessional.com, O=abc, OU=abc, ST=abc, C=DE, L=abc	Certificate	1024	Download Delete
-------------	----	---	-------------	------	---

Step 8: PC_A and PC_B send their own certificates to each other by emails.

Step 9: PC_A imported the digital certificate of Router_2 to the remote certificate management list of Router_1.



Step 10: PC_B imported the digital certificate of Router_1 to the remote certificate management list of Router_2.



Step 11: If you add one IPSEC tunnel, you need to delete the tunnel Router1-2, because one remote Intranet can only be created one IPSEC tunnel. We modify the current tunnel to start configuration. Change the IPSEC tunnel

of Router_1, the authentication mode is X.509, the local certificate Router_cer1, the remote certificate Router_cer2, and other settings kept.

Step 12: Change Router_2's IPSEC tunnel, Authentication: X.509, Local certificate: Remote Certificate: Router_cer2, the other configuration remains unchanged.

When the IPSEC tunnel configuration is modified and then saved again, the IPSEC process will restart, and the earlier SA will be removed. When PC_A and PC_B communicate again, the new configuration will be used to negotiate SA, namely using the certificate to create IPSEC VPN.

❖ How to Enable manually setting to build IPSEC VPN

Set after the last example.

Step 1: Change NR50's IPSEC tunnel, the key negotiation change in to "Manual", according to the setting of other parameters.

IPSEC Setting	
Enable:	<input checked="" type="checkbox"/>
WAN port:	WAN2 ▾
Connection Name:	Router_1-2
Tunnel Protocol:	ESP ▾
Remote security gateway IP (Domain Name):	112.88.101.76
Local Intranet segment/mask:	192.168.0.0/24 Eg. 192.168.0.0/24
Remote Intranet segment/mask:	192.168.1.0/24 Eg. 192.168.0.0/24
Key Negotiation Method:	Manual ▾
ESP Encryption Algorithm:	3DES ▾
ESP Encryption Key:	1234567890
ESP Authentication Algorithm:	NONE ▾
ESP Authentication Key:	123456
ESP Egress SPI:	1234 Range: 256-2147483647
ESP Ingress SPI:	5678 Range: 256-2147483647

Step 2: Change NR50-2's IPSEC tunnel, the key negotiation change in to "Manual", according to the setting of other parameters.

IPSEC Setting

Enable:	<input checked="" type="checkbox"/>		Save
WAN port:	WAN1 ▼		Cancel
Connection Name:	Router_2-1		Help
Tunnel Protocol:	ESP ▼		
Remote security gateway IP (Domain Name):	113.108.19.35		
Local Intranet segment/mask:	192.168.1.0/24	Eg. 192.168.0.0/24	
Remote Intranet segment/mask:	192.168.0.0/24	Eg. 192.168.0.0/24	
Key Negotiation Method:	Manual ▼		
ESP Encryption Algorithm:	3DES ▼		
ESP Encryption Key:	1234567890		
ESP Authentication Algorithm:	NONE ▼		
ESP Authentication Key:	123456		
ESP Egress SPI:	5678	Range: 256-2147483647	
ESP Ingress SPI:	1234	Range: 256-2147483647	

Step 3: When the IPSEC tunnel's configuration is modified and save change again, the IPSEC process will restart, before SA will be removed. PC-A and PC-B again communication, IPSEC VPN will enable manually setting's SA to add the decryption.

Note:

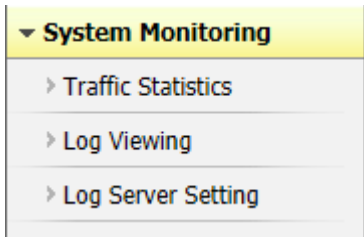
When the two routers are added the IPSEC tunnels, VPN hasn't been created yet. When there's data communication, the IPSEC VPN starts to be created.

When one router saves the configuration, or disconnected to the Ethernet cable, or the system restarts, IPSEC process will restart, and IPSEC tunnel will be interrupted. At this moment, one router_1 has no SA, the other Router_2 is still using the old SA; Router_2'intranet PC will not ping the intranet PC of Router_1.

Only when the PC in the intranet of this side is connect to the PC of intranet in that side, will this side start to negotiate the secret key to create the VPN.

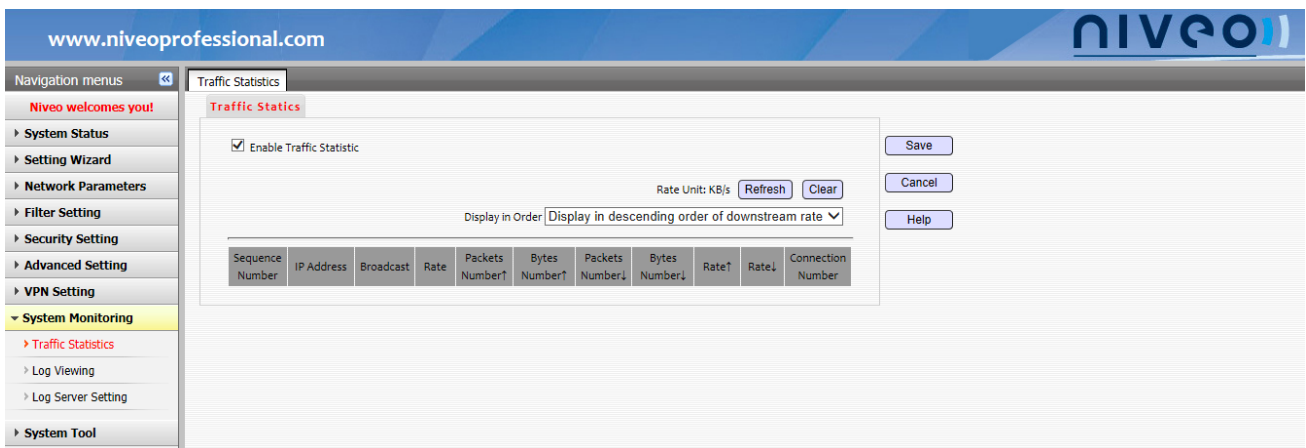
3. When using the digital certificate to create the IPSEC VPN, the Router should generate the certificate by itself, and then share the certificate with the remote Router.

8 System Monitoring



Traffic Statistics

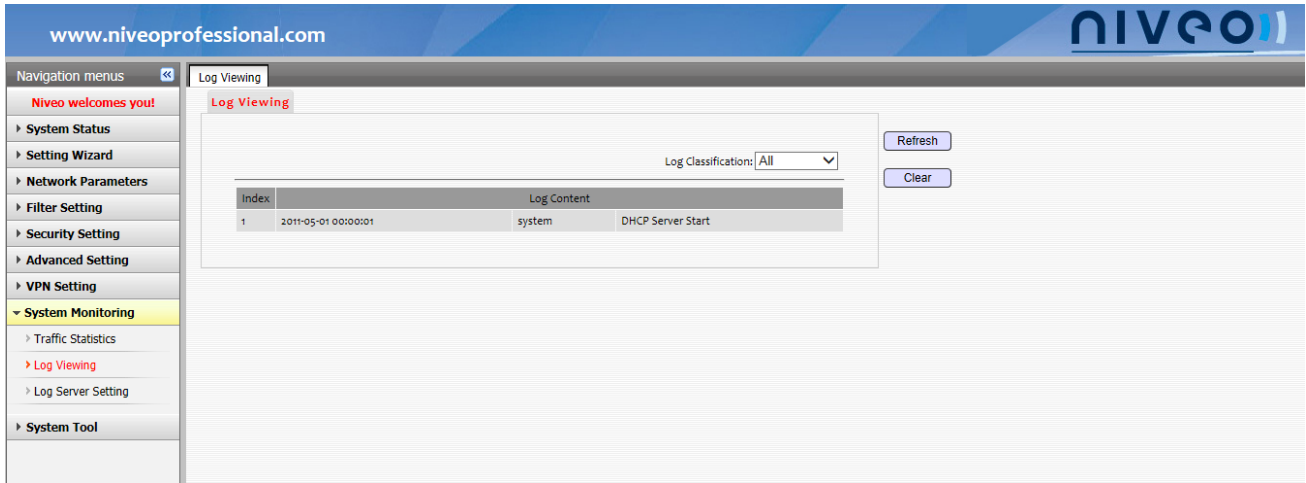
You can view the traffic statistics of hosts in the LAN, which makes the management optimization of network resources easy.



- **Enable Traffic Statistics:** Check this box to enable traffic statistics feature. It is recommended to disable this feature if unnecessarily.
- **Refresh:** Click this button to refresh the current statistics.

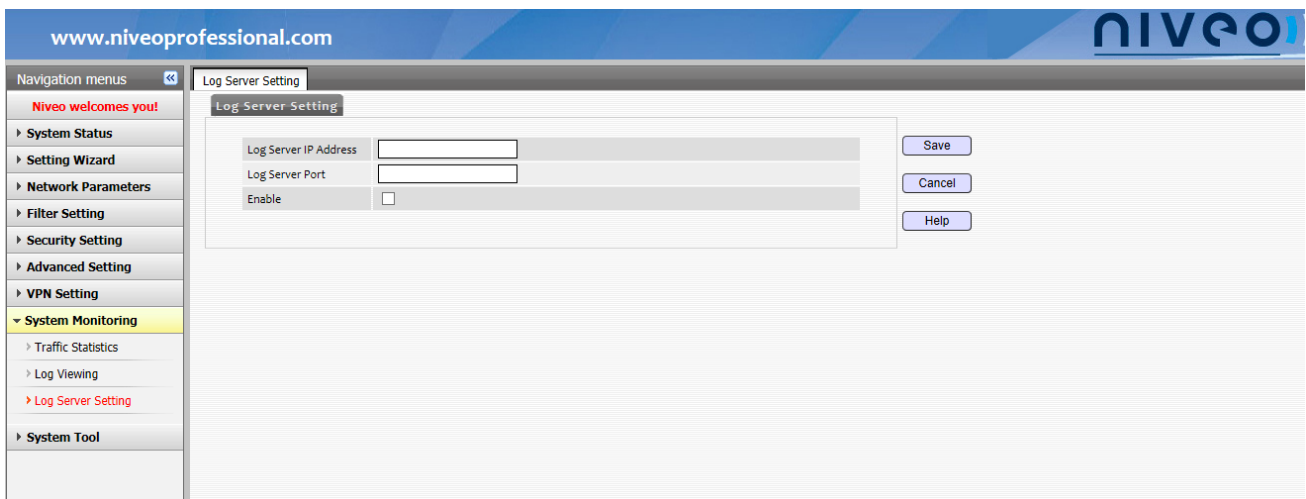
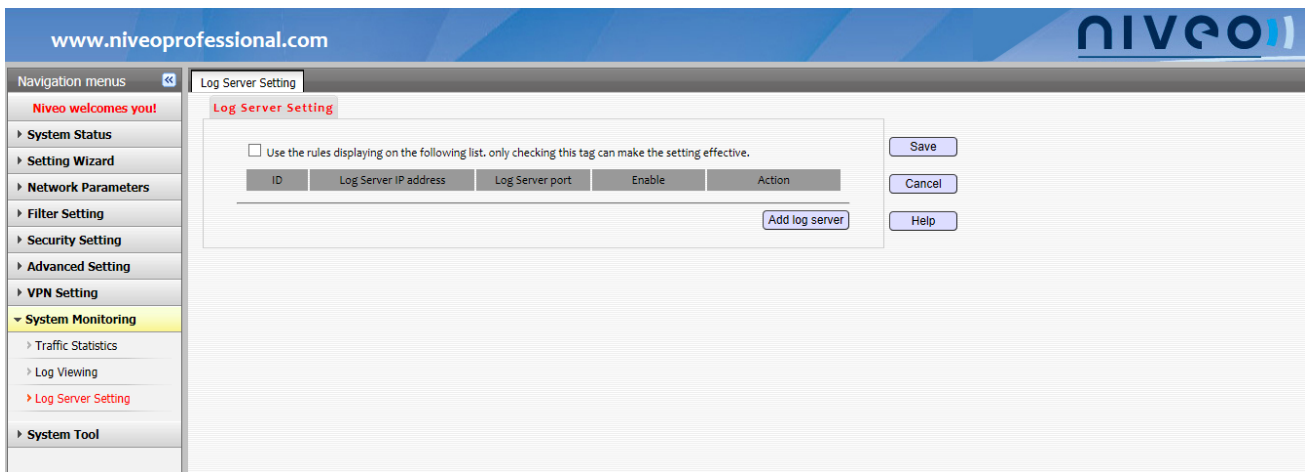
Log Viewing

You can view all the operations of the router since the system has operated. Also you can check whether there is a network attack or not.



Log Setting

By default, if the recorded logs get to 200 entries, the old logs will be cleared automatically. For comprehensively getting to know how the router operates, a log server is needed which is used to receive logs. Click **Add log server** to show configuration page as below:

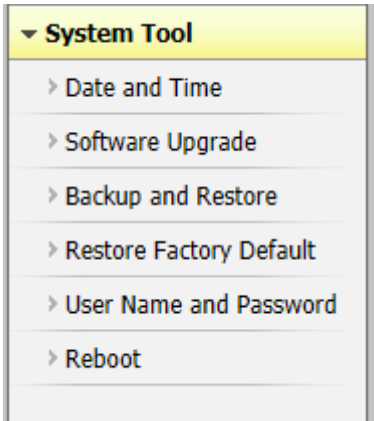


Log Server IP Address: Specify an IP address of host to be a log server.

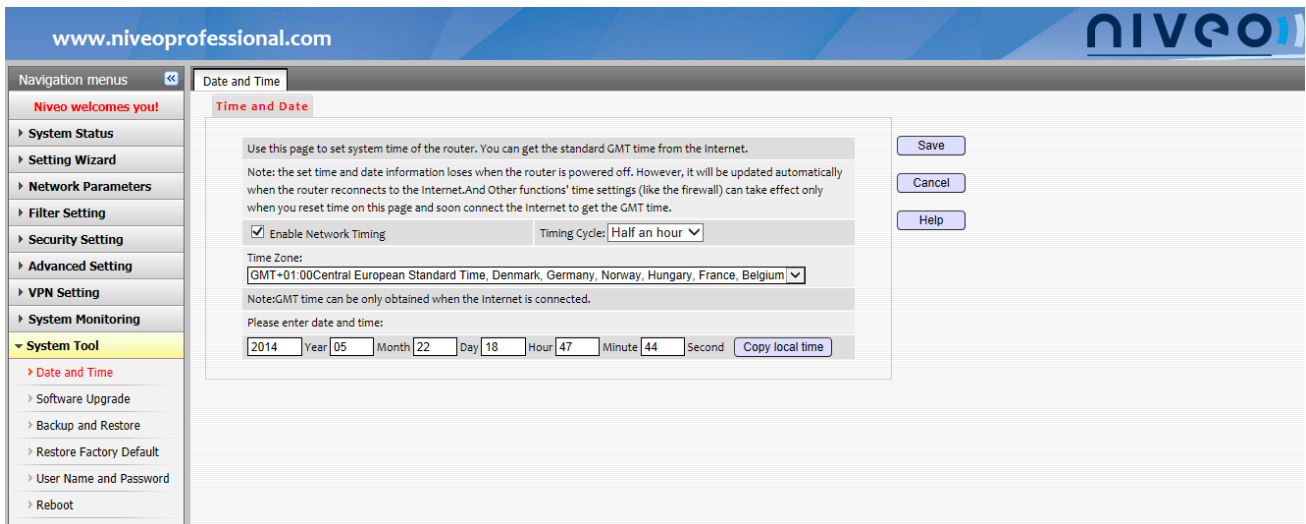
Log Server Port: Specify a port to be the server port.

Enable: Check the **Enable** box to apply this log server.

9 System Tools



Date and Time



You can get the standard GMT time from the Internet, which means only after you have connected to the Internet, you can get the latest GMT time. Or you can configure time settings manually.

Enable Network Timing: Means the device system synchronizes its time settings with the Internet automatically.

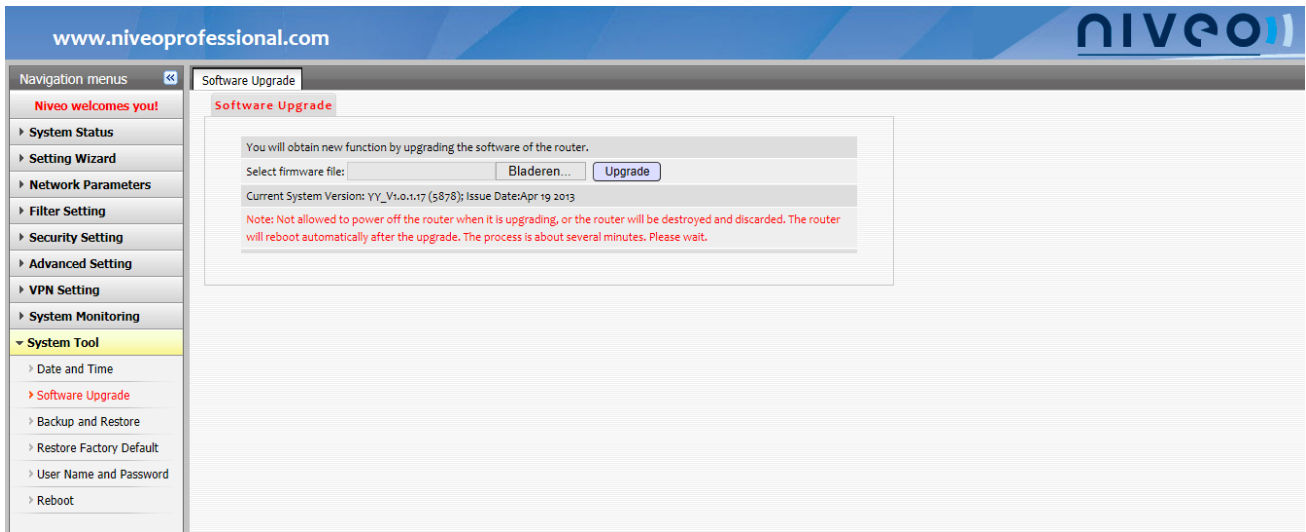
Timing Cycle: Displays how often the system synchronizes time settings with the Internet. Please configure a proper value according to your needs. The default value is half an hour.

Time Zone: Specify your local time zone.

Copy local time: Click this button to copy your PC's time settings to the router.

Software Upgrade

Upgrading the router’s software can help you get new features and more stable performance.



To upgrade software:

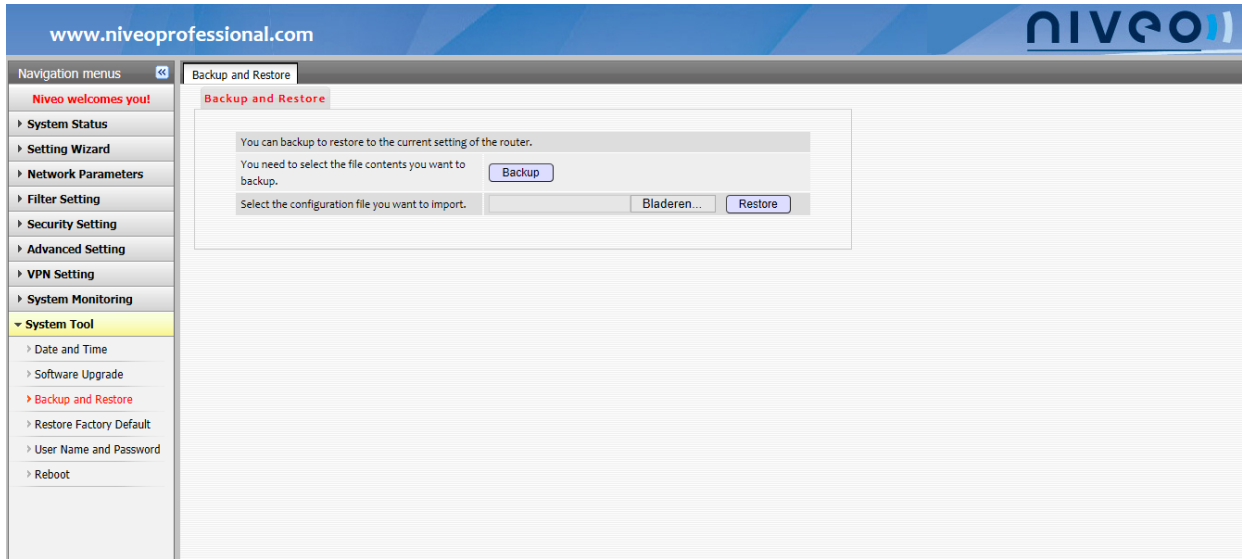
Locate the upgrade file and upload it, and then click “Upgrade” to upgrade the device software. After a successful upgrade, the router will automatically reboot.

Note:

Do not disconnect the device from power during the upgrade process; otherwise the router may be damaged. It will take several minutes to finish upgrade, please wait patiently. After a successful upgrade, the router will reboot automatically.

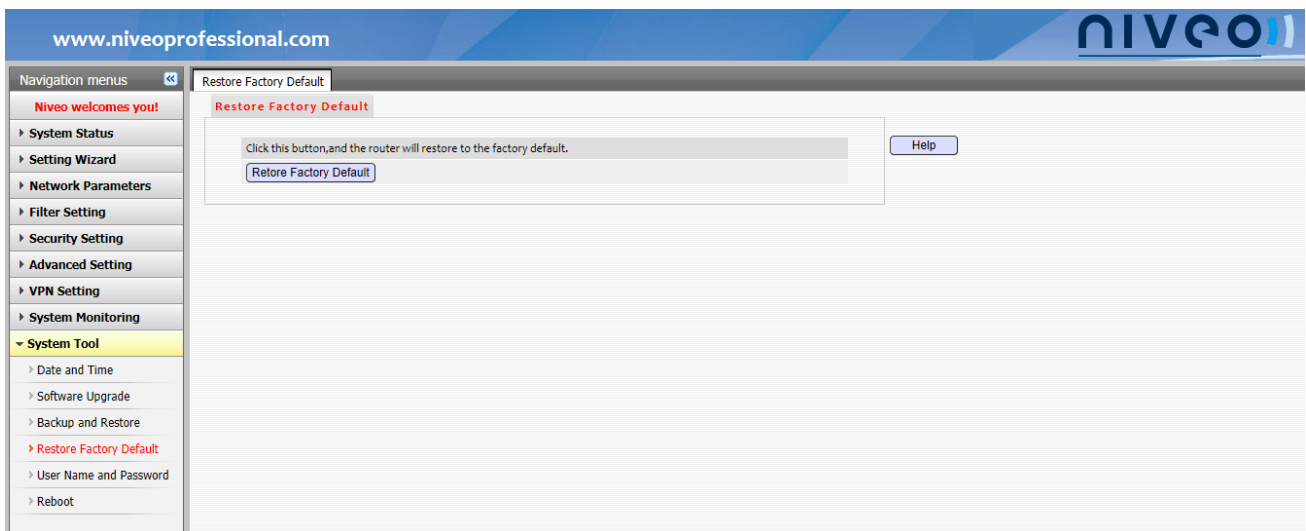
Backup and Restore

You can backup your current configurations or restore your backup configurations on the screen shown as below.



- **Backup:** Click the **Backup** button to download the configurations as a file, and specify a path to save the backup file.
- **Restore:** Upload the backup file you want to restore, and click the **Restore** button. For activating the configurations, it is recommended to reboot the router after restoring the config.

Restore Factory Default



Click the **Restore Factory Default** button to reset router to factory default settings.

Default value:

Username: admin

Password: admin

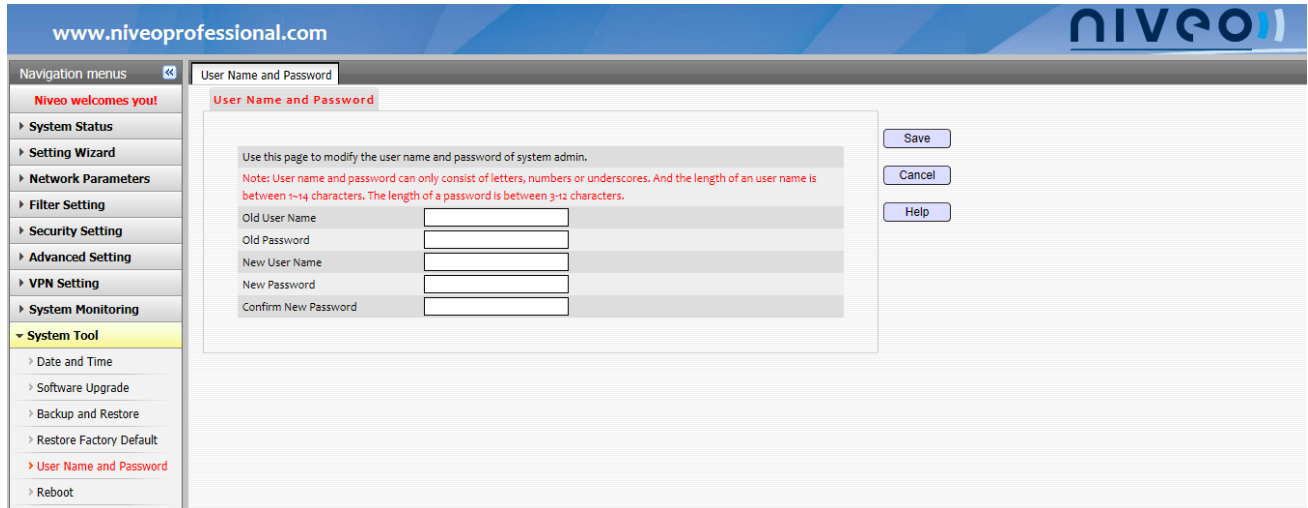
IP Address: 192.168.2.254

Subnet Mask: 255.255.255.0

After restoring to factory default settings successfully, the router will reboot.

User Name and Password

You can change the username and password of system admin on the below screen.



To change User Name/Password

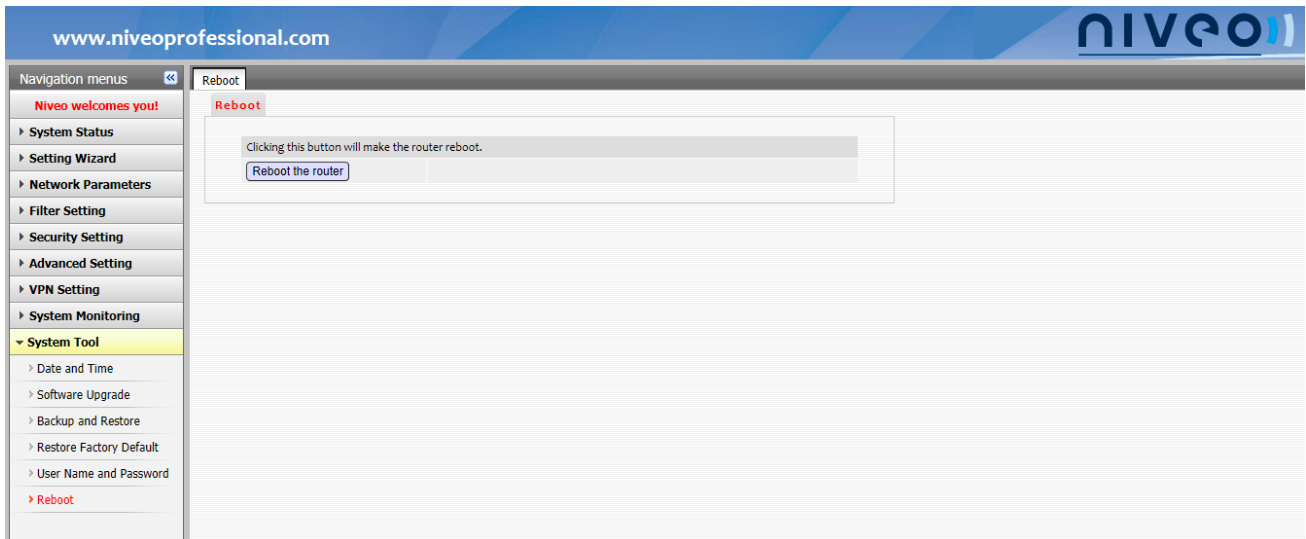
1. Enter the old user name/password.
2. Specify a new user name/password.
3. Confirm the new set user name/password.
4. Click **Save** to apply the modifications.

Note:

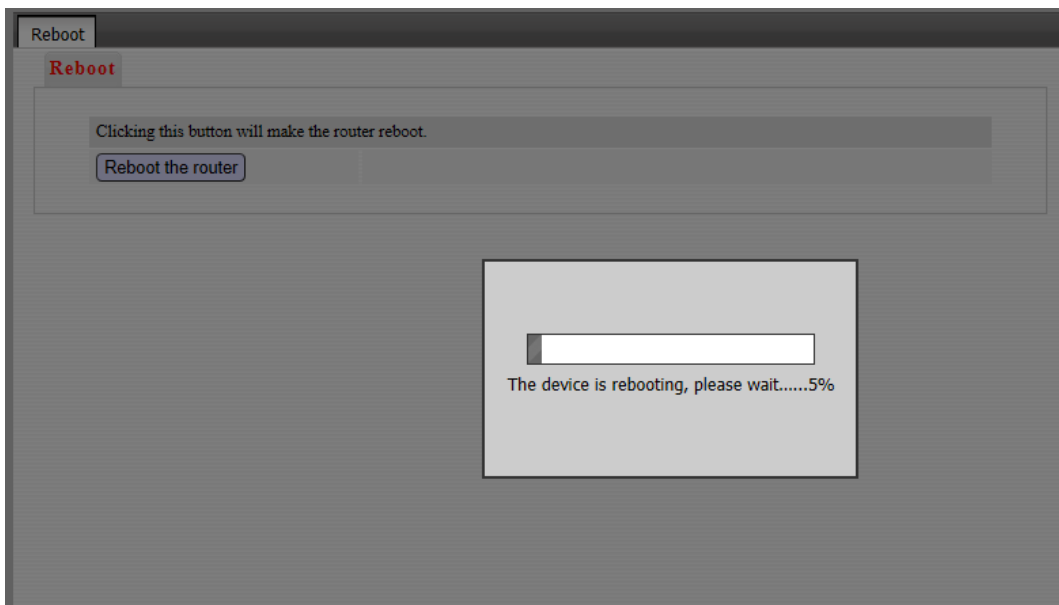
For your network security, it is strongly recommended to change the default user name and password settings.

Reboot

You can reboot the router by clicking the software reboot button on the web page, except for pressing the hard **Reset** button with a needle.



It takes around 40 seconds to reboot. Please wait patiently.



Rebooting can help activate configurations. During the rebooting process, the network connection will be cut, and be rebuilt automatically after rebooting.

Appendix 1: Commands Introduction

Common Commands	Description
cmd	Used to access the Command mode in windows 2000 or higher quickly.
ipconfig	Used to display the PC's IP address. You can also enter ipconfig /all to view it.
ping	This is the most useful command in the TCP/IP protocol. Use ping to send packets to another system and get responses from it, which is very much helpful to search a remote host. The response your PC gets indicates whether the packets reach the destination host or not, and also the response progress time.
netstat	Used to check the current IP connections status. If basic communication is undertaking on your PC, it will verify system services. This service can check the communication scale or verify that you're creating a session with the remote station. This command can easily do it.
tracert	Tracert Command is used to display the route of the packets to the destination host, and also display the time when the packets reach every nodes. It's similar to the Ping command, but by using tracert, more detailed information can be obtained. It will offer you all the paths the packets go through, every node's IP, and the time consumption.
net stop	Stop Windows NT service. Eg. net stop dnscache
net send	Send messages to other users, computers or communication name on the network. You need to launch net send for receiving messages.

Appendix 2: Safety Statement & Emissions

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.