# User Manual

## NR70 Router

## Prelimary version 2.8

# Copyright Notice

# Table of Contents

# About this Manual

⌖ **Note:**

For better use experience, it is strongly recommended to use Internet Explorer 8.0 or above, Google Chrome and Firefox.

## 0.1 Web UI Style

The Device's Web User Interface (Web UI) follows the web standards, as follows:

◉ **Radio Button:** Allows you to choose from only one of a predefined set of options.

☑ **Check Box:** Allows you to select one or more options.

**Button:** Allows you to click to perform an action.

**Text Box:** Allows you to enter text information.

: **List Box:** Allows you to select one or more items from a static multiple line text box.

: **Drop-down List:** Allows you to choose one item from a list. When a drop-down list is inactive, it displays a single item. When activated, it drops down a list of items, from which you may select one.

## 0.2 Documents Conventions

### Format

⌖ **Notes**: You need pay attention to the notes content.

◈ **Parameters**: Describe the meaning of parameter or button. If there have "*" before parameters, it couldn't be empty.

- **Bullets**: List the parallel content.

**Boldface font:** Examples of information displayed on the screen.

### Icons

Router

Switch

Modem

Server

Wired Client

Wireless client

PDA

## 0.3 Factory Default Settings

The factory default settings of interfaces are shown in the following table.

| Parameter | Default Value | Description |
|---|---|---|
| User Name | admin | Both the User Name and Password are case sensitive. |
| Password | admin | |
| LAN IP Address | 192.168.1.1/255.255.255.0 | You can use this IP address to access the Device through a Web browser. |

**Table 0- 1 Factory Default Settings of Interface**

# Chapter 1. Hardware Installation

This chapter describes the physical characteristics of the Device, and explains how to install them.

## 1.1 Panel Description

### 1) Front Panel

The LED indicators, the interface and the button are located on the front panel of the Device please see the product.

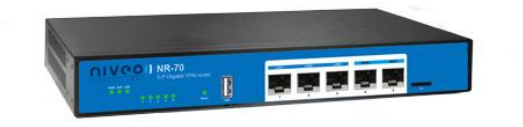


**Figure 1-1 Front Panel_NR70**

| LED | Description |
|---|---|
| PWR | The Power LED indicator is on when the Device is powered on. |
| SYS | The LED indicator blinks twice per second when the system is working properly, and it will blink slower under heavy load. |
| USB | The LED indicator is on when the USB interface is connected properly. |

}

| | |
|---|---|
| 1,2,3,4,5 | The LAN LED indicator is on when Ethernet cable connection is normal, and it blinks when the LAN port is sending or receiving data. |

**Table 1-1 LEDs Description**

| Interface | Description |
|---|---|
| LAN Port | These interfaces provide a LAN connection to network devices, such as PCs or switches. |
| WAN Port | The WAN interface is connected to your Internet device, such as PCs or switches. The number of WAN ports depends on the device model. |
| TF | Connect TF card for data sharing. |
| USB | Plug-in a USB storage for specific features. |

**Table 1-2 Ports Description**

| Button | Description |
|---|---|
| Reset | Reset current settings to the factory default settings. When the Device is powered on, use a pin or paperclip to press and hold the Reset button for more than 5 seconds, and then release the button. After that, the Device will restart with the factory default settings. |
| **Note:** The reset operation will clear all the settings and preferences that you have configured.<br>You can also recover the Device 's factory configuration on the **System > Configuration** page. | |

**Table 1-3 Ports Description**

## 1.2 Installation Guideline

When determining where to place the Device, please observe these guidelines:

- Make sure that your workbench or standard rack is level and stable.
- Do not place heavy objects on the Device!

}

- Make sure that there is proper heat dissipation and adequate ventilation around the Device.

- Position the Device out of direct sunlight and away from sources of heat and ignition.

- Please install the Device in a place far away from the High Power Radio or Radar Station.

- Keep the Device far away from water!

- Please use the supplied power cord.

## 1.3 Installation Requirements

The following items are required for installation:

1) Broadband Internet connection

2) Tools and equipment

   (1) Broadband modem (optional)

   (2) PC with an Ethernet card and TCP/IP installed

   (3) Network devices like hub, switch, wireless access point

   (4) Network cables

   (5) Screwdriver

   (6) Power outlet

## 1.4 Installation Procedure

Follow these steps to install the Device on a flat surface such as a bench:

1) Make sure the Device is powered off.

2) Place the Device upside down on a sturdy, flat bench with a power outlet nearby. Verify that the bench is well grounded.

3) Remove the adhesive backing from the supplied rubber feet. Attach the four rubber feet to the round recessed areas on the bottom of the Device.

4) Turn the Device over to make it right side up on the bench.

## 1.5 Connecting the Device

Before you install the Device, please make sure your PC can connect to the Internet through your broadband service successfully. If there is any problem, please contact with your ISP for help.

After that, please install the Device according to the following steps. Don’t forget to pull out the power plug and keep your hands dry.

1) Power off your PC(s), CableDSL modem, and the Device.

2) Connect the Cable/DSL modem to the Device’s WAN port.

3) Connect one end of an Ethernet cable to one of the LAN ports on the Device, and the other end to a network port on a PC, hub, switch or wireless access point. Repeat this step to connect more PCs or other network devices to the Device.

4) Connect the power cord to the power port of the Device. Then plug the other end of the power cord to a grounded AC power outlet.

5) Power on your network devices, PCs, Switches, Hubs, and so on.

# Chapter 2. the Device

This chapter describes how to configure TCP/IP settings on your computer, and how to login to the Device. In addition, it briefly describes the layout of the Device's Web interface.

## 2.1 Configuring your computer

To configure the Device via Web UI, you need to properly configure TCP/IP settings on the computer that you use to manage the Device. To do this, follow these steps:

**Step 1** Connect the computer to a LAN port of the Device, or connect the computer to the Device through wireless.

**Step 2** Install TCP/IP protocol on your computer. If it is already installed, please skip this step.

**Step 3** Configure TCP/IP settings as **Obtain an IP address automatically** and **Obtain DNS server address automatically**. More information about how to configure TCP/IP, please refer to the chapter: Appendix A FAQ.

**Step 4** Use the Ping command to verify network connectivity between the computer and the Device. Open the command prompt on the computer, type **ping 192.168.1.1**, and then press Enter.

- A successful ping will look like this:

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1:   bytes=32 time<1ms TTL=255

Reply from 192.168.1.1:   bytes=32 time<1ms TTL=255

Reply from 192.168.1.1:   bytes=32 time<1ms TTL=255

Reply from 192.168.1.1:   bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:

     Packets:   Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:
```

}

- An unsuccessful ping will look like this:

```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.1.1:

Packets:    Sent = 4, Received = 0, Lost = 4 (100% loss),
```

If the Ping command is successful, the connection between the computer and the Device is working properly. If the Ping command fails, please do the following:

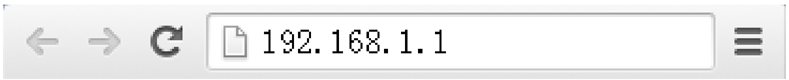
1) Check physical connection: Verify that the LAN LED on the Device and the LED on your computer's network card are lit.

2) Check TCP/IP settings: Verify that your computer is on the same subnet as the Device's LAN interface. E.g., if the Device's LAN IP address is 192.168.1.1 (default), the computer's IP address must be an unused IP address in the 192.168.1.0/24 subnet.

## 2.2 Logging to the Device

No matter what operating system is installed on your computer, such as, MS Windows, Macintosh, UNIX, or Linux, and so on, you can configure the Device through the Web browser (e.g., Internet Explorer, Firefox).

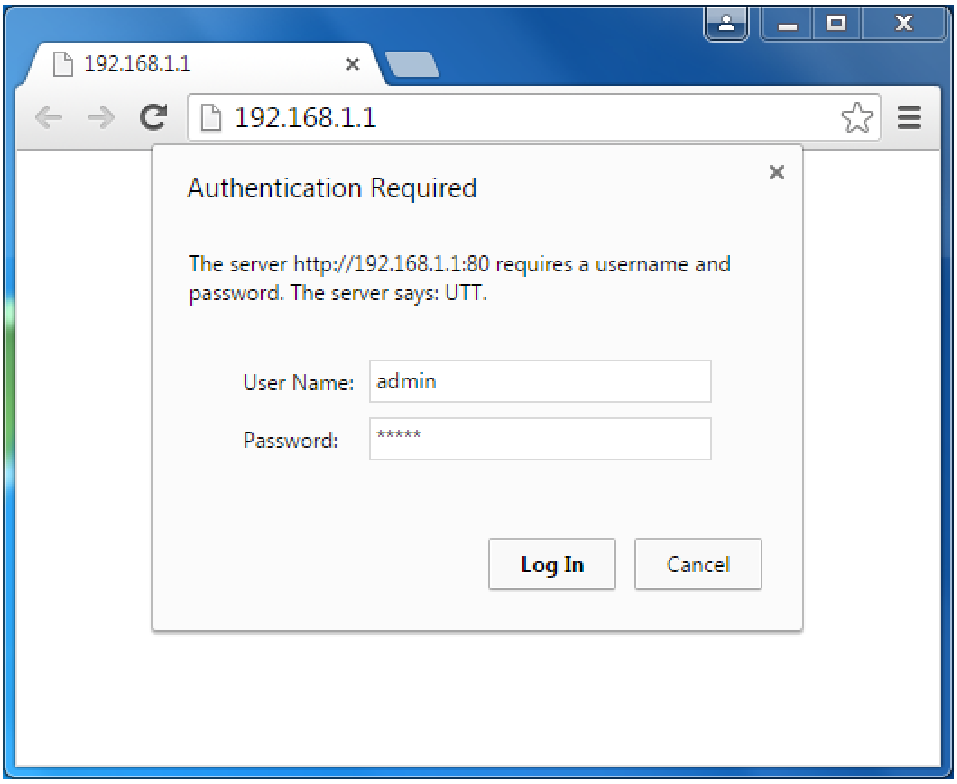
**Step 1:** For local access of the Device's web-based utility, launch your web browser, and enter the Device's default IP address: **192.168.1.1**, in the URL filed. Then press the Enter key.



192.168.1.1

**Figure 2-1 Address Bar**

**Step 2:** A login screen prompts you for your User name and Password. Enter **admin** (case sensitive) in the User name field, and enter **admin** in the Password field. Then click **Log In**.



Authentication Required

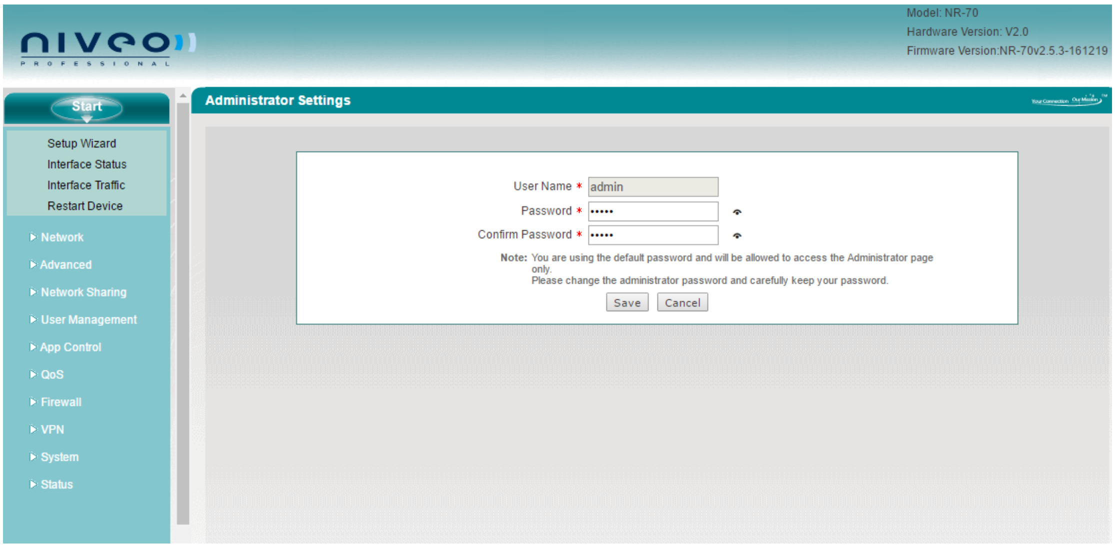
The server http://192.168.1.1:80 requires a username and password. The server says: UTT.

User Name: admin

Password: *****

**Figure 2-2 Login Screen**

**Step 3:** After log in the Device, the first screen that appears is the Homepage.



Model: NR-70
Hardware Version: V2.0
Firmware Version:NR-70v2.5.3-161219

Administrator Settings

User Name * admin

Password * •••••

Confirm Password * •••••

**Note:** You are using the default password and will be allowed to access the Administrator page only.
Please change the administrator password and carefully keep your password.

**Figure 2-3 Homepage**

Home page Description:

}

(1) Niveo Logo: Click to go to the home page on the UTT website.

(2) Model, Hardware Version and Software Version: Displays the model number, software version and firmware version of the Device.

(3) Quick Link Icons: Provide quick links to the corresponding pages on the UTT website.

- Product: Click to go to the products page on the UTT website to find more products.
- Forum: Click to go to the forum home page on the UTT website to participate in product discussions.
- Feedback: Click to send us your feedback by email.

1) On left side there is two-level main menu bar. You can click a first level menu item to reveal its submenu items, click again to hide them.

2) The main operating page is located on the centre of the page, in which you can configure various functions, view the related configuration information and status information, etc.

3) The bottom of the page there is copyright information.

# Chapter 3. Start Menu

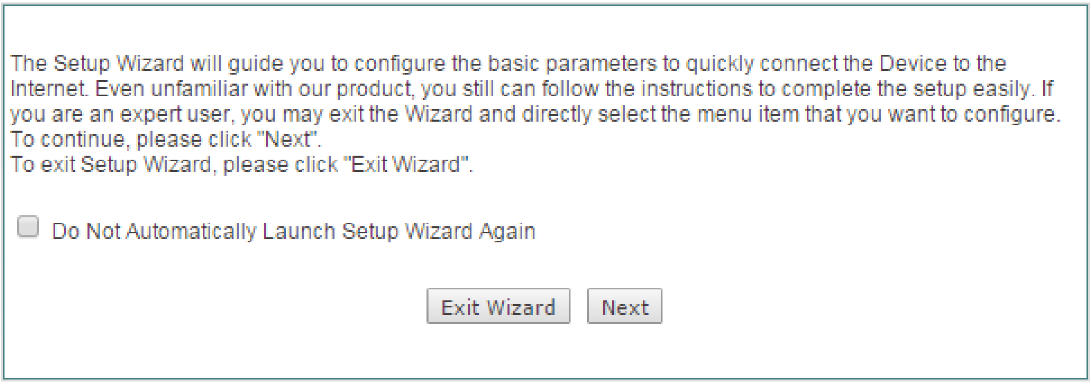
The **Start** menu is located in the upper left of the WEB interface, which provides you four commonly used functions: **Setup Wizard**, **Interface Status**, **Interface Traffic**, and **Restart Device**. In this chapter, you can configure the basic parameters to access to internet, view each physical interface's detail information and restart the Device.

## 3.1 Setup Wizard

This section describes the **Start > Setup Wizard** page. The Setup Wizard will guide you to configure the basic parameters to quickly connect the Device to the Internet. Even unfamiliar with the product, you still can follow the instructions to complete the setup easily.

### .1.1 Running the Setup Wizard

The first page appears is **Setup Wizard** immediately after your first login.



The Setup Wizard will guide you to configure the basic parameters to quickly connect the Device to the Internet. Even unfamiliar with our product, you still can follow the instructions to complete the setup easily. If you are an expert user, you may exit the Wizard and directly select the menu item that you want to configure.
To continue, please click "Next".
To exit Setup Wizard, please click "Exit Wizard".

□ Do Not Automatically Launch Setup Wizard Again

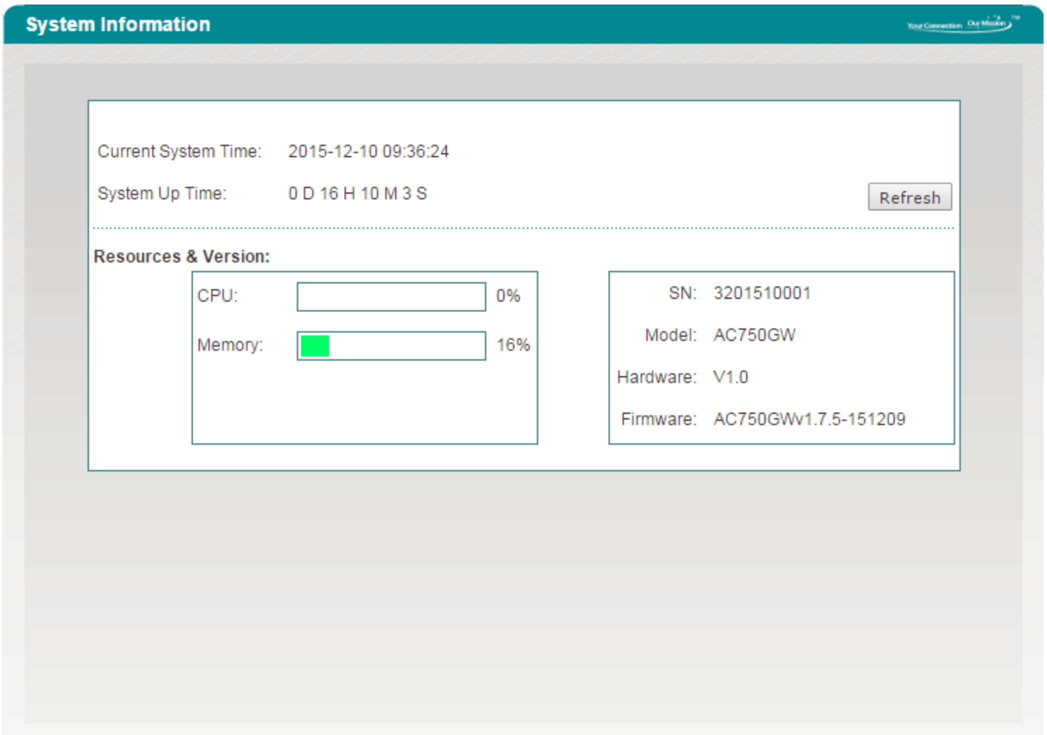
**Figure 3-1 Running the Setup Wizard**

- **Do Not Automatically Launch Setup Wizard Again:** If selected, the system don't automatically launch the **Setup Wizard** the next time you login to the Device, instead directly open the **System Information** page(see Figure 3-2). Else, the system will still launch the **Setup Wizard** automatically.

- **Exit Wizard:** Click to exit the **Setup Wizard** and go to the **System Information** page (see Figure 3-2). The changes made in the **Setup Wizard** will be discarded.

- **Next:** Click to enter into the next page of the **Setup Wizard**.

}



System Information

Current System Time: 2015-12-10 09:36:24

System Up Time: 0 D 16 H 10 M 3 S

Refresh

Resources & Version:

CPU: 0%

Memory: 16%

SN: 3201510001

Model: AC750GW

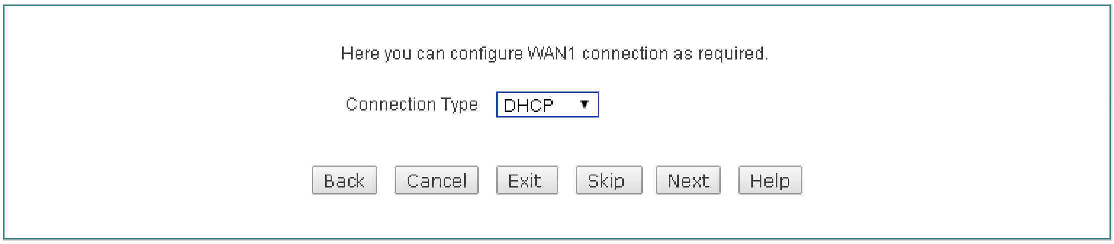
Hardware: V1.0

Firmware: AC750GWv1.7.5-151209

**Figure 3-2 System Information**

## .1.2 Setup Wizard - WAN1 Settings

There are three connection types you can configure for WAN Internet connection: PPPoE, Static IP and DHCP. For the detail information, you can refer to the chapter: 4.1 WAN.



Here you can configure WAN1 connection as required.

Connection Type DHCP

**Figure 3-3 Setup Wizard_WAN1 Settings**

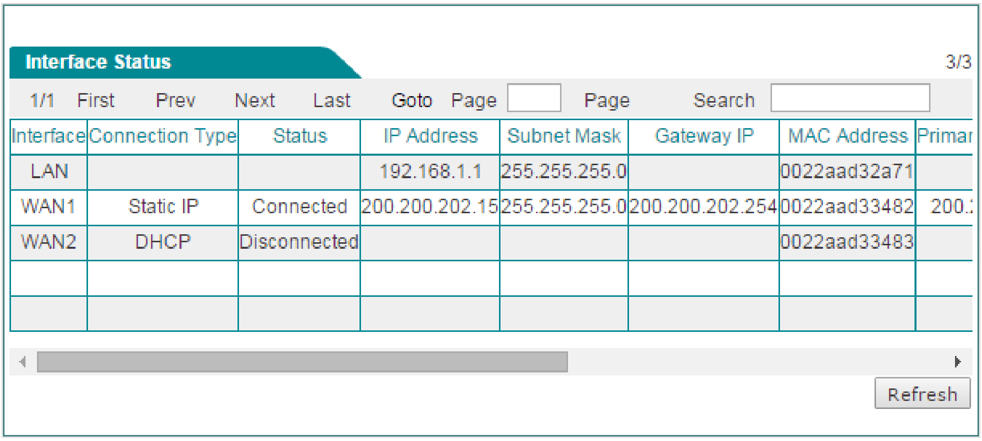
**Figure 3-4 Setup Wizard_2.4G Wireless Settings**

- the optimal channel bandwidth.

}

## 3.2 Interface Status

On the **Start** > **Interface Status** page, you can view the current status of all physical interface, including the type of interface, connection type, status, IP address, duration and so on.



| Interface | Connection Type | Status | IP Address | Subnet Mask | Gateway IP | MAC Address | Primar |
|---|---|---|---|---|---|---|---|
| LAN | | | 192.168.1.1 | 255.255.255.0 | | 0022aad32a71 | |
| WAN1 | Static IP | Connected | 200.200.202.15 | 255.255.255.0 | 200.200.202.254 | 0022aad33482 | 200.: |
| WAN2 | DHCP | Disconnected | | | | 0022aad33483 | |
| | | | | | | | |
| | | | | | | | |

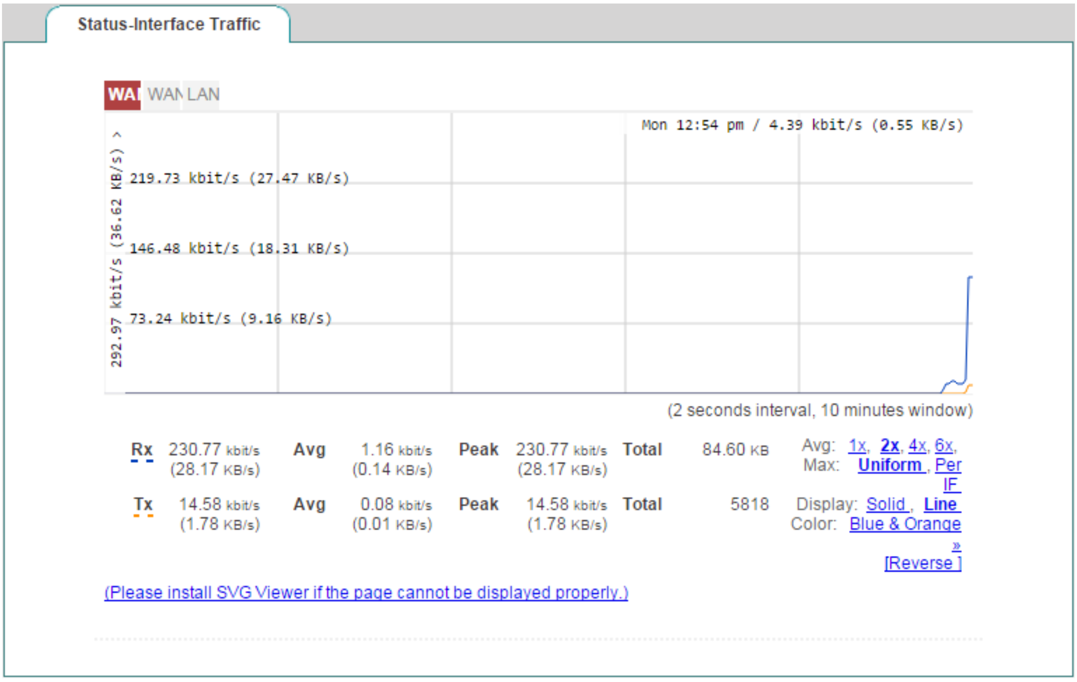
Figure 3-5 Interface Status

## 3.3 Interface Traffic

The interface rate chart dynamically displays the real-time RX/TX rate, average RX/TX rate, maximum RX/TX rate and total RX/TX traffic of each physical interface. If you want to view the rate chart of an interface, click the corresponding interface name hyperlink.

In the interface rate chart, the abscissa (x-axis) shows the time axis, and the ordinate (y-axis) shows the real-time RX/TX rate axis. Furthermore, you can adjust some parameters of the chart if needed, such as the time interval during which the real-time rates are calculated and displayed, and the displayed colors.

**Note:** The rate chart can only show the rate and traffic information in the last ten minutes. Each time you launch this page, the rate chart refreshes.


Status-Interface Traffic
WAN
WAN LAN
Mon 12:54 pm / 4.39 kbit/s (0.55 KB/s)
292.97 kbit/s (36.62 KB/s) ^
219.73 kbit/s (27.47 KB/s)
146.48 kbit/s (18.31 KB/s)
73.24 kbit/s (9.16 KB/s)

(2 seconds interval, 10 minutes window)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Rx | 230.77 kbit/s<br>(28.17 KB/s) | Avg | 1.16 kbit/s<br>(0.14 KB/s) | Peak | 230.77 kbit/s<br>(28.17 KB/s) | Total | 84.60 KB | Avg: 1x, 2x, 4x, 6x,<br>Max: Uniform, Per IF |
| Tx | 14.58 kbit/s<br>(1.78 KB/s) | Avg | 0.08 kbit/s<br>(0.01 KB/s) | Peak | 14.58 kbit/s<br>(1.78 KB/s) | Total | 5818 | Display: Solid, Line<br>Color: Blue & Orange »<br>[Reverse] |

(Please install SVG Viewer if the page cannot be displayed properly.)

Figure 3-6 Interface Status

- **RX:** Displays the real-time RX rate of the physical interface, which refreshes every two seconds. For the LAN interface, RX means uploading; for the WAN interface, it means downloading.

- **TX:** Displays the real-time TX rate of the physical interface, which refreshes every two seconds. For the LAN interface, TX means downloading; for the WAN interface, it means uploading.

- **Avg:** Displays the average RX or TX rate of the physical interface since last opened the current page.

- **Peak:** Displays the maximum RX or TX rate of the physical interface since last opened the current page.

- **Total:** Displays the total RX or TX traffic of the physical interface since last opened the current page.

- **LAN/WANx:** Click the interface name hyperlink to view the rate chart of the selected interface. Therein, x (value: 1, 2, 3, 4) indicates the corresponding WAN interface, and the number of WAN interfaces depends on the specific product model. For example, click the **WAN1** hyperlink to view the rate chart of the WAN1 interface.

**Note:**

If the SVG Viewer isn't installed on your PC, the rate chart cannot be displayed properly. To view the rate chart, click the **(Please install svgviewer if the page cannot display properly.)** hyperlink to download and install the SVG Viewer.

}

## 3.4 Restart Device

On the **Start > Restart Device** page, you can restart the Device. Clicking the **Restart** button, the system will pop up a dialog. Then you can click the **OK** button to restart the Device, or click the **Cancel** button to cancel the operation.

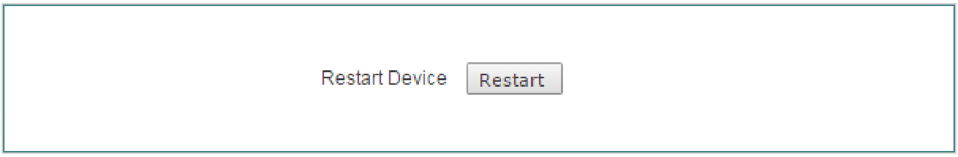


**Figure 3-7 Restart Device**

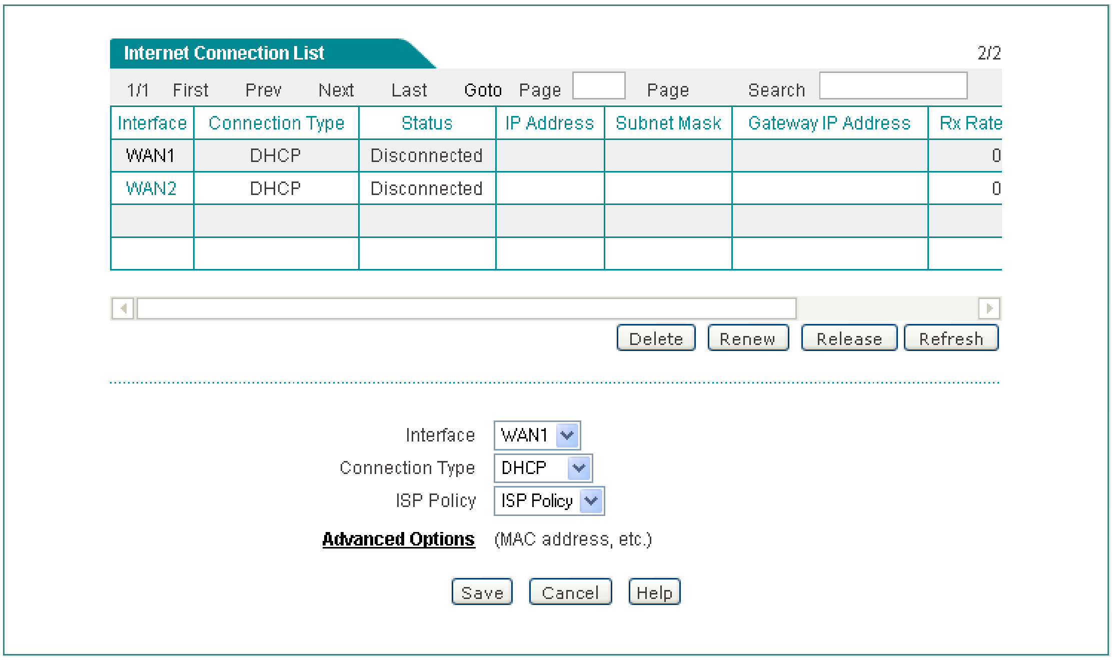
**Note:** Because restarting the Device will disconnect all the sessions, please do it with caution.

}

# Chapter 4. Network Menu

## 4.1 WAN

This section describes **Network > WAN** page, you can setup the way access to Internet. There are three connection types: **PPPoE**, **Static IP** and **DHCP** (Obtain an IP automatically). Depending on which connection type you select, you will see various settings. We will describe the settings for each connection type respectively.



Internet Connection List 2/2

| Interface | Connection Type | Status | IP Address | Subnet Mask | Gateway IP Address | Rx Rate |
|---|---|---|---|---|---|---|
| WAN1 | DHCP | Disconnected | | | | 0 |
| WAN2 | DHCP | Disconnected | | | | 0 |
| | | | | | | |
| | | | | | | |

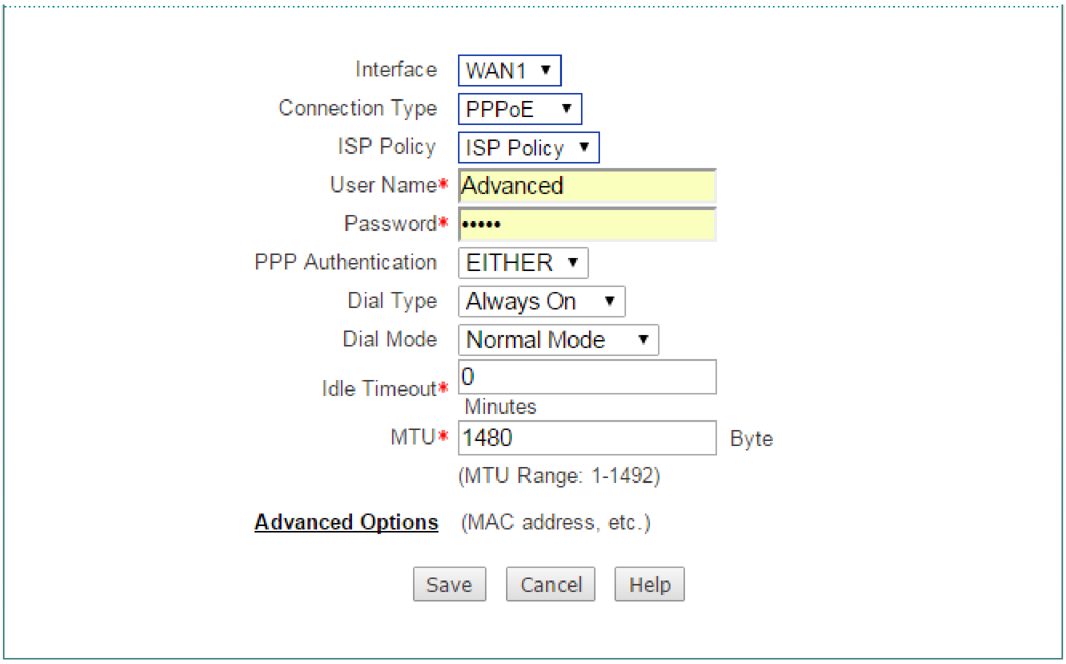
| | |
|---|---|
| Interface | WAN1 |
| Connection Type | DHCP |
| ISP Policy | ISP Policy |
| **Advanced Options** | (MAC address, etc.) |

**Figure 4-1 Select Connection Type**

### .1.1 PPPoE Connection

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Most DSL-based Internet Service Providers (ISPs) use PPPoE to establish Internet connections for end-users. If you use a DSL line, check with your ISP to see if they use PPPoE, and then select **PPPoE**.

}



| | |
|---|---|
| Interface | WAN1 ▼ |
| Connection Type | PPPoE ▼ |
| ISP Policy | ISP Policy ▼ |
| User Name* | Advanced |
| Password* | ••••• |
| PPP Authentication | EITHER ▼ |
| Dial Type | Always On ▼ |
| Dial Mode | Normal Mode ▼ |
| Idle Timeout* | 0<br>Minutes |
| MTU* | 1480 Byte<br>(MTU Range: 1-1492) |
| Advanced Options | (MAC address, etc.) |

**Figure 4-2 PPPoE Connection Setup**

- **ISP Policy:** Select the ISP Policy (i.e., route policy database) for each Internet connection. Thus all traffic destined to an ISP's servers will be forwarded through that ISP's connection.

- **User Name and Password**: Enter the PPPoE login user name and password provided by your ISP.

- **PPP Authentication:** Specify the PPP authentication mode, available options: **NONE**, **PAP**, **CHAP** and **Either**.

  - **None:** If selected, no protocol will be used.

  - **PAP:** If selected, PAP (Password Authentication Protocol) protocol will be used for PPP authentication.

  - **CHAP:** If selected, CHAP (Challenge Handshake Authentication Protocol) protocol will be used for PPP authentication.

  - **Either:** If selected, the Device will automatically negotiate with the peer device to use PAP or CHAP protocol.

- **Dial Type:** Select the type of dial connection, available options are **Always On**, **On Demand** and **Manual**.

  - **Always On:** If selected, the Device will establish a PPPoE session when starting up and automatically re-establish the PPPoE session once disconnected.

}

  - **On Demand:** If selected, the Device will establish a PPPoE session only when there are packets requesting to access the Internet (i.e., when a program on your computer attempts to access the Internet).

  - **Manual:** If selected, you can dial or hang up a PPPoE session manually.

- **Dial Mode:** If the PPPoE connection isn't established successfully even using correct user name and password, you may try to use other modes.

- **Idle Timeout:** Specify the during time the Device keeps the Internet connection active after no traffic. Which means not terminate Internet connection when the value is zero.

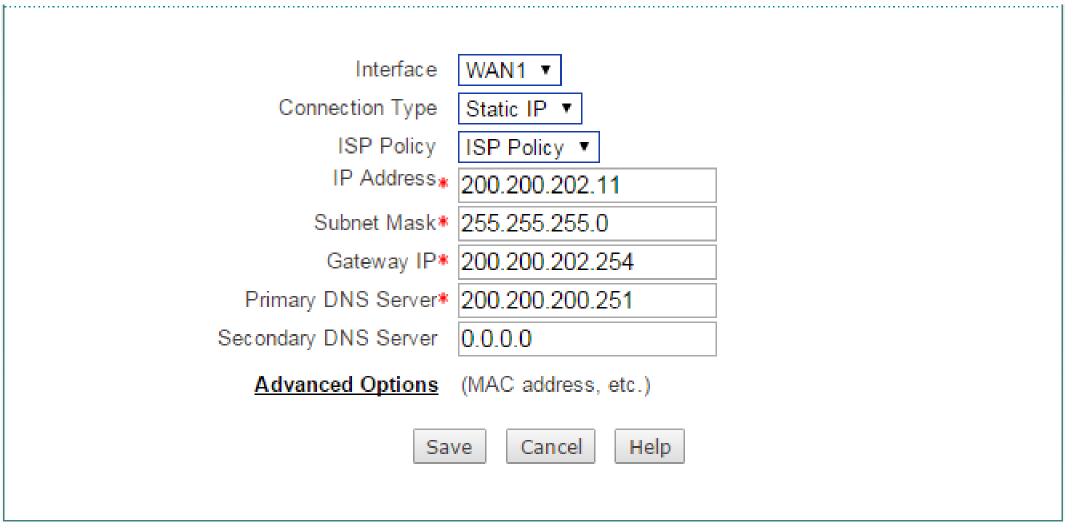
- **MTU:** When dialing, the Device will automatically negotiate MTU (maximum transmission unit) with the peer device. Please leave the default value of 1480 bytes, unless you have a special application.

- **Advanced Options:** Click to configure advanced parameters. In most case, you need not configure them.

## .1.2 Static IP Connection

Some infrastructure situations have to use static address, such as finding the Domain Name System (DNS) host where it is, the Device will translate domain names to IP addresses. Static addresses are convenient, but not absolutely necessary, to locate servers inside an enterprise.

If you are required to use a permanent IP address, select **Static IP**.



| | |
|---|---|
| Interface | WAN1 ▾ |
| Connection Type | Static IP ▾ |
| ISP Policy | ISP Policy ▾ |
| IP Address* | 200.200.202.11 |
| Subnet Mask* | 255.255.255.0 |
| Gateway IP* | 200.200.202.254 |
| Primary DNS Server* | 200.200.200.251 |
| Secondary DNS Server | 0.0.0.0 |
| Advanced Options | (MAC address, etc.) |

**Figure 4-3 Static IP Connection Setup**

}

- **ISP Policy:** Select the ISP Policy (i.e., route policy database) for each Internet connection. Thus all traffic destined to an ISP's servers will be forwarded through that ISP's connection.

- **IP Address:** Enter the IP address for the Device's WAN interface, which is provided by your ISP.

- **Subnet Mask:** Enter the subnet mask for the Device's WAN interface, which is provided by your ISP.

- **Gateway IP:** Enter the IP address for the default gateway, which is provided by your ISP.

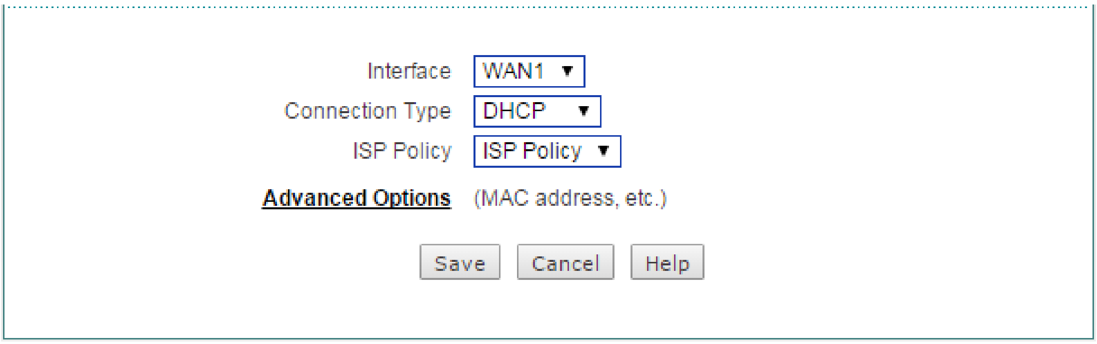
- **Primary DNS Server:** Enter the IP address of your ISP's primary DNS server.

- **Secondary DNS Server:** Enter the IP address of your ISP's secondary DNS server if it is available.

## .1.3 DHCP Connection

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

If your ISP automatically assigns an IP address, select **DHCP**. Most cable modem subscribers use this connection type.



Interface: WAN1

Connection Type: DHCP

ISP Policy: ISP Policy

Advanced Options (MAC address, etc.)

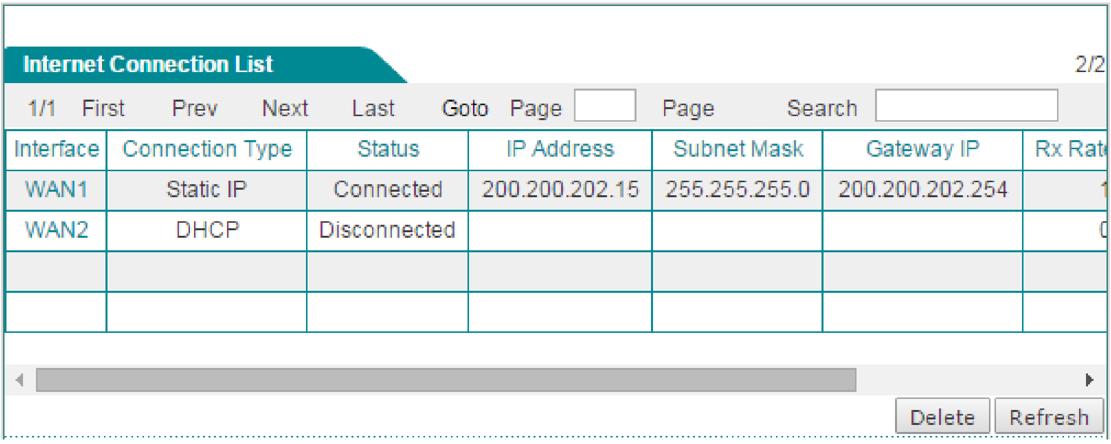
**Figure 4-4 DHCP Connection Setup**

## .1.4 Internet Connection List

When you have configured the Internet connection, you can view its status in the

}

**Internet Connection List**. Click **Refresh** button to view current status of the connection.



Internet Connection List 2/2

1/1 First Prev Next Last Goto Page Page Search

| Interface | Connection Type | Status | IP Address | Subnet Mask | Gateway IP | Rx Rat |
|---|---|---|---|---|---|---|
| WAN1 | Static IP | Connected | 200.200.202.15 | 255.255.255.0 | 200.200.202.254 | 1 |
| WAN2 | DHCP | Disconnected | | | | 0 |
| | | | | | | |
| | | | | | | |

Figure 4-5 Internet Connection List

- **Interface:** Displays the name of the physical interface to which the connection is bound.

- **Connection Type:** Displays the type of the Internet connection.

- **Status:** Displays the current status of the Internet connection. If the connection is successful, it displays Connected, else it displays Disconnected. When the status is connected on PPPoE mode, it will also display the elapsed time (day: hour: minute: second) since connected. And when the status is connected on DHCP mode, it will also display the time left before the lease expires (day: hour: minute: second) for current IP address, which is assigned by your ISP’s DHCP server.

- **IP Address, Subnet Mask and Gateway IP:** When the connection type is **PPPoE** or **DHCP**, it displays the IP Address, Subnet Mask and Gateway IP provided by ISP. When the connection type is **Static IP**, it displays the IP Address, Subnet Mask and Gateway IP you set.

- **Rx Rate(bps):** Displays the current download rate of the connection between the refresh interval.

- **Tx Rate(bps):** Displays the current upload rate of the connection between the refresh interval.

## .1.5 Edit the Connection

If you want to edit the connection, do the following:

**Step 1** In the **Internet Connection List**, click the WAN interface hyperlink, the

}

related information will be displayed in the setup fields.

**Step 2** Modify the connection settings.

**Step 3** Click the **Save** button to save the settings.

## .1.6 Delete the Connection

If you want to delete the connection, do the following:

**Step 1** In the **Internet Connection List**, click the related WAN hyperlink, the related information will be displayed in the setup fields.

**Step 2** Click the **Delete** button below the **Internet Connection List**.

**Step 3** In the pop-up window, click the **OK** button to delete the connection.

**Note:** The default **WAN1** connection can’t be deleted but edited.

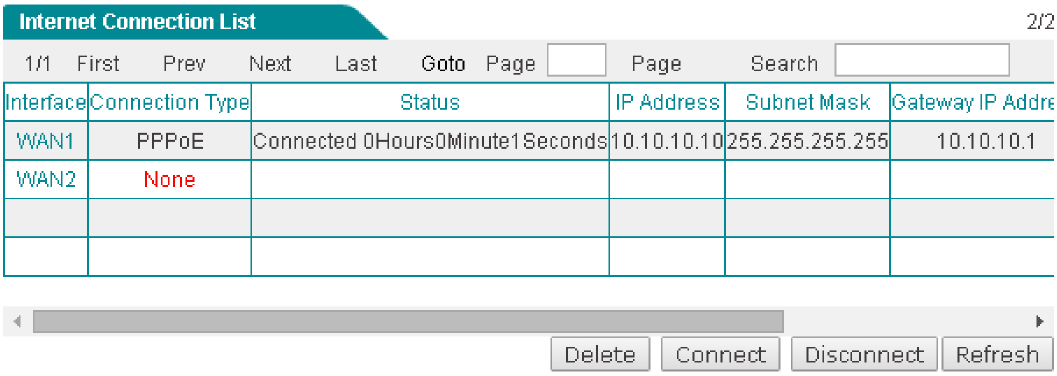
## .1.7 Dial or Hang up a PPPoE connection

If the connection type is PPPoE, when you click the **WAN1** hyperlink, the **Connect**, **Disconnect** and **Refresh** buttons will be shown on the Internet Connection List.

**Note:**

1) If you have chosen **Manual** as Dial Type for PPPoE connection, you need click the **Connect** button to dial-up the Internet connection, and click the **Disconnect** button to hang it up.

2) Click the **Refresh** button to view current status of the connection.



| Interface | Connection Type | Status | IP Address | Subnet Mask | Gateway IP Addre |
|---|---|---|---|---|---|
| WAN1 | PPPoE | Connected 0Hours0Minute1Seconds | 10.10.10.10 | 255.255.255.255 | 10.10.10.1 |
| WAN2 | None | | | | |
| | | | | | |
| | | | | | |

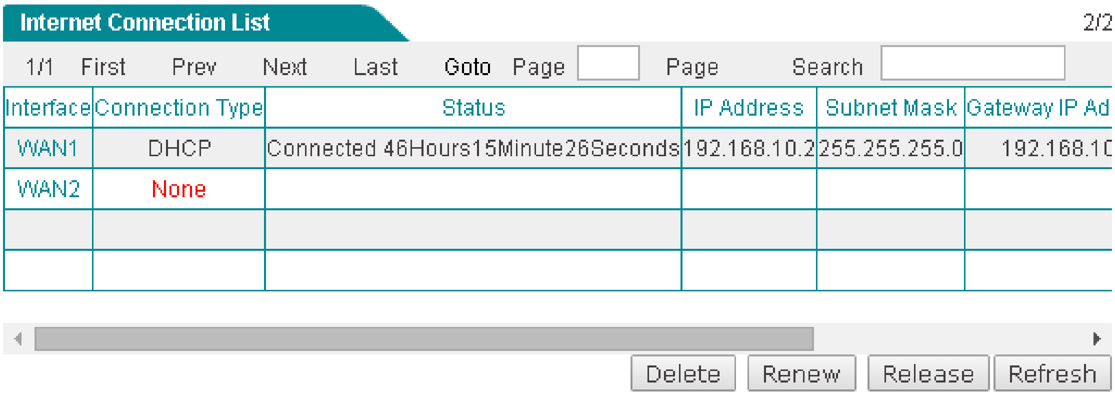
}

**Figure 4-6 Internet Connection List_PPPoE Connection**

### .1.8 Renew or Release a DHCP Connection

If the connection type is DHCP, when you click the **WAN1** hyperlink, the **Renew**, **Release** and **Refresh** buttons will be shown on the Internet Connection List.

Click the **Renew** button to re-acquire an IP address from the ISP's DHCP server. Click the **Release** button to release the IP address obtained from the ISP's DHCP server. Click the **Refresh** button to view current status of the connection.



| Interface | Connection Type | Status | IP Address | Subnet Mask | Gateway IP Ad |
|---|---|---|---|---|---|
| WAN1 | DHCP | Connected 46Hours15Minute26Seconds | 192.168.10.2 | 255.255.255.0 | 192.168.1C |
| WAN2 | None | | | | |
| | | | | | |
| | | | | | |

**Figure 4-7 Internet Connection List - DHCP Connection**

## 4.2 Load Balancing

This section describes the **Network > Load Balancing** page. When using multiple Internet connections, you can configure load balancing related parameters, such as, load balancing mode, detection interval, retry times, and ID binding, and so on.

### .2.1 Internet Connection Detection Mechanism

When using multiple Internet connections, the Device should has the ability to real-time monitor each Internet connection to ensure the network will not be interrupted even a connection is faulty. To this end, we design flexible automatic detection mechanism on the Device, and provide multiple detection methods to meet the actual requirements.

For the sake of convenience, we firstly introduce several parameters.

- **Detection Target IP:** The IP address of a target device. The Device will monitor an Internet connection by sending the detection packets to the specified target IP address.

}

- **Detection Interval:** The time interval at which the Device periodically sends detection packets, one packet at a time. Especially, if you don’t want to monitor an Internet connection, please set it as 0.

- **Retry Times:** The number of retries per detection period.

For a normal Internet connection and a faulty Internet connection, the detection mechanisms are different.

For a faulty normal Internet connection, the detection mechanism is as follows: The Device periodically sends a detection packet at the specified time interval to the target IP address. Once no response packet received during a detection period, the Device will consider that the connection is faulty and shield it immediately. For example, by default, if the Device has sent three detection packets but not received any response packet during a detection period, it will consider that the connection is faulty.

For a normal Internet connection, the detection mechanism is as follows: Similarly, the Device also periodically sends a detection packet at the specified time interval to the target IP address. Once more than half of the response packets received during a detection period, the Device will consider that the connection is back to normal and enable it immediately. For example, by default, if the Device has sent three detection packets and received two packets during a detection period, it will consider that the connection is back to normal.

**Note:** If you don’t want to monitor an Internet connection, please set the value of **Detection Interval** as 0.

## .2.2 Global Settings

The Device provides two connection groups: primary connection group and backup connection group. An Internet connection belonging to the primary connection group is a primary connection, while an Internet connections belonging to the backup connection group is a backup connection. By default, all the Internet connections are primary connections. It allows you to divide one or more connections into the backup connection group.

The Device provides two load balancing modes: **Full Load Balancing** and **Partial Load Balancing**.

If you choose to use **Full Load Balancing**, all the Internet connections are used as primary connections. The operation principle is as follows:

1) If all the Internet connections are normal, the LAN users will use these connections to access the Internet.

}

2) If an Internet connection is faulty, the Device will shield it immediately, and the traffic through the faulty connection will be distributed to other normal connections automatically.

3) Once the faulty connection is back to normal, the Device will enable it immediately, and the traffic will be redistributed automatically.

If you choose to use **Partial Load Balancing**, some Internet connections are used as primary connections, and others are used as backup connections. The operation principle is as follows:

1) As long as one or more primary connections are normal, the LAN users will use the primary connection(s) to access the Internet. In this case, if there is more than one primary connection, the Device will control and balance the traffic among these connections.

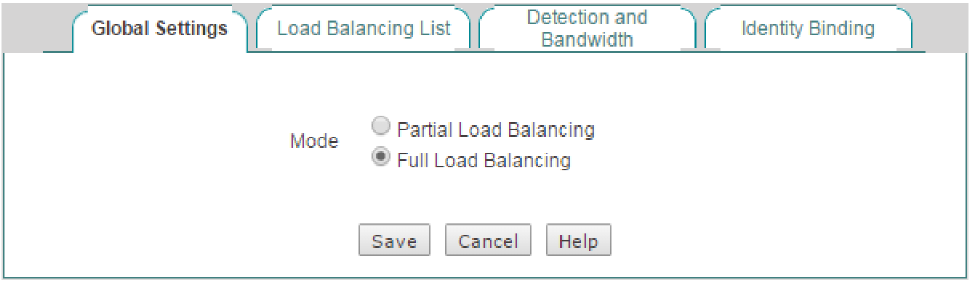
2) If all the primary connections are faulty, it will automatically switch to the backup connection(s) to let the LAN users use them to access the Internet. In this case, if there is more than one backup connection, the Device will control and balance the traffic among these connections.

3) Once one or more faulty primary connections are back to normal, it will automatically switch back to the primary connection(s).

⌖ **Note:** During connections switching, some user applications (such as some online games) may be interrupted unexpectedly due to the nature of TCP connection. UTT Technologies Co., Ltd. will not bear all the losses and legal proceedings caused by it.

## 4.2.2.1 Full Load Balancing

Select the **Full Load Balancing** checkbox and click the **Save** button to save the settings.



Mode ○ Partial Load Balancing ● Full Load Balancing

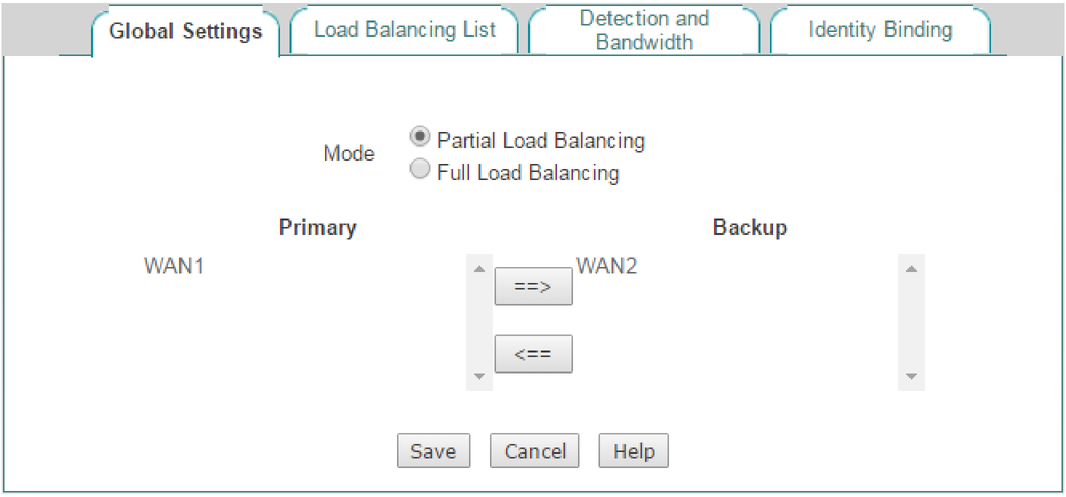
**Figure 4-8 Full Load Balacing**

## 4.2.2.2 Partial Load Balancing

Select the **Partial Load Balancing** checkbox and then set primary connection and

}

backup connection, lastly click the **Save** button to save the settings.



Mode ● Partial Load Balancing ○ Full Load Balancing

Primary: WAN1

Backup: WAN2

**Figure 4-9 Partial Load Balancing**

- **Mode:** Specify the mode of load balancing. Here please select **Partial Load Balancing**.

- **Primary:** Specify the primary connection group. An Internet connection in the **Primary** list box is a primary connection.

- **Backup:** Specify the backup connection group. An Internet connection in the **Backup** list box is a backup connection.

- **==>:** Select one or more Internet connections in the **Primary** list box, and then click **==>** to move the selected connection(s) to the **Backup** list box.

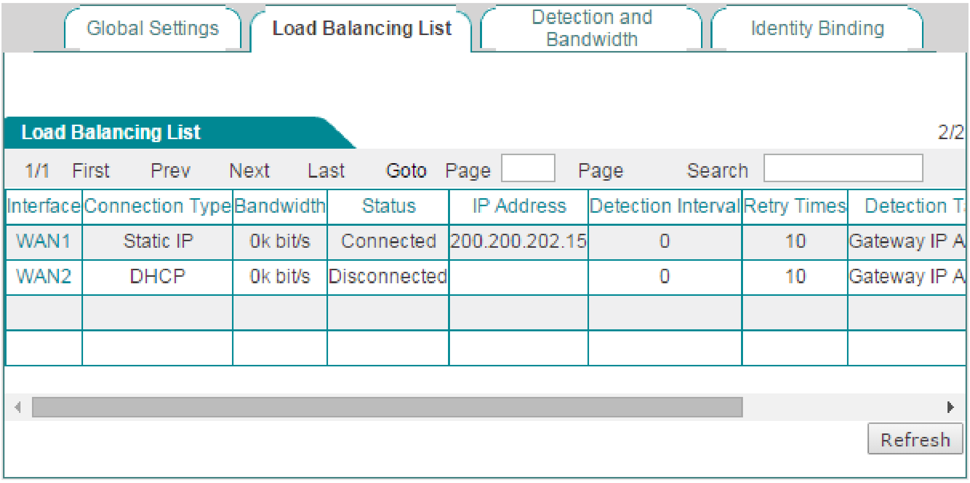
- **<==:** Select one or more Internet connections in the **Backup** list box, and then click **<==** to move the selected connection(s) to the **Primary** list box.

## .2.3 Load Balancing List

When you have configured load balancing parameters for one or more Internet connections, you can view the related configuration and status information in the **Load Balancing List**.

If you want to modify the detection related parameters, click its **Edit** hyperlink, the related information will be displayed in the **Detection and Bandwidth** page. Then configure or modify it, and click the **Save** button.

}

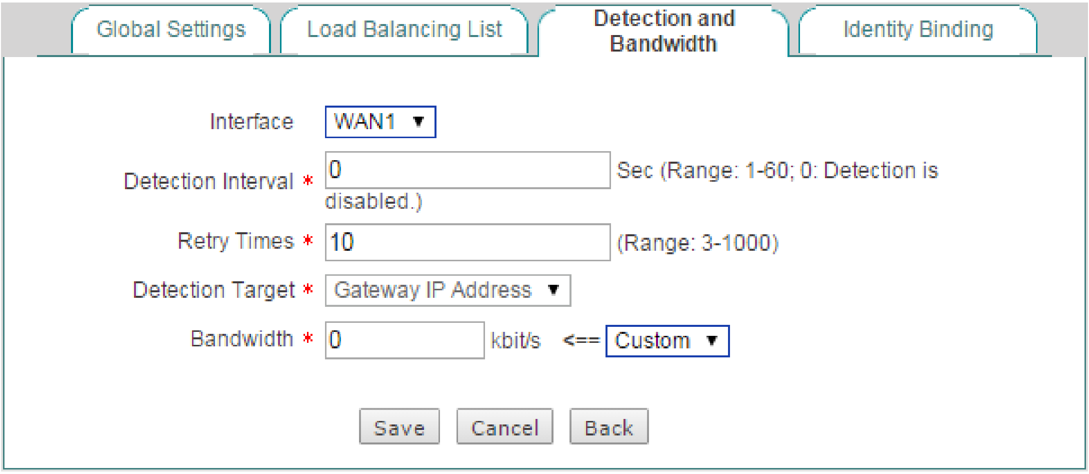


| Interface | Connection Type | Bandwidth | Status | IP Address | Detection Interval | Retry Times | Detection T |
|---|---|---|---|---|---|---|---|
| WAN1 | Static IP | 0k bit/s | Connected | 200.200.202.15 | 0 | 10 | Gateway IP A |
| WAN2 | DHCP | 0k bit/s | Disconnected | | 0 | 10 | Gateway IP A |
| | | | | | | | |
| | | | | | | | |

Figure 4-10 Load Balancing List

## .2.4 Detection and Bandwidth

In the **Network > Load Balancing > Detection and Bandwidth** page, you can configure the connection detection related parameters for each Internet connection respectively.



Interface: WAN1 ▼

Detection Interval *: 0 Sec (Range: 1-60; 0: Detection is disabled.)

Retry Times *: 10 (Range: 3-1000)

Detection Target *: Gateway IP Address ▼

Bandwidth *: 0 kbit/s <== Custom ▼

Figure 4-11 Detection and Bandwidth Settings

- **Interface:** Select the physical interface you want to set load balancing.

- **Detection Interval:** Specify the time interval at which the Device periodically sends detection packets, one packet at a time. The value should be between 1 and 60 seconds, or 0. 0 means that connection detection is disabled on the selected Internet connection.

- **Retry Times:** Specify the number of retries per detection period.

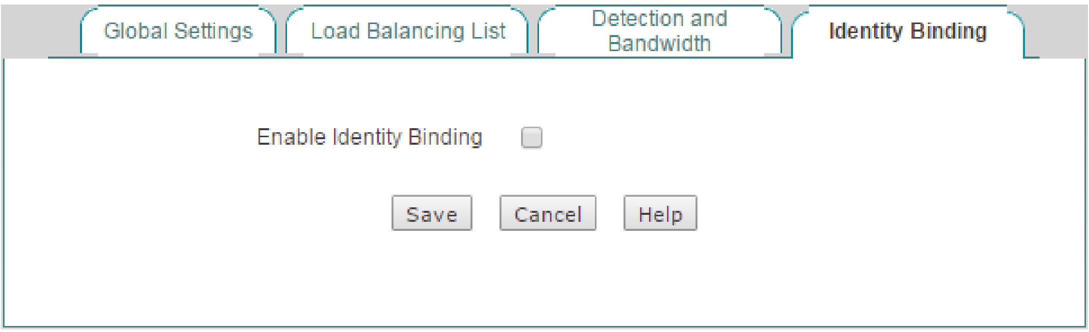
}

- **Detection Target:** The IP address of a detection target device. The Device will monitor an Internet connection by sending the detection packets to the detection target IP address. If you select **Gateway IP Address** from the drop-down list, the Device will send the detection packets to the selected Internet connection's default gateway; If you select **Other IP Address** from the drop-down list, you need enter an appropriate public IP address in the associated text box, then the Device will send the detection packet to this IP address.

- **Bandwidth:** Specify the bandwidth of this interface provided by ISP.

### .2.5 Identity Binding

When using multiple Internet connections, the same application will be assigned to the different connections, thus some applications (such as online banking, QQ, etc.) cannot be used normally due to the identity change. We provide ID binding feature to solve this problem: After you enable Identity Binding, the Device will assign the same application to the same Internet connection. For example, when a LAN user logs in to an online banking system, if the first session is assigned to the WAN2 Internet connection, henceforth all the subsequent NAT sessions of the online banking application will be assigned to the WAN2 connection until the user logs out.



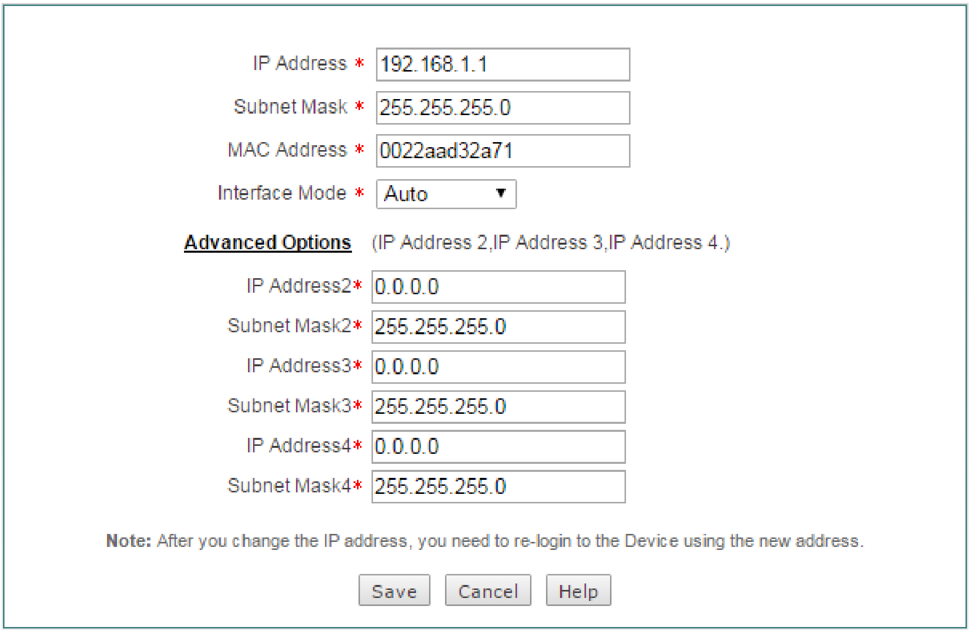
Enable Identity Binding □

**Figure 4-12 Identity Binding**

- **Enable ID Binding:** If selected, you will enable ID binding feature for some applications such as online banking, QQ, etc.

## 4.3 LAN

This section describes **Network > LAN** page. You can set up to four IP addresses for the LAN interface. With the IP address of LAN interface, you can login to the Device. If the IP address has been changed, you need to re-login to the Device using the new address.



IP Address * 192.168.1.1

Subnet Mask * 255.255.255.0

MAC Address * 0022aad32a71

Interface Mode * Auto

Advanced Options (IP Address 2,IP Address 3,IP Address 4.)

IP Address2* 0.0.0.0

Subnet Mask2* 255.255.255.0

IP Address3* 0.0.0.0

Subnet Mask3* 255.255.255.0

IP Address4* 0.0.0.0

Subnet Mask4* 255.255.255.0

**Note:** After you change the IP address, you need to re-login to the Device using the new address.

**Figure 4-13 LAN Settings**

- **IP Address:** Specify the IP address of the LAN interface. The default value is 192.168.1.1.

- **Subnet Mask:** Specify the subnet mask that defines the range of the LAN. The default value is 255.255.255.0.

- **MAC Address:** The MAC address of the LAN interface. We recommend that you do not change the default value unless absolutely necessary.

- **Interface Mode:** Specify the speed and duplex mode of the LAN interface. The Device supports five or six modes (Note that only the gigabit LAN interface supports **1000M-HD**), which include **Auto** (Auto-negotiation), **10M-HD** (10M Half-Duplex), **10M-FD** (10M Full-Duplex), **100M-HD** (100M Half-Duplex), **100M-FD** (100M Full-Duplex), and **1000M-FD** (1000M Full-Duplex). In most cases, please leave the default value. If a compatibility problem occurred, or the network device connected to the LAN interface doesn't support auto-negotiation function, you may modify it as required.

**Note:**

1) You can assign two IP addresses to the Device's LAN interface to connect two subnets. The hosts on the two subnets can communicate with each other.

2) If you have changed the LAN IP address and saved the change, you should use the new IP address to re-login to the Device. And the default gateway of each LAN host should be changed to this new IP address, thus the LAN hosts can access the Device and Internet.

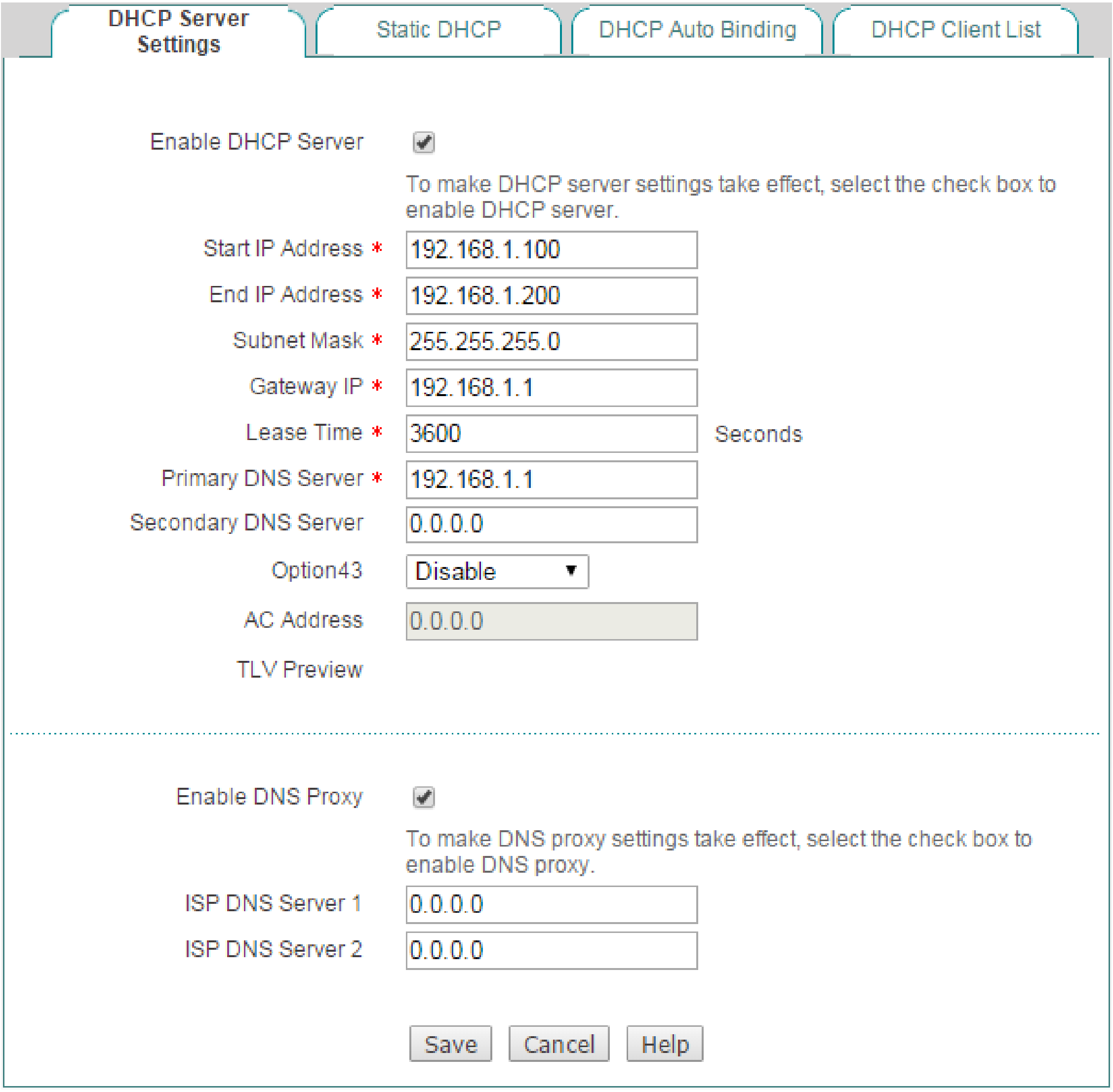
}

# 4.4 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP allows a host to be configured automatically, eliminating the need for intervention by a network administrator. The Device can act as a DHCP server to assign network addresses and deliver other TCP/IP configuration parameters (such as gateway IP address, DNS server IP address, etc.) to the LAN hosts.

## .4.1 DHCP Server Settings

The DHCP server assigns an IP address to a requesting client from a DHCP address pool, which also can be configured to provide other TCP/IP configuration parameters to the client, such as the DNS Server, gateway IP address, etc.



Enable DHCP Server ☑

To make DHCP server settings take effect, select the check box to enable DHCP server.

| | |
|---|---|
| Start IP Address * | 192.168.1.100 |
| End IP Address * | 192.168.1.200 |
| Subnet Mask * | 255.255.255.0 |
| Gateway IP * | 192.168.1.1 |
| Lease Time * | 3600 Seconds |
| Primary DNS Server * | 192.168.1.1 |
| Secondary DNS Server | 0.0.0.0 |
| Option43 | Disable ▼ |
| AC Address | 0.0.0.0 |
| TLV Preview | |

Enable DNS Proxy ☑

To make DNS proxy settings take effect, select the check box to enable DNS proxy.

| | |
|---|---|
| ISP DNS Server 1 | 0.0.0.0 |
| ISP DNS Server 2 | 0.0.0.0 |

**Figure 4-14 DHCP Server Settings**

}

- **Enable DHCP Server:** Select to enable DHCP server.

- **Start and End IP Address:** Specify the range of IP addresses assigned to DHCP clients. The range of IP addresses must be on the same subnet as the LAN interface of the Device, and cannot include the IP address of the LAN interface.

- **Subnet Mask:** The subnet mask address assigned by the DHCP server to the intranet computers automatically. This subnet mask must match the subnet mask of the LAN interface.

- **Gateway IP:** Specify the gateway IP address assigned by the DHCP server to the intranet computers automatically. This gateway IP address must match the gateway IP address of the LAN interface.

- **Lease Time:** The leasing time for the network computers to obtain the IP address assigned by the Device (Unit: Seconds).

- **Primary DNS Server:** The primary DNS server IP address assigned by the DHCP server to the Intranet computers automatically.

- **Secondary DNS Server:** The secondary DNS server IP address assigned by the DHCP server to the Intranet computers automatically.

- **Option 43:** By modifying the variable length fields of option 43 attribute in the DHCP protocol packets which is used to carry the IP address of AC, AP analyze the AC address carried by option 43 to discover AC. The available options are **Disable**, **HEX Length**, **ASCII Length**, and **Customized**.

- **AC Address:** The IP address of AC.

- **Enable DNS Proxy:** Select to enable DNS Proxy. When acting as a DNS proxy, the Device listens for incoming DNS requests on the LAN interface, relays the DNS requests to the current public network DNS servers, and replies as a DNS resolver to the requesting LAN hosts.

- **ISP DNS Server 1** or **ISP DNS Server 2:** Specify the IP address of ISP's DNS server that is available to a DHCP client.

⌖ **Note:**

1) If the DHCP Server is enabled, the LAN computer could obtain an IP address and other TCP/IP parameters from the Device's built-in DHCP server after setting the way of computer's getting IP address as "obtain an IP address automatically".

2) If the DNS proxy is enabled on the Device, in order to use DNS proxy service normally, you need set the LAN hosts' primary DNS server to the Device's LAN IP address. Note: If the DHCP server is also enabled on the Device, the Device will assign its LAN IP address as the primary DNS server address to the LAN hosts automatically.

}

3) To ensure that the DNS proxy works well, you should at least specify the primary DNS server provided by your ISP on the Device. It is obvious that you can specify the secondary DNS server provided by your ISP.

4) The Device can act as a DNS proxy server to all LAN users; this greatly simplifies the LAN hosts setup. For example, there is a LAN DNS proxy server on which a DNS proxy software is installed (e.g., Wingate), and the LAN users take this server's IP address as the primary DNS server address. Now, the Device will be used as a new gateway for the LAN hosts. In this case, in order to use DNS proxy service normally, the administrator only need change the Device's LAN IP address to the old proxy DNS server's IP address, and enable DNS proxy on the Device, without modify the LAN hosts' related settings.

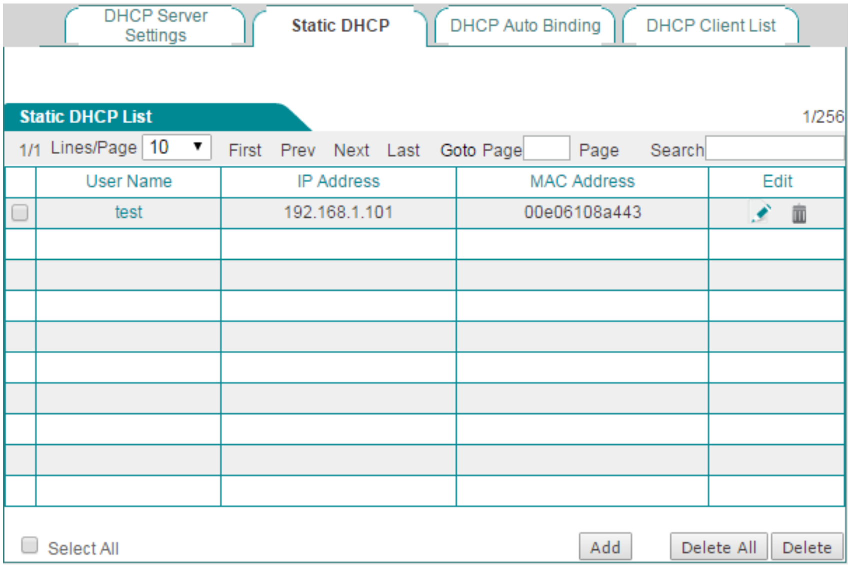
## .4.2 Static DHCP

This section describes the static DHCP list and the way to configure a static DHCP.

Using the DHCP Server to automatically configure TCP/IP properties for the LAN computers is very convenient, but it can cause a computer to be assigned with different IP address at different times. Some Intranet computers may need a fixed IP address; in this case, the static DHCP function is required, to bind the computer's MAC address with an IP address. As shown in Figure 4-15, when a computer with 00E06108A443 as MAC address requests the IP address from the DHCP server, the DHCP server will find a corresponding fixed IP address (192.168.1.101) based on its MAC address and assign it to the computer.

### 4.4.2.1 Static DHCP List

You can add, view, modify and delete static DHCP entries on the **Network > DHCP Server > Static DHCP** page.



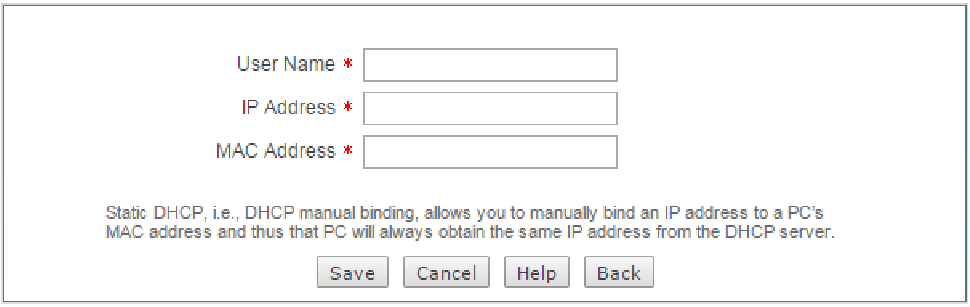
| | User Name | IP Address | MAC Address | Edit |
|---|---|---|---|---|
| □ | test | 192.168.1.101 | 00e06108a443 | ✎ 🗑 |

**Figure 4-15 Static DHCP List**

}

### 4.4.2.2 Static DHCP Settings

Click the **Add** button in the page as shown in Figure 4-15 to enter into the **Static DHCP Settings** page as shown below, and then configure it.



User Name *

IP Address *

MAC Address *

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

**Figure 4-16 Static DHCP settings**

- **User Name:** Specify a unique name for the static DHCP entry.
- **IP Address:** Specify the reserved IP address, which must be the valid IP address within the range of IP addresses assigned by the DHCP server.
- **MAC Address:** Specify the MAC address of the computer to use this reserved IP address in a fixed way.

**Note:**

1) After the setting is successful, the Device will assign the preset IP address for the specified computer in a fixed way.

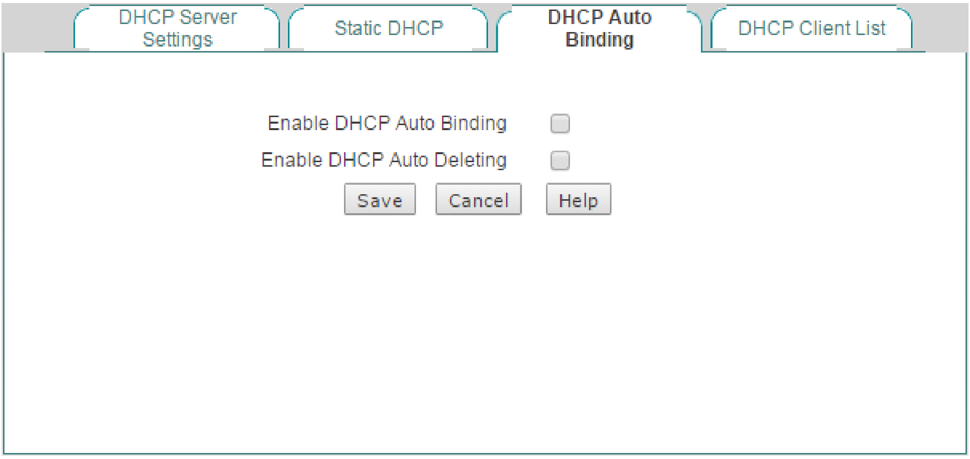
2) The assigned IP addresses must be within the range provided by the DHCP server.

## .4.3 DHCP Auto Binding

If the hosts change frequently on the local area network, it is very troublesome to configure static DHCP entries manually. And it will cause some users who can't access the Device and Internet. To deal with these issues, the Device provides DHCP auto binding feature.

Once the DHCP auto binding is enabled, the Device will immediately scan the LAN to detect active hosts connected to the Device, learn dynamic ARP information and bind the related valid IP and MAC address as a static DHCP entry.

}



Enable DHCP Auto Binding □

Enable DHCP Auto Deleting □

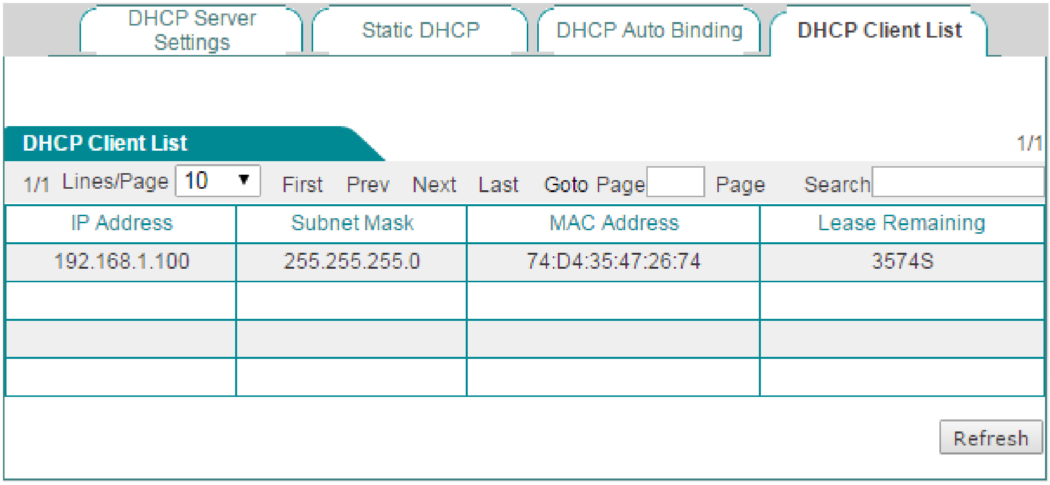
Figure 4-17 DHCP Auto Binding

- **Enable DHCP Auto Binding:** If selected, once a LAN host obtains an IP address from the Device that acts as a DHCP server, the Device will immediately bind the host's IP and MAC address as a static DHCP entry.

- **Enable DHCP Auto Deleting:** If selected, the Device will automatically delete the static DHCP entry when the corresponding host releases the IP address initiatively or its lease time expires.

## .4.4 DHCP Client List

When acting as a DHCP client, the Device can dynamically obtain an IP address and other TCP/IP configuration parameters from a DHCP server. The information of those DHCP clients who have obtained an IP address and other TCP/IP configuration parameters will be display in the **DHCP Client List**. Such as in the following figure, the DHCP server assigns the IP address of 192.168.1.100 in the address pool to the network computers whose MAC address is 74:D4:35:47:26:74, and the rest of the time for the computer to lease this IP address is 3,574 seconds.



| IP Address | Subnet Mask | MAC Address | Lease Remaining |
|---|---|---|---|
| 192.168.1.100 | 255.255.255.0 | 74:D4:35:47:26:74 | 3574S |
| | | | |
| | | | |
| | | | |

Figure 4-18 DHCP Client List

}

## .4.5 Example of DHCP

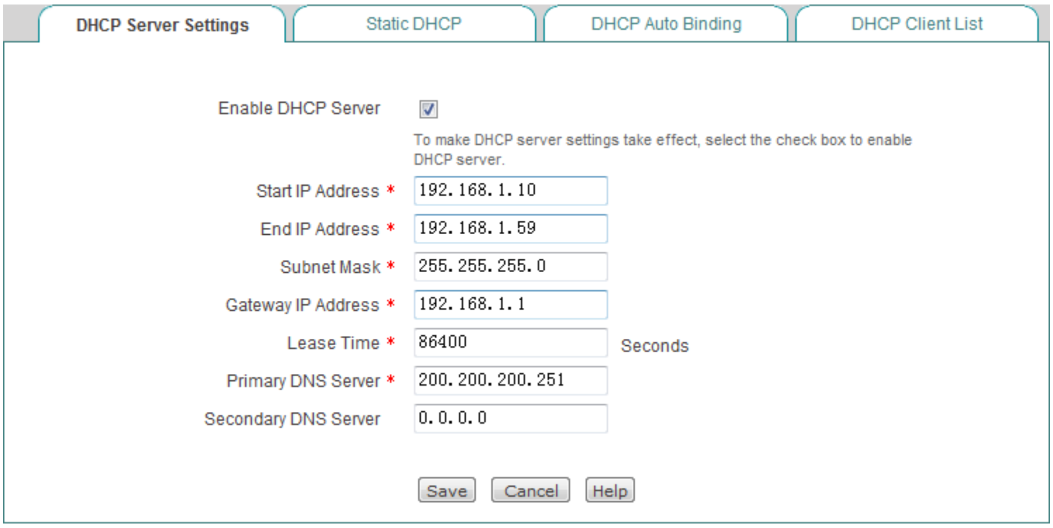
### 1) Requirements

In this case, the DHCP function must be enabled on the Device, with the start IP Address as 192.168.1.10, and a total of 50 addresses can be assigned; here, the host with the MAC address of 00:21:85:9B:45:46 assigns the fixed IP address of 192.168.1.15, and the host with the MAC address of 00:1F:3C:0F:07:F4 assigns the fixed IP address of 192.168.1.10.

### 2) Configuration Steps

**Step 1** Go to **Network > DHCP Server > DHCP Server Settings** page.

**Step 2** Select **Enable DHCP Server**, enter **192.168.1.10** and **192.168.1.59** in the **Start IP Address** and **End IP Address** textbox, configure other parameters as required, and click the **Save** button after the end of configuration.



Enable DHCP Server ☑

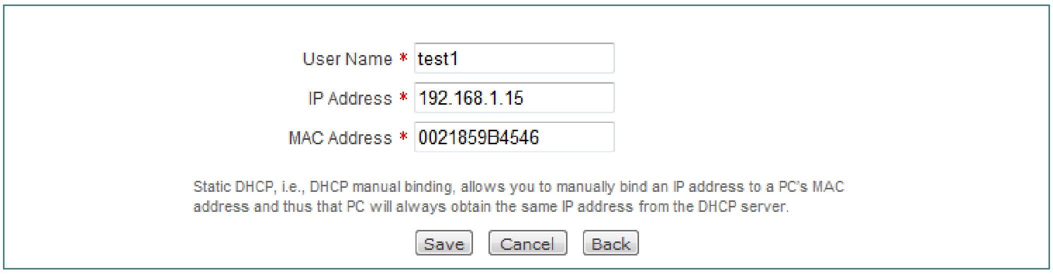
To make DHCP server settings take effect, select the check box to enable DHCP server.

| | | |
|---|---|---|
| Start IP Address * | 192. 168. 1. 10 | |
| End IP Address * | 192. 168. 1. 59 | |
| Subnet Mask * | 255. 255. 255. 0 | |
| Gateway IP Address * | 192. 168. 1. 1 | |
| Lease Time * | 86400 | Seconds |
| Primary DNS Server * | 200. 200. 200. 251 | |
| Secondary DNS Server | 0. 0. 0. 0 | |

**Figure 4-19 DHCP Server Settings_Example**

**Step 3** Go to **Network > DHCP Server > Static DHCP** page and click the **Add** button.

**Step 4** Configure the two static DHCP instances in the request, as shown the following two figures.

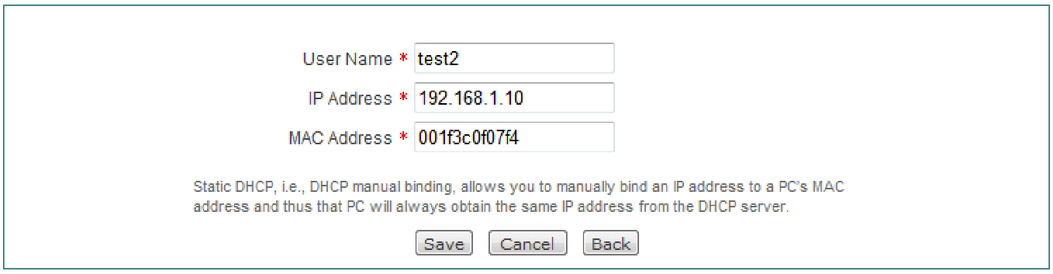


| | |
|---|---|
| User Name * | test1 |
| IP Address * | 192.168.1.15 |
| MAC Address * | 0021859B4546 |

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

**Figure 4-20 Static DHCP Settings_Example A**

}

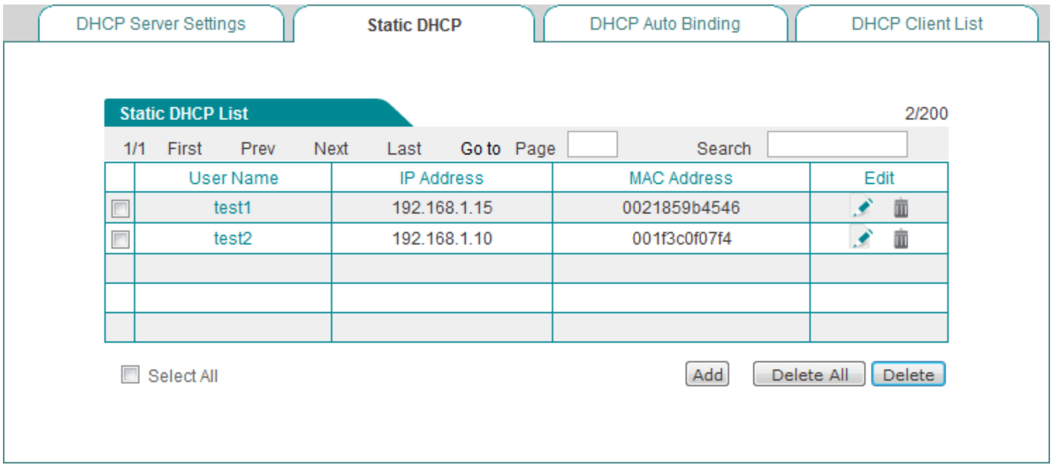


| | |
|---|---|
| User Name * | test2 |
| IP Address * | 192.168.1.10 |
| MAC Address * | 001f3c0f07f4 |

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

**Figure 4-21 Static DHCP Settings_Example B**

At this point, the configuration is complete, and you can view the information about 2 static DHCP entries in the **Static DHCP List**, as shown in the following figure.



| | User Name | IP Address | MAC Address | Edit |
|---|---|---|---|---|
| □ | test1 | 192.168.1.15 | 0021859b4546 | ✎ 🗑 |
| □ | test2 | 192.168.1.10 | 001f3c0f07f4 | ✎ 🗑 |
| | | | | |
| | | | | |
| | | | | |

**Figure 4-22 Static DHCP List_Example**

# 4.5 DDNS

Dynamic Domain Name Service (DDNS) is a service used to map a domain name which never changes to a dynamic IP address which may change quite often. For example, if you have applied PPPoE connection with dynamically assigned IP address from the ISP, you can use DDNS to allow the external computers to access the Device by a static domain name.

In order to use DDNS service, you need to register an account with a DDNS provider. Each DDNS provider offers its own specific network services. The DDNS service provider reserves the right to change, suspend or terminate your use of some or all network services at any time for any reason.

## .5.1 DDNS Service provided by no-ip.com

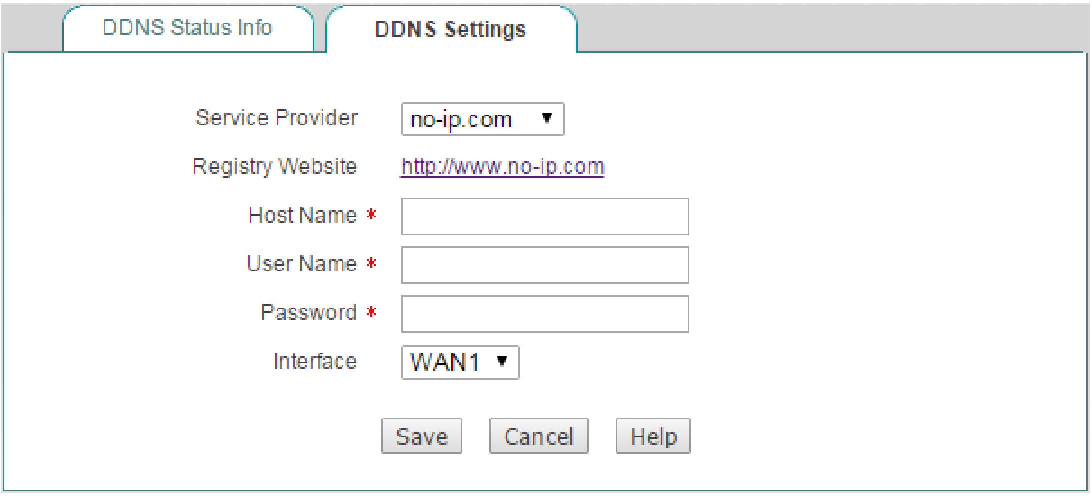
1) Register a Domain Name with no-ip.com

Please login to http://www.noip.com/ to register a domain name with the suffix of

}

no-ip.com.

2) DDNS Settings – no-ip.com



Service Provider: no-ip.com

Registry Website: http://www.no-ip.com

Host Name *

User Name *

Password *

Interface: WAN1

Figure 4-23 DDNS_no-ip.com

- **Service Provider:** Select the DDNS service provider who offers services to the Device. Here please select **no-ip.com**.
- **Host Name:** Specify the host name of the Device.
- **User Name:** Enter the user name of the account. It should be the same with the user name that you entered when registering the DDNS account.
- **Password:** Enter the key that you got when registering the DDNS account.

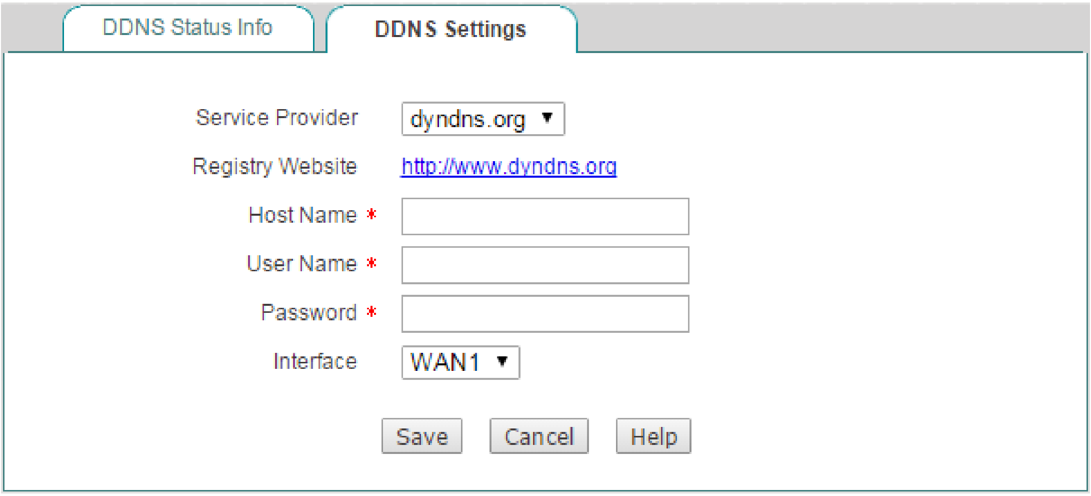
## .5.2 DDNS Service provided by dyndns.org

1) Register a Domain Name with no-ip.com

Please login to http://www.dyndns.org to register a domain name with the suffix of dyndns.org.

2) DDNS Settings –dyndns.org

}



Service Provider: dyndns.org

Registry Website: http://www.dyndns.org

Host Name *

User Name *

Password *

Interface: WAN1

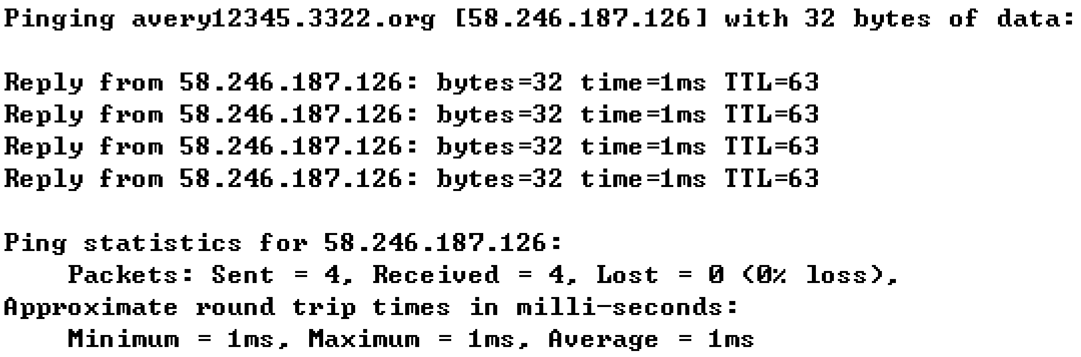
**Figure 4-24 DDNS_dyndns.org**

- **Service Provider:** Select the DDNS service provider who offers services to the Device. Here please select **dyndns.org**.
- **Host Name:** Specify the host name of the Device.
- **User Name:** Enter the user name of the account. It should be the same with the user name that you entered when registering the DDNS account.
- **Password:** Enter the key that you got when registering the DDNS account.

## .5.3 DDNS Verification

To verify whether DDNS is updated successfully, you can use the ping command at the command prompt on the PC (for example: **ping avery12345.3322.org**).

If the displayed page is similar to the screenshot below, the domain name is resolved to an IP address successfully (58.246.187.126 in this example), that is, DDNS is updated successfully.



```
Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:

Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63

Ping statistics for 58.246.187.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

**Note:**

}

1) If your ISP assigns a private IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x) instead of a public IP address to the Device, DDNS will not work.

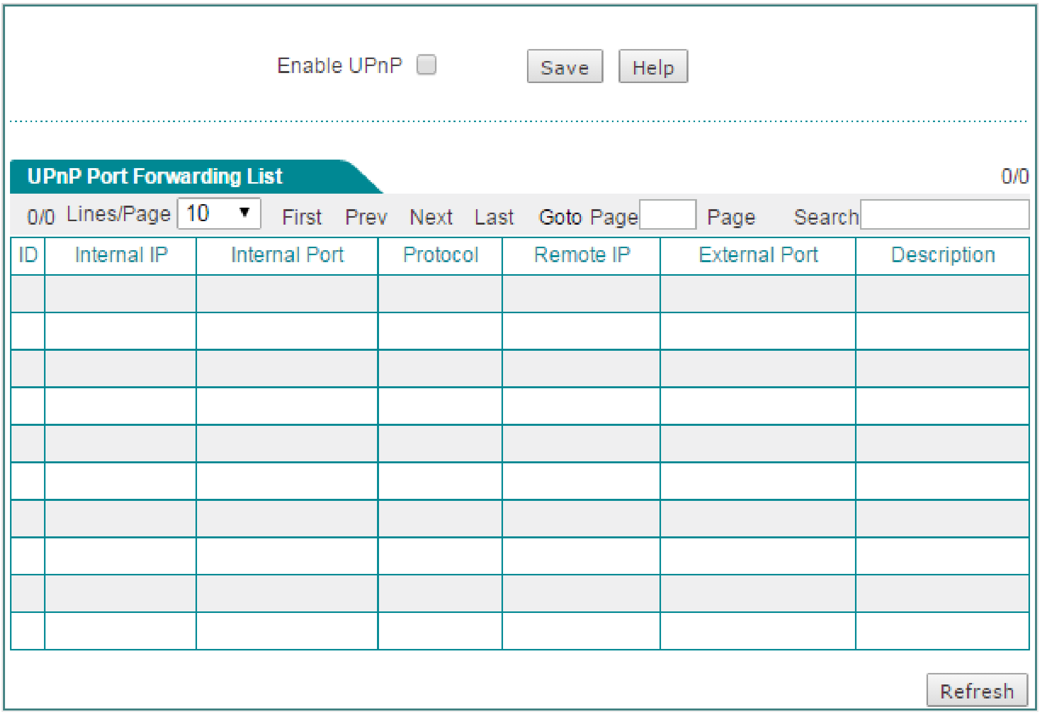
2) DDNS feature can help you implement VPN tunnels using dynamic IP addresses on the Device.

## 4.6 UpnP

The Universal Plug and Play (UPnP) is architecture that implements zero configuration networking, that is, it provides automatic IP configuration and dynamic discovery of the UPnP compatible devices from various vendors. An UPnP compatible device can dynamically join a network, obtain an IP address, announce its name, convey its capabilities upon request, and learn about the presence and capabilities of other devices on the network.

The Device can implement NAT traversal by enabling UPnP. When you enable UPnP, the Device allows any LAN UPnP-enabled device to perform a variety of actions, including retrieving the public IP address, enumerate existing port mappings, and add or remove port mappings. By adding a port mapping, an UPnP-enabled device opens the related service ports on the Device to allow the Internet hosts access. Windows Messenger is an example of an application that supports NAT traversal and UPnP.

The Device provides the **UPnP Port Forwarding List**, which lists all the port forwarding rules established using UPnP. You can view each port forwarding rule's detailed information in the list, which includes internal IP address, internal port, protocol, remote IP address, external port, and description.



Enable UPnP □

UPnP Port Forwarding List 0/0

0/0 Lines/Page 10

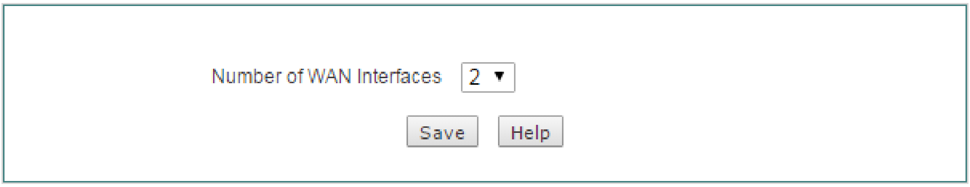
| ID | Internal IP | Internal Port | Protocol | Remote IP | External Port | Description |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Figure 4-25 UPnP

}

## 4.7 Number of WAN

On the **Network** > **Number of WAN** page, you can set the number of WAN interface. Select the number of WAN interface and click the **Save** button to save the settings.



Number of WAN Interfaces 2

**Figure 4-26 Number of WAN Settings**

**Note:**

1) After the number of WAN interface is changed, you need to restart the Device for the setting take effect.

2) After the Device restart, all customer settings will be reset to the factory default settings.

# Chapter 5. Advanced Menu

## 5.1 NAT&DMZ

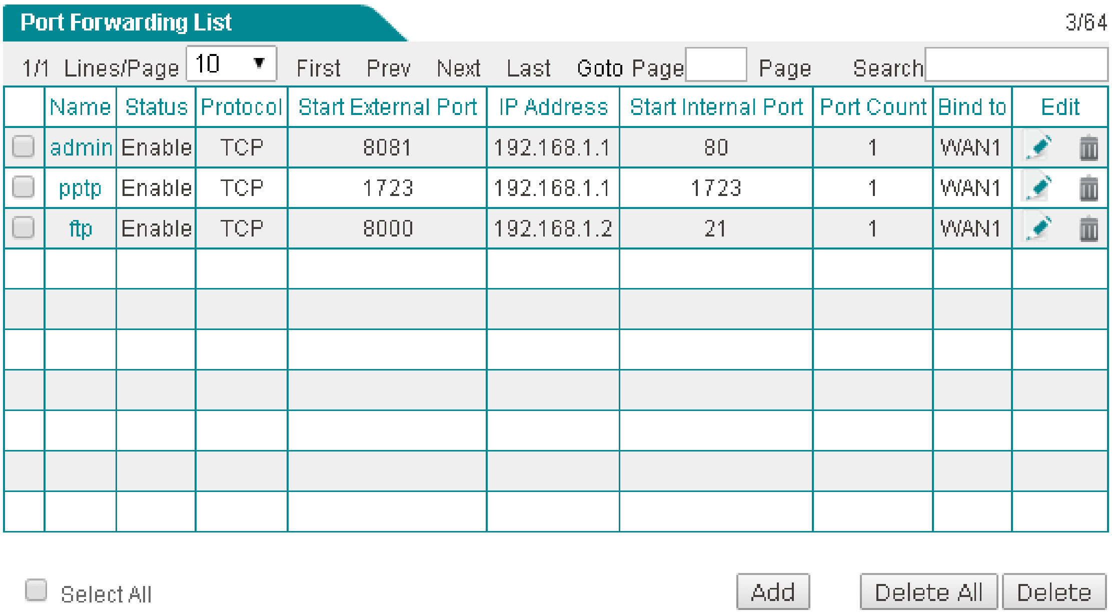
This chapter describes how to configure and use NAT features, including port forwarding, DMZ hosts, and NAT rule.

### 5.1.1.1 Port Forwarding

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your network, the Device can forward those requests to computers equipped to handle the requests. For example, if you set the port number 21 (ftp) to be forwarded to IP address 192.168.1.2, then all the related requests from outside users will be forwarded to 192.168.1.2.

### 5.1.1.2 Port Forwarding List

On the **Advanced** > **NAT & DMZ > Port Forwarding** page, you can setup some port forwarding rules.



Port Forwarding List 3/64

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | Name | Status | Protocol | Start External Port | IP Address | Start Internal Port | Port Count | Bind to | Edit |
|---|---|---|---|---|---|---|---|---|---|
| □ | admin | Enable | TCP | 8081 | 192.168.1.1 | 80 | 1 | WAN1 | ✎ 🗑 |
| □ | pptp | Enable | TCP | 1723 | 192.168.1.1 | 1723 | 1 | WAN1 | ✎ 🗑 |
| □ | ftp | Enable | TCP | 8000 | 192.168.1.2 | 21 | 1 | WAN1 | ✎ 🗑 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

□ Select All

**Figure 5-1 Port Forwarding List**

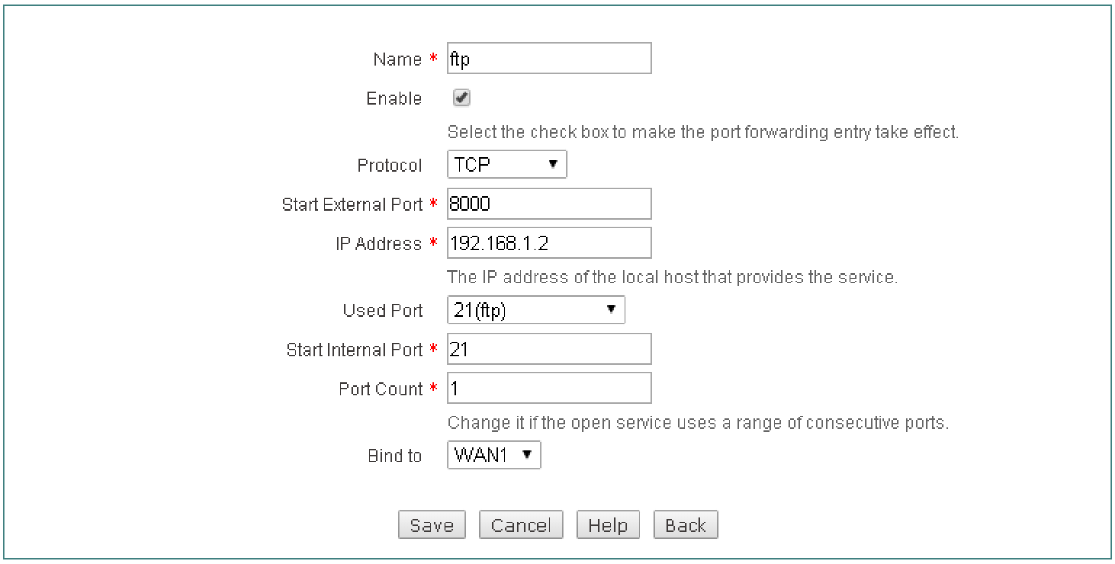
- Add a Port Forwarding Rule: Click the **Add** button, then setup it, lastly click the **Save** button.

}

- Edit a Port Forwarding Rule: Click the **Name** or **Edit** hyperlink of this rule entry, the related information will display in the setup fields. Then modify it, and click the **Save** button.

- Delete Port Forwarding Rule(s): Select the leftmost check boxes of entries, and then click the **Delete** button.

### 5.1.1.3 Port Forwarding settings



| | |
|---|---|
| Name * | ftp |
| Enable | ☑ |
| | Select the check box to make the port forwarding entry take effect. |
| Protocol | TCP ▼ |
| Start External Port * | 8000 |
| IP Address * | 192.168.1.2 |
| | The IP address of the local host that provides the service. |
| Used Port | 21(ftp) ▼ |
| Start Internal Port * | 21 |
| Port Count * | 1 |
| | Change it if the open service uses a range of consecutive ports. |
| Bind to | WAN1 ▼ |

**Figure 5-2 Port Forwarding Setup**

- **Name:** Specify a name of this entry. It should be between 1 and 11 characters long.

- **Enable:** Select to enable this Port Forwarding entry.

- **Protocol:** Select the transport protocol used by the service, available options are TCP, UDP and TCP/UDP.

- **Start External Port:** Specify the lowest port number provided by the Device. The external ports are opened for outside users to access.

- **IP Address:** Specify the IP address of the local server that you want outside users to access.

- **Start Internal Port:** Specify the lowest port number of the service provided by the LAN host. The **Start External Port** and **Start Internal Port** can be different.

- **Port Count:** Specify the number of ports used by the service. If the service uses only one port number, enter 1. For example, if the start internal port is 21, the start external port is 2001 and the port count is 10, then the internal port range is from 21 to 30, and the external port range is from 2001 to 2010.

}

- **Bind to:** Select the NAT rule to which this port forwarding rule is bound. The port forwarding rule will use the WAN interface's IP address as the external IP address.

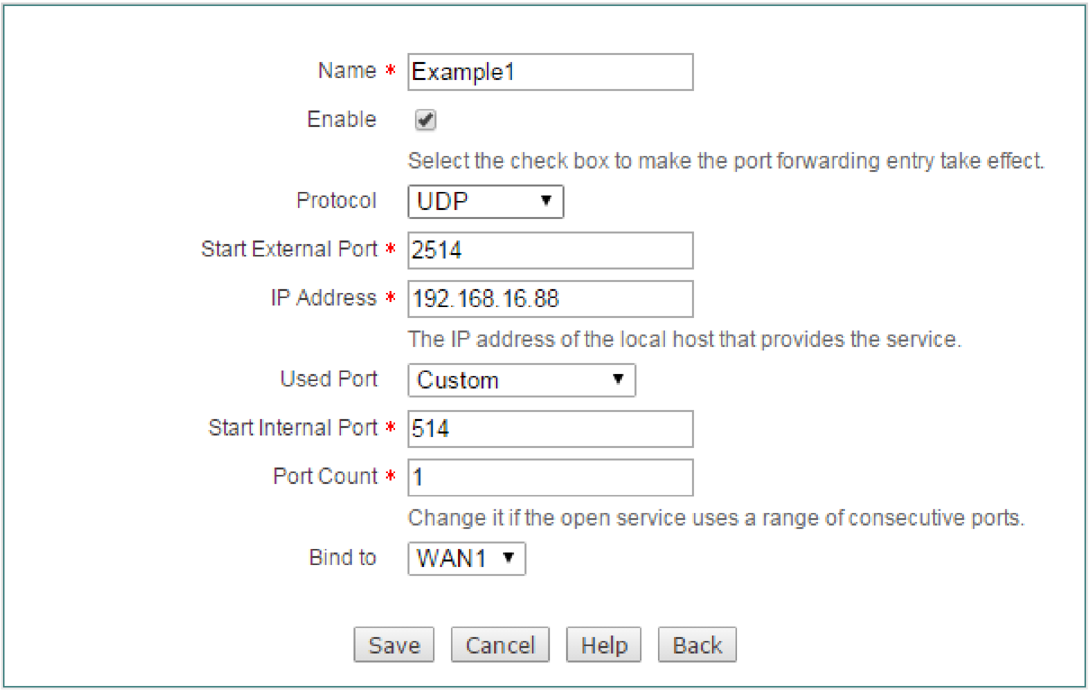
**Note:** The system will automatically create some port forwarding rules. You cannot modify or delete them.

## 5.1.1.4 Examples of Port Forwarding

### 5.1.1.4.1 Example One

An organization wants a LAN server (IP Address: 192.168.16.88) to open syslog service (Protocol: UDP; Port: 514) to the outside users. And the Device will use 2514 as the external port and the WAN1 IP address (200.200.200.88 in this example) as the external IP address. Then all the requests for syslog from outside users to 200.200.200.88:2514 will be forwarded to 192.168.16.88:514.

The following figure shows the detailed settings.



Name * Example1

Enable ☑

Select the check box to make the port forwarding entry take effect.

Protocol UDP ▼

Start External Port * 2514

IP Address * 192.168.16.88

The IP address of the local host that provides the service.

Used Port Custom ▼

Start Internal Port * 514

Port Count * 1

Change it if the open service uses a range of consecutive ports.

Bind to WAN1 ▼

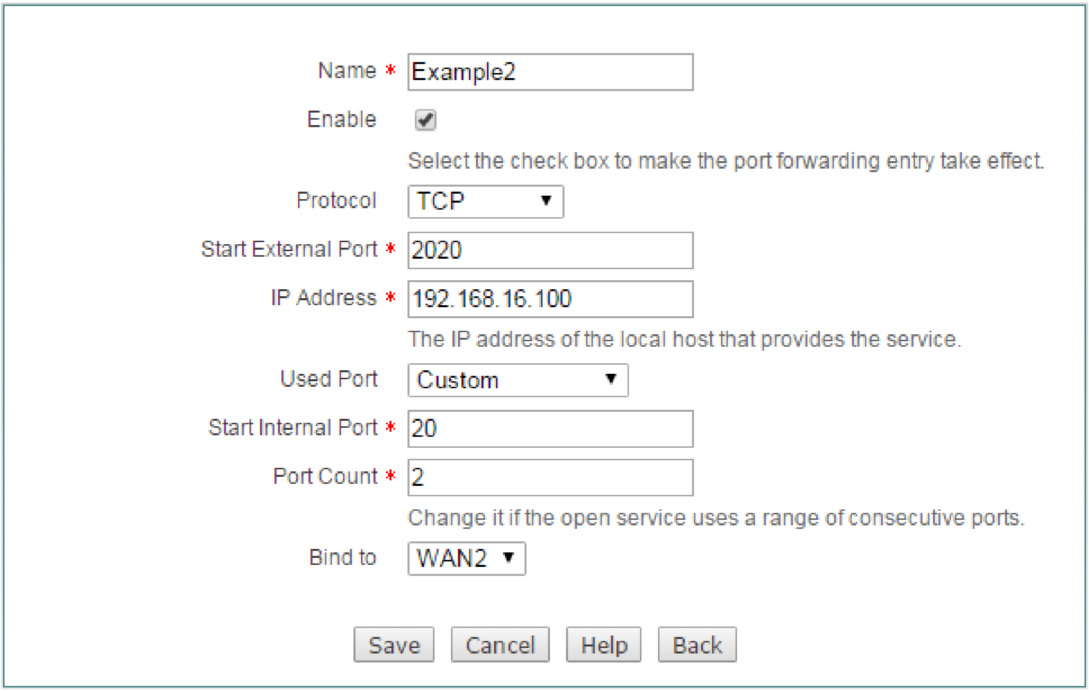
**Figure 5-3 Port Forwarding settings - Example One**

### 5.1.1.4.2 Example Two

An organization wants a LAN server (IP Address: 192.168.16.100) to open ftp service (Protocol: TCP; Port: 20, 21) to the outside users. And the Device will use 2020 and 2021 as the external ports and the WAN2 IP address (200.200.201.18 in this example) as the external IP address. As the ftp service uses two ports, so we need set the **Port Count** to 2. Then all the requests for ftp from outside users to 200.200.201.18:2020 or 200.200.201.18:2021 will be forwarded to 192.168.16.100:20 or 192.168.16.100:21.

}

The following figure shows the detailed settings.



|  |  |
|---|---|
| Name * | Example2 |
| Enable | ☑ |
|  | Select the check box to make the port forwarding entry take effect. |
| Protocol | TCP |
| Start External Port * | 2020 |
| IP Address * | 192.168.16.100 |
|  | The IP address of the local host that provides the service. |
| Used Port | Custom |
| Start Internal Port * | 20 |
| Port Count * | 2 |
|  | Change it if the open service uses a range of consecutive ports. |
| Bind to | WAN2 |

**Figure 5-4 Port Forwarding Settings - Example Two**

### 5.1.1.4.3 Example Three

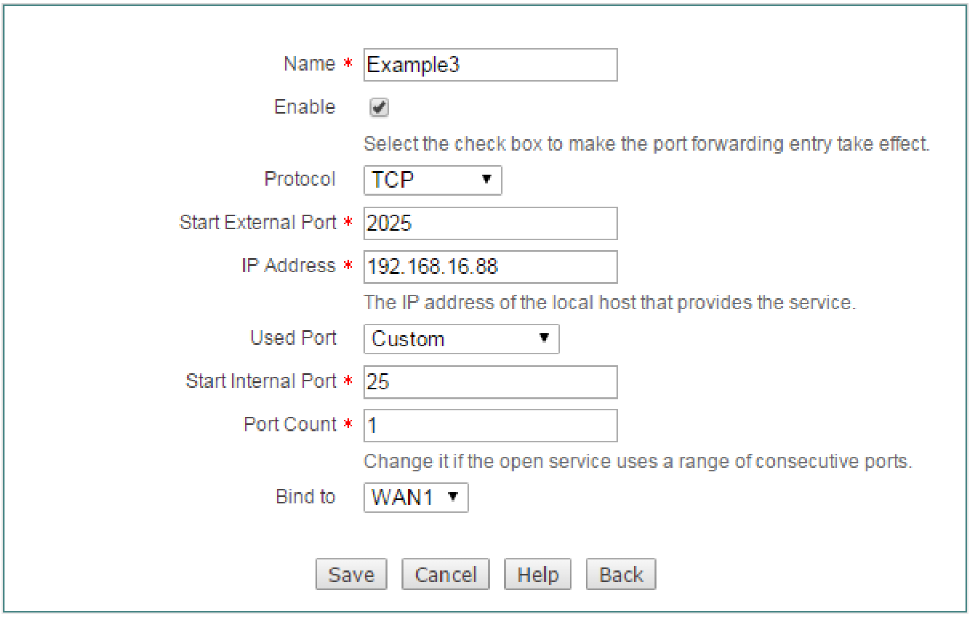
An organization obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29) from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection’s gateway IP address, 218.1.21.2/29 is used as the Device’s WAN1 interface’s IP address.

The organization wants a LAN server (IP Address: 192.168.16.88) to open SMTP service (Protocol: TCP; Port: 25) to the outside users. And the Device will use 2025 as the external port and 218.1.21.3 as the external IP address.

Firstly, we need to create a NAT rule, and set its **External IP Address** to 218.1.21.3, see section 7.1.2 NAT Rule for detailed information. Then we need to create the port forwarding rule.

The following figure shows the detailed settings.

}



Name * Example3

Enable ☑

Select the check box to make the port forwarding entry take effect.

Protocol TCP

Start External Port * 2025

IP Address * 192.168.16.88

The IP address of the local host that provides the service.

Used Port Custom

Start Internal Port * 25

Port Count * 1

Change it if the open service uses a range of consecutive ports.

Bind to WAN1

**Figure 5-5 Port Forwarding Settings - Example Three**

## 5.1.1.5 NAT Rule

## 5.1.1.6 Introduction to NAT

The NAT (Network Address Translation) is an Internet standard that is used to map one IP address space (i.e., Intranet) to another IP address space (i.e., Internet). The NAT is designed to alleviate the shortage of IP addresses, that is, it allows all the LAN hosts to share a single or a small group of IP addresses: On the Internet, there is only a single device using a single or a small group of public IP addresses; but the LAN hosts can use any range of private IP addresses, and these IP addresses are not visible from the Internet. As the internal network can be effectively isolated from the outside world, the NAT can also provide the benefit of network security assurance.

The Device provides flexible NAT features, and the following sections will describe them in detail.**NAT Address Space Definitions**

To ensure that NAT operates properly, the Device uses and maintains two address spaces:

- **Internal IP address:** It indicates the IP address that is assigned to a LAN host by the administrator. It is usually a private IP address.

- **External IP address:** It indicates the IP address that is assigned to the Device's Internet connection by the ISP. It is a legal public IP address that can represent one or more internal IP addresses to the outside world.

}

### 5.1.1.8 NAT Types

The Device provides two types of NAT: **One2One** and **EasyIP**.

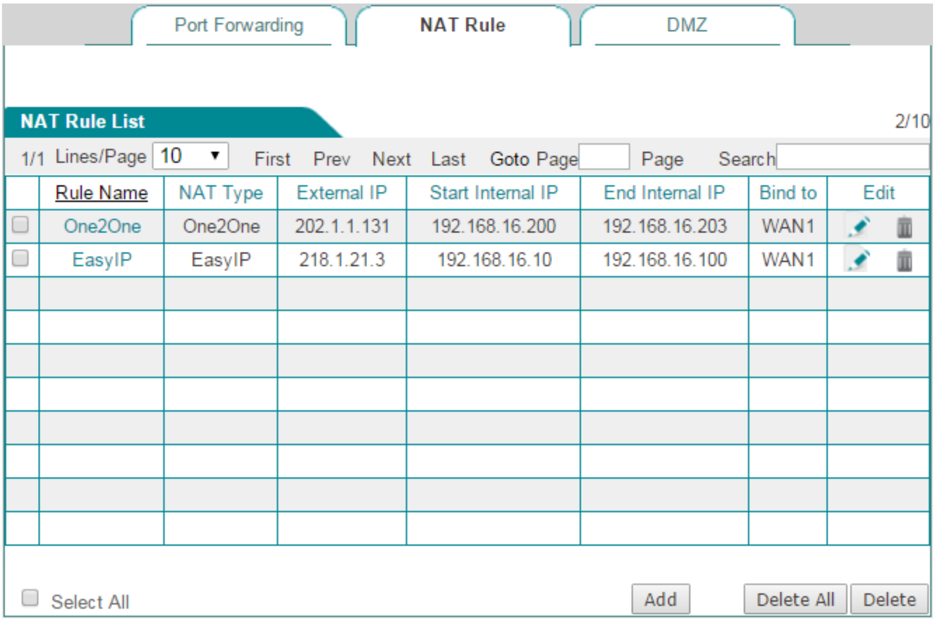
**One2One (One to One):** It indicates static network address translation. It is always referred to as Basic NAT, which provides a one to one mapping between an internal and an external IP address. In this type of NAT, IP address need be changed, but port needn't.

One to One NAT can be used to allow the outside users to access a LAN server: In the local network, the LAN server still use the private IP address, which is provided to the LAN hosts to access; and on the Internet, the Device will assign an external IP address to the local server, then the outside users can using this external IP address to access the server through the Device.

**EasyIP:** It indicates network address and port translation (NAPT). Since it is the most common type of NAT, it is often simply referred to as NAT. NAPT provides many-to-one mappings between multiple internal IP addresses and a single external IP addresses, that is, these multiple internal IP addresses will be translated to the same external IP address. In this type of NAT, to avoid ambiguity in the handling of returned packets, it must dynamically assign a TCP/UDP port to an outgoing session and change the packets' source port to the assigned port before forwarding them. Besides, the Device must maintain a translation table so that return packets can be correctly translated back.

When you obtain multiple public IP addresses from your ISP, you can create more than one NAT rule for each type of NAT. In actual network environment, different types of NAT rules are often used together.

### 5.1.1.9 NAT Rule List



| | Rule Name | NAT Type | External IP | Start Internal IP | End Internal IP | Bind to | Edit |
|---|---|---|---|---|---|---|---|
| □ | One2One | One2One | 202.1.1.131 | 192.168.16.200 | 192.168.16.203 | WAN1 | ✎ 🗑 |
| □ | EasyIP | EasyIP | 218.1.21.3 | 192.168.16.10 | 192.168.16.100 | WAN1 | ✎ 🗑 |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Figure 5-6 NAT Rule list**

}

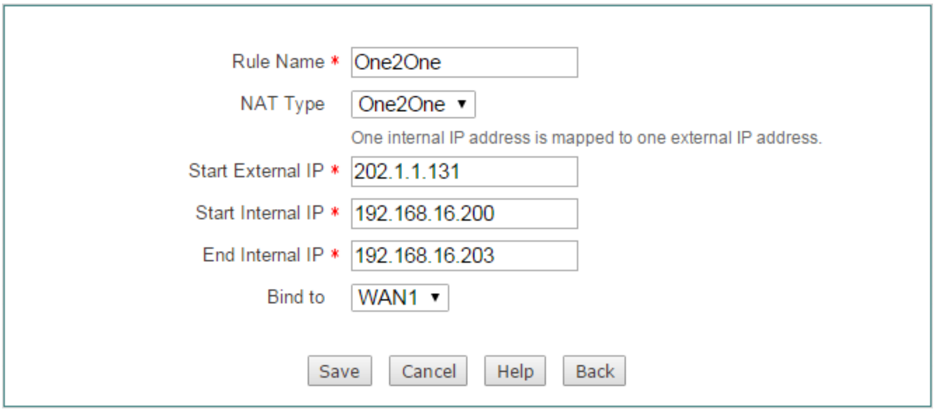
- **Add a NAT Rule:** Click the **Add** button to go to the setup page, and then configure it, lastly click the **Save** button.

- **Edit a NAT Rule:** Click its **Edit** button, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete NAT Rule(s):** Select the leftmost check boxes of them, and then click the **Delete** button.

## 5.1.1.10 NAT Rule settings

### 5.1.1.10.1 One2One settings



Rule Name * One2One

NAT Type One2One ▼

One internal IP address is mapped to one external IP address.

Start External IP * 202.1.1.131

Start Internal IP * 192.168.16.200

End Internal IP * 192.168.16.203

Bind to WAN1 ▼

**Figure 5-7 One2One settings**

- **Rule Name:** Specify the name of this NAT rule entry.

- **NAT Type:** Specify the type of the NAT rule. Here please select **One2One**.

- **Start External IP:** Specify the start external IP address to which the start internal IP address is mapped.

- **Start Internal IP** and **End Internal IP:** Specify the internal address range of the NAT rule. The LAN hosts that belong to this address range will use the NAT rule.

- **Bind to:** Specify an Internet connection to which the NAT rule is bound. The LAN hosts that match the NAT rule will access the Internet through this Internet connection.

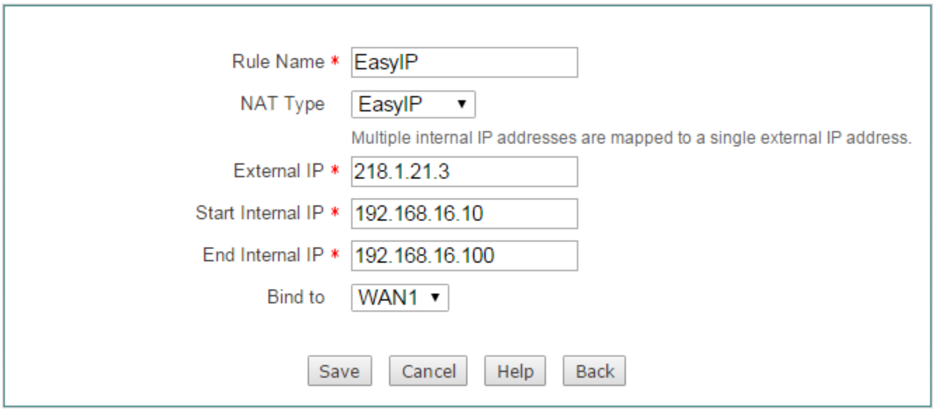
**Note:**

1) When creating a **One2One** NAT rule, you should set the **Start External IP Address**, and the number of the external IP addresses is the same with the number of internal IP addresses, which is determined by the **Start Internal IP Address** and **End Internal IP Address**. For example, if the **Start Internal IP Address** is 192.168.16.6, **End Internal IP Address** is 192.168.16.8, and **Start External IP Address** is 200.200.200.116, then 192.168.16.6, 192.168.16.7, and 192.168.16.8 will be mapped to 200.200.200.116, 200.200.200.117, and

}

200.200.200.118 respectively.

### 5.1.1.10.2 EasyIP settings



Rule Name * EasyIP

NAT Type EasyIP ▾

Multiple internal IP addresses are mapped to a single external IP address.

External IP * 218.1.21.3

Start Internal IP * 192.168.16.10

End Internal IP * 192.168.16.100

Bind to WAN1 ▾

**Figure 5-8 EasyIP settings**

- **Rule Name:** Specify the name of this NAT rule entry.
- **NAT Type:** Specify the type of the NAT rule. Here please select **EasyIP**.
- **External IP:** Specify the external IP address to which the LAN hosts' IP addressed are mapped. A system reserved NAT rule's external IP address is **0.0.0.0**, which means that the rule will use the related WAN interface's IP address as its external IP address; and it is non-editable. A user-defined NAT rule's external IP address can be neither 0.0.0.0 nor the WAN interface's IP address, that is, you can only use the other public IP addresses provided by your ISP as its external IP addresses.
- **Start Internal IP** and **End Internal IP:** Specify the internal address range of the NAT rule. The LAN hosts that belong to this address range will preferential use the NAT rule.
- **Bind to:** Specify an Internet connection to which the NAT rule is bound. The LAN hosts that match the NAT rule will access the Internet through this Internet connection.

## 5.1.1.11 Examples for NAT Rule

### 5.1.1.11.1 Example for Configuring One2One NAT Rule

#### 1) Requirements

In this example, a business has a single static IP Internet connection, and obtains eight public IP addresses (from 202.1.1.128/29 to 202.1.1.1.135/29) from the ISP. Therein, 202.1.1.129/29 is used as the Internet connection's gateway IP address, 202.1.1.130/2 is used as the Device's WAN1 interface's IP address. Note that 202.1.1.128/29 and 202.1.1.1.135/29 cannot be used as they are the subnet number and broadcast address respectively.

}

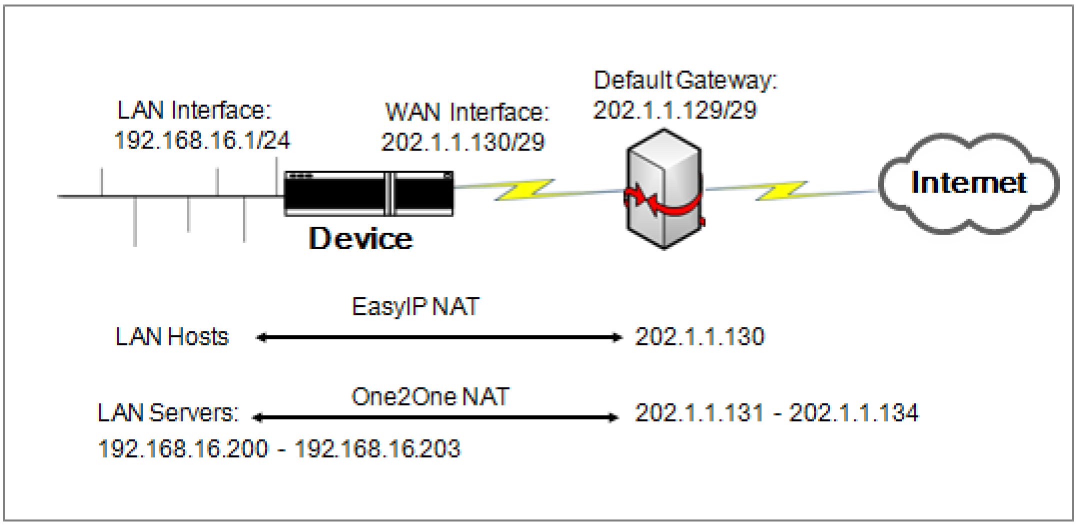


**Figure 5-9 Network Topology for One2One NAT Rule Configuration Example**

The business employees will share a single public IP address of 202.1.1.130/29 to access the Internet. The LAN's subnet number is 192.168.16.0, and subnet mask is 255.255.255.0. And the business want to use the remaining four public IP addresses (from 202.1.1.131/29 to 202.1.1.134/29) to create a **One2One** rule for the four local servers, then the outside users can use these public addresses to access the local servers through the Device. The four local servers IP addresses are from 192.168.16.200/24 to 192.168.16.203/24, which are mapped to 202.1.1.131/29, 202.1.1.132/29, 202.1.1.133/29, 202.1.1.134/29 respectively.

### 2) Analysis

Firstly we need configure a static IP Internet connection on the WAN1 interface in the **Basic > WAN** page or through the **Setup Wizard**. After you have configured the Internet connection, the Device will automatically create a related system reserved NAT rule, and also enable NAT.

Secondly, we need to create a One2One NAT rule for the four local servers. After you have configured this rule, the Device will automatically create the related static route.

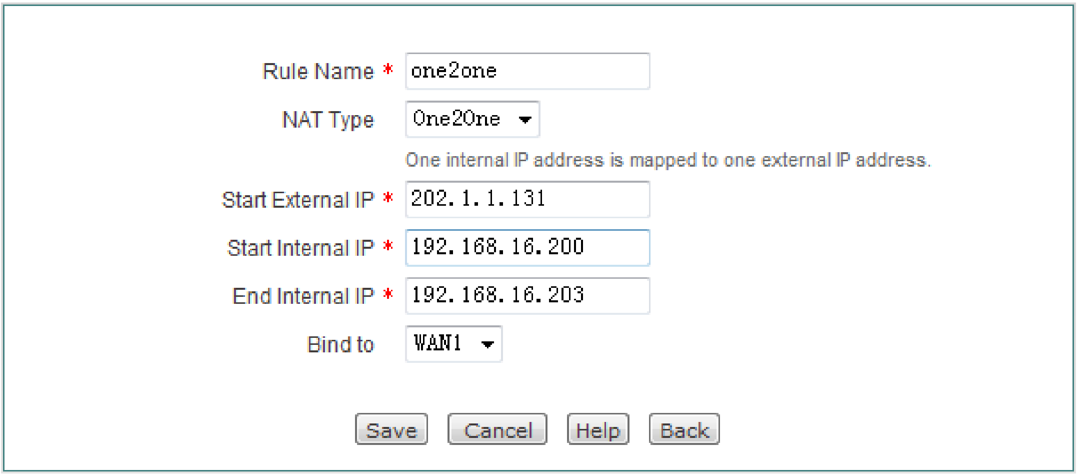
### 3) Configuration Procedure

The configuration steps are as following:

**Step 1** Go to the **Advanced > NAT & DMZ > NAT Rule** page, and click the **Add** button to go to the setup page.

**Step 2** Enter the name of this NAT rule entry in the **Rule name** text box and select **One2One** from the **NAT Type** drop-down list, see the following figure.

}



| | |
|---|---|
| Rule Name * | one2one |
| NAT Type | One2One |
| | One internal IP address is mapped to one external IP address. |
| Start External IP * | 202.1.1.131 |
| Start Internal IP * | 192.168.16.200 |
| End Internal IP * | 192.168.16.203 |
| Bind to | WAN1 |

Figure 5-10 One2One NAT Rule Settings - Example

**Step 3** Enter **202.1.1.131** in the **Start External IP** text box, enter **192.168.16.200** in the **Start Internal IP** text box, and enter **192.168.16.203** in the **End Internal IP** text box.

**Step 4** Select **WAN1** from the **Bind to** drop-down list.

**Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and then you can view its related configuration in the **NAT Rule List**.

## 5.1.1.11.2 Example for Configuring EasyIP NAT Rule

### (1) Requirements

In this example, an Internet cafe has a single Internet connection, and obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29) from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection's gateway IP address, 218.1.21.2/29 is used as the Device's WAN1 interface's IP address. Note that 218.1.21.0/29 and 218.1.21.7/29 cannot be used as they are the subnet number and broadcast address respectively.

The administrator want the hosts in the online game area (its address range is from 192.168.16.10/24 to 192.168.16.100/24) to use 218.1.21.3/29 to access the Internet. To achieve this purpose, he should create an **EasyIP** NAT rule for them. The rule's **External IP Address** is 218.1.21.3, **Start Internal IP** is 192.168.16.10, **End Internal IP** is 192.168.16.100, and **Bind to** is WAN1.

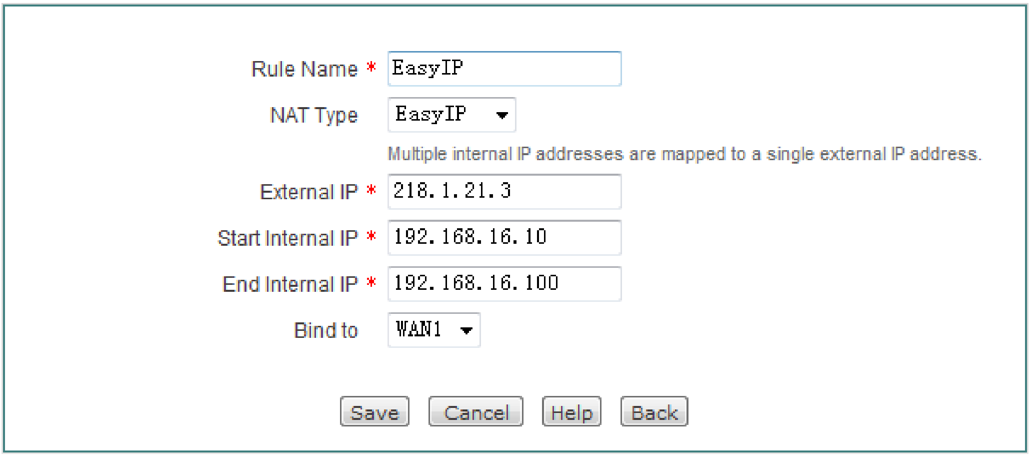
### (2) Configuration Procedure

The configuration steps are as following:

**Step 1** Go to the **Advanced > NAT & DMZ > NAT Rule** page, and click the **Add** button to go to the setup page.

**Step 2** Enter the name of this NAT rule entry in the **Rule name** text box and select **EasyIP** from the **NAT Type** drop-down list, see the following figure.

}



|  |  |
|---|---|
| Rule Name * | EasyIP |
| NAT Type | EasyIP |
|  | Multiple internal IP addresses are mapped to a single external IP address. |
| External IP * | 218.1.21.3 |
| Start Internal IP * | 192.168.16.10 |
| End Internal IP * | 192.168.16.100 |
| Bind to | WAN1 |

**Figure 5-11 EasyIP NAT Rule Settings - Example**

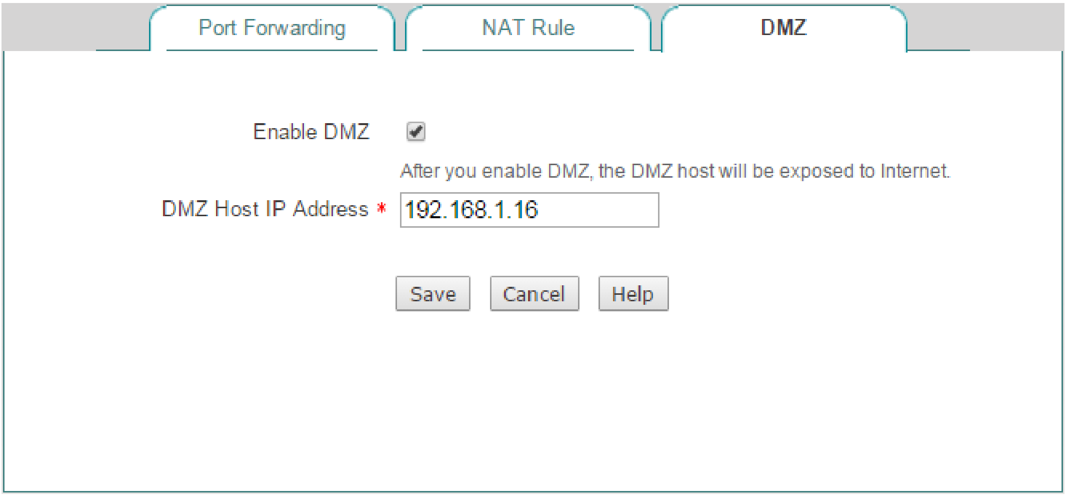
**Step 3** Enter **218.1.21.3** in the **External IP** text box, enter **192.168.16.10** in the **Start Internal IP** text box, and enter **192.168.16.100** in the **End Internal IP** text box.

**Step 4** Select **WAN1** from the **Bind to** drop-down list.

**Step 5** Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and then you can view its configuration in the **NAT Rule List**.

## 5.1.1.12 DMZ

The DMZ (Demilitarized Zone) feature allows one local computer to be exposed to the Internet for the use of a special service such as online game or video conferencing. When receiving the requests initiated from outside users, the Device will directly forward these requests to the specified DMZ host.



|  |  |
|---|---|
| Enable DMZ | ☑ |
|  | After you enable DMZ, the DMZ host will be exposed to Internet. |
| DMZ Host IP Address * | 192.168.1.16 |

**Figure 5-12 DMZ**

- **Enable DMZ:** Select to enable DMZ Host.

}

- **DMZ Host IP Address:** Specify the private IP address of the DMZ host.

⌖ **Note:**

The computer designated as the DMZ host will lose firewall protection provided by the Device. As the DMZ host is exposed to many exploits from the Internet, it may be used to attack your network.

### 5.1.1.13 Priorities for Port Forwarding and DMZ Host

The port forwarding has higher priority than the DMZ host. When receiving a request packet initiated from an outside user, the Device will firstly search the **Port Forwarding List** to find out if there is a port forwarding rule matching the destination IP address and port of the packet. If a match is found, the Device will forward the packet to the mapped local host. Else, the Device will try to find out if there is an available DMZ host.

## 5.2 Static Route

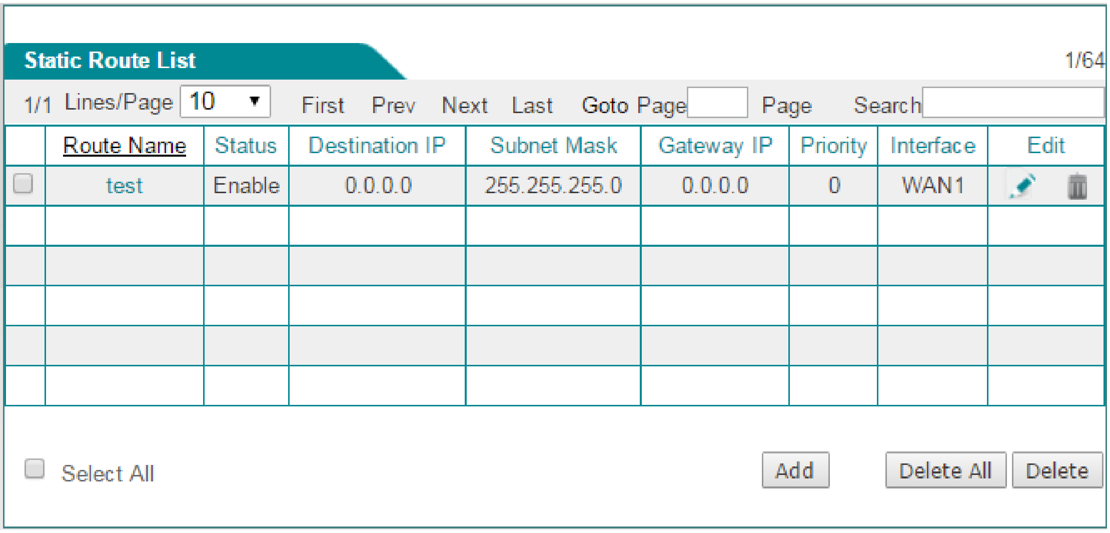
A static route is manually configured by the network administrator, which is stored in a routing table. By using routing table, the Device can select an optimal transmission path for each received packet, and forward the packet to the destination site effectively. The proper usage of static routes can not only improve the network performance, but also achieve other benefits, such as traffic control, provide a secure network environment.

The disadvantage of using static routes is that they cannot dynamically adapt to the current operational state of the network. When there is a change in the network or a failure occurs, some static routes will be unreachable. In this case, the network administrator should update the static routes manually.

### 5.2.1.1 Static Route List

All static routes you have configured will be displayed in the **Static Route List** (see the following figure).

}



Static Route List
1/64
1/1 Lines/Page 10 ▾ First Prev Next Last Goto Page Page Search

| | Route Name | Status | Destination IP | Subnet Mask | Gateway IP | Priority | Interface | Edit |
|---|---|---|---|---|---|---|---|---|
| □ | test | Enable | 0.0.0.0 | 255.255.255.0 | 0.0.0.0 | 0 | WAN1 | ✎ 🗑 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

□ Select All
Add
Delete All
Delete

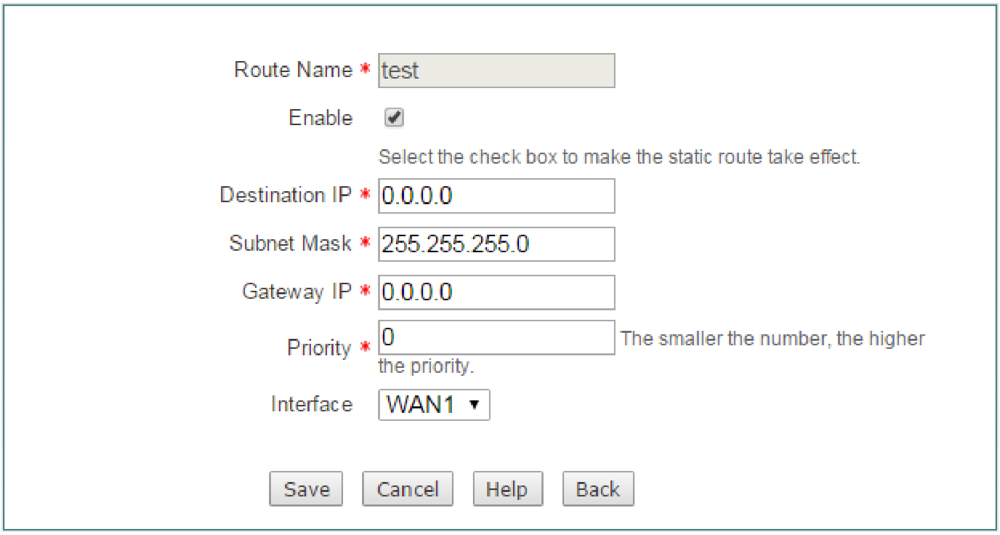
Figure 5-13 Static Route List

- **Add Static Route:** Click the **Add** button, then setup it, lastly click the **Save** button.

- **Edit Static Route: C**lick its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete Static Route(s):** Select the leftmost check boxes of them, and then click the **Delete** button.

## 5.2.1.2 Static Route settings



Route Name * test

Enable ☑

Select the check box to make the static route take effect.

Destination IP * 0.0.0.0

Subnet Mask * 255.255.255.0

Gateway IP * 0.0.0.0

Priority * 0 The smaller the number, the higher the priority.

Interface WAN1 ▾

Figure 5-14 Static Route setting

- **Route Name:** Specify the name of this static route entry.

- **Enable:** Select to enable this static route entry.

}

- **Destination IP:** Specify the IP address of the destination network or host.

- **Subnet Mask:** Specify the subnet mask of the destination network or host.

- **Gateway IP Address:** Specify the IP address of the next hop router to which to forward the packets.

- **Priority:** Specify the priority of the static route. If there are multiple routes to the same destination with different priorities, the Device will choose the route with the highest priority to forward the packets. The smaller the number, the higher the priority.

- **Interface**: Specify the outbound interface through which the packets are forwarded to the next hop gateway or router. The available options are the name of each physical interface.

⌖ **Note:**

1) When creating a static route, you should specify the next hop IP address by the **Gateway IP Address** or **Interface**.

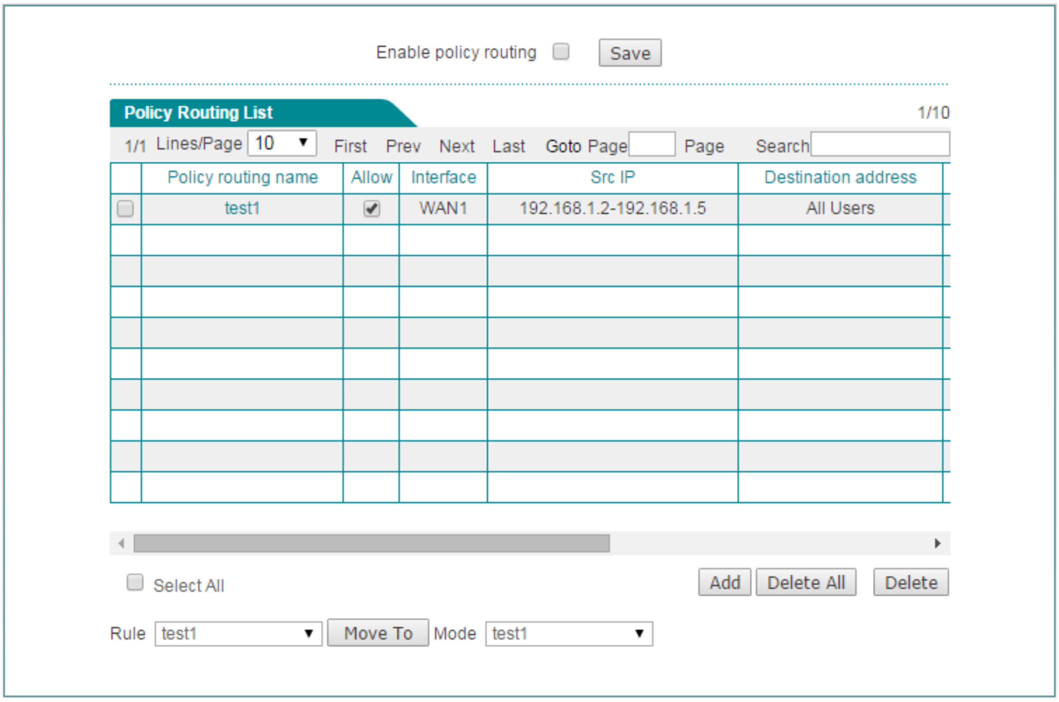
2) In most cases, please don't modify the system reserved static route (e.g., Default, Detect) to avoid surfing the Internet abnormally.

## 5.3 Policy Routing

This section describes the **Advanced > Policy Routing** page.

Policy Routing provides a tool for forwarding and routing data packets based on the user-defined policies. Different from the traditional destination-based routing mechanism, Policy Routing enables you to use policies based on source and destination address, protocol, port, schedule, and other criteria to route packets flexibly.

### 5.3.1.1 Policy Routing List



Enable policy routing □ Save

Policy Routing List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page ☐ Page Search ☐

|  | Policy routing name | Allow | Interface | Src IP | Destination address |
|---|---|---|---|---|---|
| □ | test1 | ☑ | WAN1 | 192.168.1.2-192.168.1.5 | All Users |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

□ Select All Add Delete All Delete

Rule test1 ▼ Move To Mode test1 ▼

**Figure 5-15 Policy Routing List**

- **Enable policy routing:** Select to enable Policy Routing.

- **Add a Policy Routing Entry:** Click the **Add** button, then setup it, lastly click the **Save** button.

- **Allow a PBR Entry:** Select the **Allow** check box to enable the corresponding Policy Routing entry. If you want to disable the Policy Routing entry temporarily instead of deleting it, please clear the check mark.

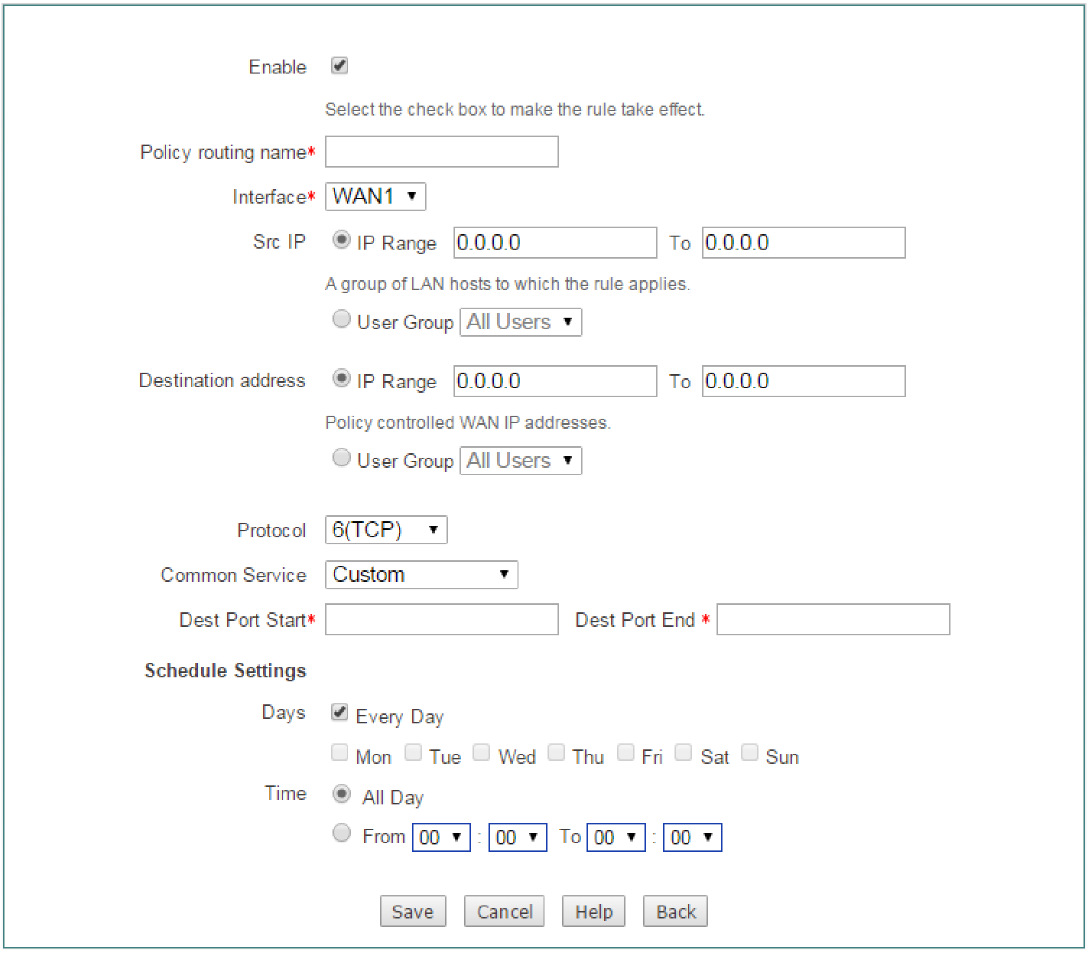
- **Edit a Policy Routing Entry: C**lick its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete Policy Routing Entry(s):** Select the leftmost check boxes of them, and then click the **Delete** button.

- **Move a Policy Routing Entry:** The operation of moving a Policy Routing entry to the front of another entry is as follows: Select the name of a Policy Routing entry from the **Rule** drop-down list, and another entry's ID from the **Mode** drop-down list, lastly click the **Move TO** button.

}

## 5.3.1.2 Policy Routing settings



Enable ☑

Select the check box to make the rule take effect.

Policy routing name*

Interface* WAN1 ▼

Src IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Destination address ● IP Range 0.0.0.0 To 0.0.0.0

Policy controlled WAN IP addresses.

○ User Group All Users ▼

Protocol 6(TCP) ▼

Common Service Custom ▼

Dest Port Start* Dest Port End *

Schedule Settings

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

**Figure 5-16 Policy Routing settings**

- **Enable:** Select to enable the Policy Routing entry. Only you have selected this checkbox, the Policy Routing entries will take effect.

- **Policy routing name:** Specify the name of this Policy Routing entry.

- **Interface:** Specify an outbound interface through which the packets matching the Policy Routing entry are forwarded.

- **Src IP:** Specify the source IP addresses of the packets to which the Policy Routing entry applies.

- **Destination address:** Specify the destination IP addresses of the packets to which the Policy Routing entry applies.

- **Protocol:** Select a protocol type from the drop-down list.

- **Common Service:** Select a common used service from the drop-down list.

}

- **Dest Port:** Specify the start and end port numbers in the associated text boxes. The port number is between 1 and 65535.

- **Schedule Settings:** Specify a schedule to restrict when the Policy Routing entry takes effect. The default value is **Every Day** and **All Day**, which means the Policy Routing entry will be in effect always.

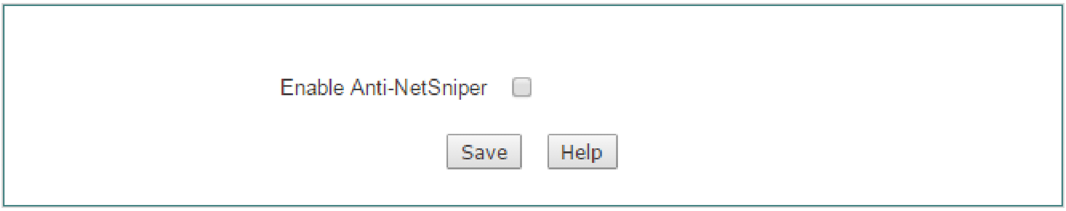
**Note:**

Policy Routing takes precedence over the Device's normal destination-based routing. That is, if a packet matches all the criteria (source address, destination address, protocol type, port, etc.) specified in a Policy Routing entry, it will be forwarded through the outbound interface specified in the Policy Routing entry. If no match is found in the Policy Routing list, the packet will be forwarded through normal routing channel (in other words, destination-based routing is performed).

## 5.4 Anti-NetSniper

This section describes **Advanced > Anti-NetSniper** page.

Anti-NetSniper is used to crack shared Internet access detection which can be performed by your ISP. Don't enable this feature unless you encounter the "shared Internet access detection" issue.

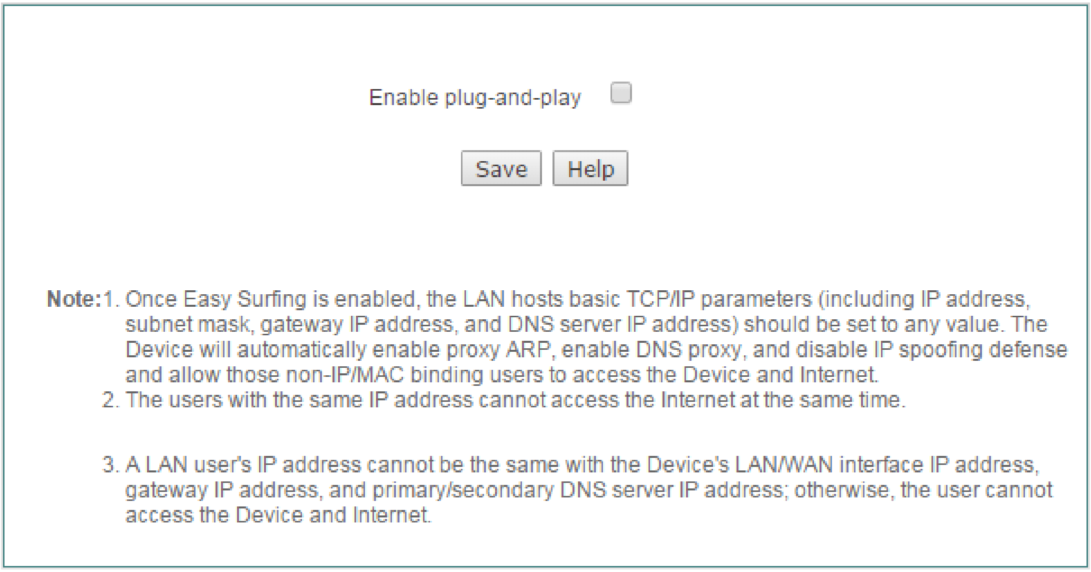


Enable Anti-NetSniper □

**Figure 5-17 Anti-NetSniper**

## 5.5 Plug and Play

Plug and Play is a new feature of Niveo series security firewalls. If you enable plug and play feature on the Device, the LAN users can access the Internet through the Device without changing any network parameters, no matter what IP address, subnet mask, default gateway and DNS server they might have. Obviously, this feature can greatly facilitate the users. As this feature is suitable for hotel network, we also call it hotel special version.



Enable plug-and-play □

Note:1. Once Easy Surfing is enabled, the LAN hosts basic TCP/IP parameters (including IP address, subnet mask, gateway IP address, and DNS server IP address) should be set to any value. The Device will automatically enable proxy ARP, enable DNS proxy, and disable IP spoofing defense and allow those non-IP/MAC binding users to access the Device and Internet.
2. The users with the same IP address cannot access the Internet at the same time.

3. A LAN user's IP address cannot be the same with the Device's LAN/WAN interface IP address, gateway IP address, and primary/secondary DNS server IP address; otherwise, the user cannot access the Device and Internet.

**Figure 5-18 Plug and Play**

**Note:**

1) The LAN hosts basic TCP/IP parameters (including IP address, subnet mask, gateway IP address, and DNS server IP address) should be set properly; otherwise, plug and play feature cannot act on those hosts.

2) Once plug and play is enabled, the Device will automatically enable proxy ARP, enable DNS proxy, and disable IP spoofing defense.

3) Once plug and play is enabled, the Device will allow those non-IP/MAC binding users to access the Device and Internet.

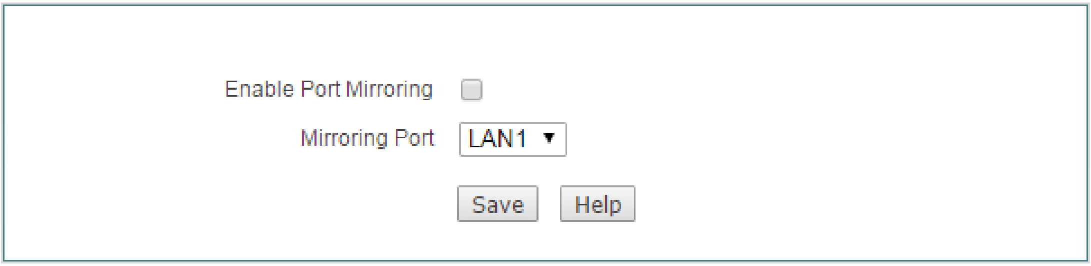
4) The users with the same IP address cannot access the Internet at the same time. For example, if a LAN user with IP address 1.1.1.1 has connected to the Device to access the Internet, another user with IP address 1.1.1.1 cannot access the Internet through the Device.

5) A LAN user’s IP address cannot be the same with the Device’s LAN/WAN interface IP address, gateway IP address, and primary/secondary DNS server IP address; otherwise, the user cannot access the Device and Internet.

## 5.6 Port Mirroring

The port mirroring allows an administrator to mirror and monitor network traffic. It copies the traffic from the specified ports to another port where the traffic can be monitored with an external network analyzer. Then the administrator can perform traffic monitoring, performance analysis and fault diagnosis.

}



Enable Port Mirroring □

Mirroring Port LAN1 ▼

**Figure 5-19 Port Mirroring**

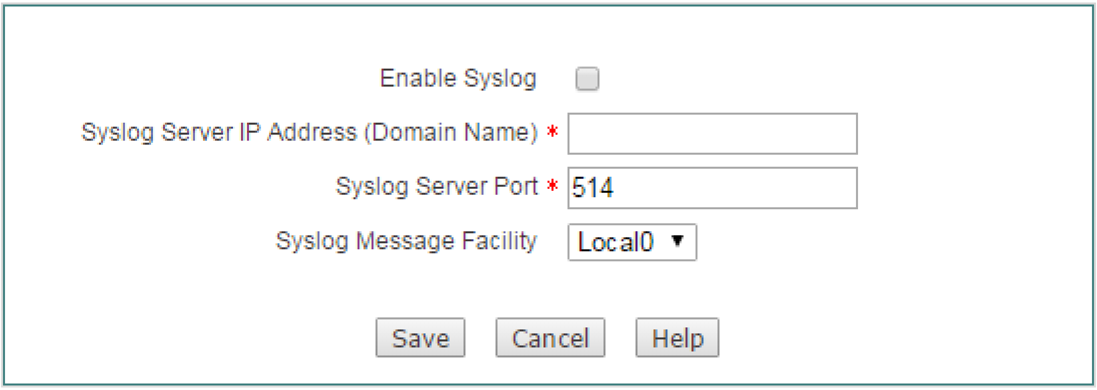
- **Enable Port Mirroring:** Select to enable port mirroring.

- **Mirroring Port:** Specify the capture port that will mirror the traffic of the mirrored port(s).

## 5.7 Syslog

This section describes the **Advanced > Syslog** page.

Syslog is a standard protocol used to capture a lot of running information about network activity. The Device supports this protocol and can send its activity logs to an external syslog server. It helps the network administrator monitor, analyze and troubleshoot the Device and network.



Enable Syslog □

Syslog Server IP Address (Domain Name) *

Syslog Server Port * 514

Syslog Message Facility Local0 ▼

**Figure 5-20 Syslog settings**

- **Enable Syslog:** Select to enable syslog feature.

- **Syslog Server IP address:** Specify the IP address or domain name of the syslog server to which the Device sends syslog messages.

- **Syslog Server Port:** Specify the port used by the syslog server to communicate with the Device. In most cases, please leave the default value of **514**, which is a well-known port number.

}

- **Syslog Message Facility:** Specify the facility level used for logging. The facilities are used to distinguish different classes of syslog messages.

**Note:** So far, only the Xport HiPER Manager software of UTT Technologies Co., Ltd. can identify the heartbeat message.

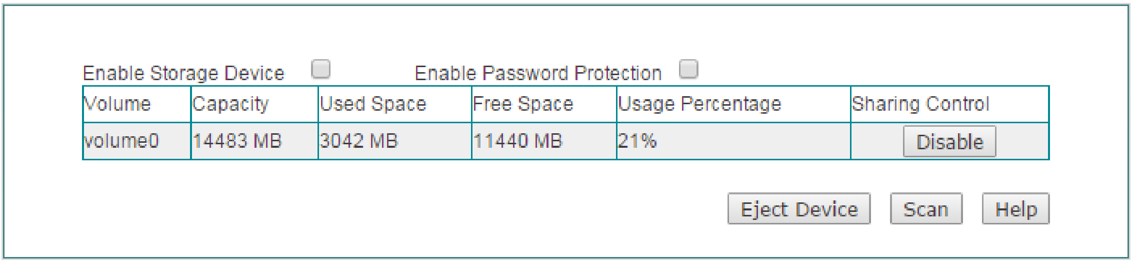
## 5.8 Network Sharing Menu

This section describes the function on the Network Sharing menu. Network Sharing is a model of data storage where the digital data is stored in USB disk/SD card. The USB disk/SD card is owned and managed by Administrator who is responsible for keeping the data available and accessible. Users access to USB disk/SD card for digital data.

## 5.9 Sharing Management

After plugging a USB/SD card into the Device, administrator could share the Data on the USB/SD card to LAN users through the FTP function. Before you enable network sharing, please first setup the account for users on the **Network Sharing > Shared Account** page.

Click **Network Sharing > Sharing Management**, you will see the following figure.



Enable Storage Device □ Enable Password Protection □

| Volume | Capacity | Used Space | Free Space | Usage Percentage | Sharing Control |
|---|---|---|---|---|---|
| volume0 | 14483 MB | 3042 MB | 11440 MB | 21% | Disable |

**Figure 5-21 Network Sharing**

- **Enable Storage Device:** Select to enable network sharing.
- **Enable Password Protection:** If selected, LAN users must use the account which is set on the **Network Sharing > Shared Account** page to access the storage device.
- **Disable:** Click to disable the storage device.
- **Eject Device:** Click to eject the storage device.
- **Scan:** Click to scan the available storage device.

**Notes:**

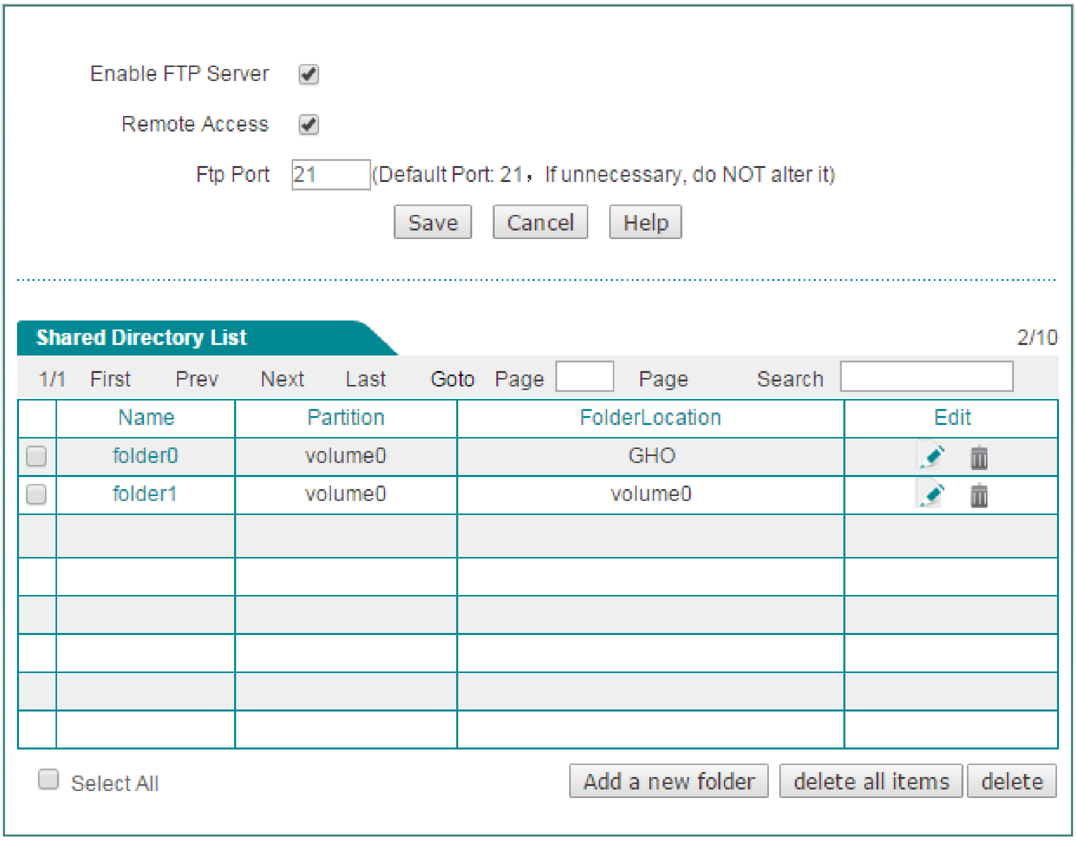
}

1) Before you eject the USB/SD card from the Device, please click the **Eject Device** button first, in case of unexpected error or irreparable hardware damage.

2) It is recommended to use NTFS file system.

## 5.10 FTP Server

On the **Network Sharing** > **FTP Server** page, you can setup FTP server to share data to local area users. All the sources you have shared are displayed on the Shared Directory List.



Enable FTP Server ☑

Remote Access ☑

Ftp Port 21 (Default Port: 21，If unnecessary, do NOT alter it)

**Shared Directory List** 2/10

| | Name | Partition | FolderLocation | Edit |
|---|---|---|---|---|
| □ | folder0 | volume0 | GHO | ✎ 🗑 |
| □ | folder1 | volume0 | volume0 | ✎ 🗑 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

□ Select All

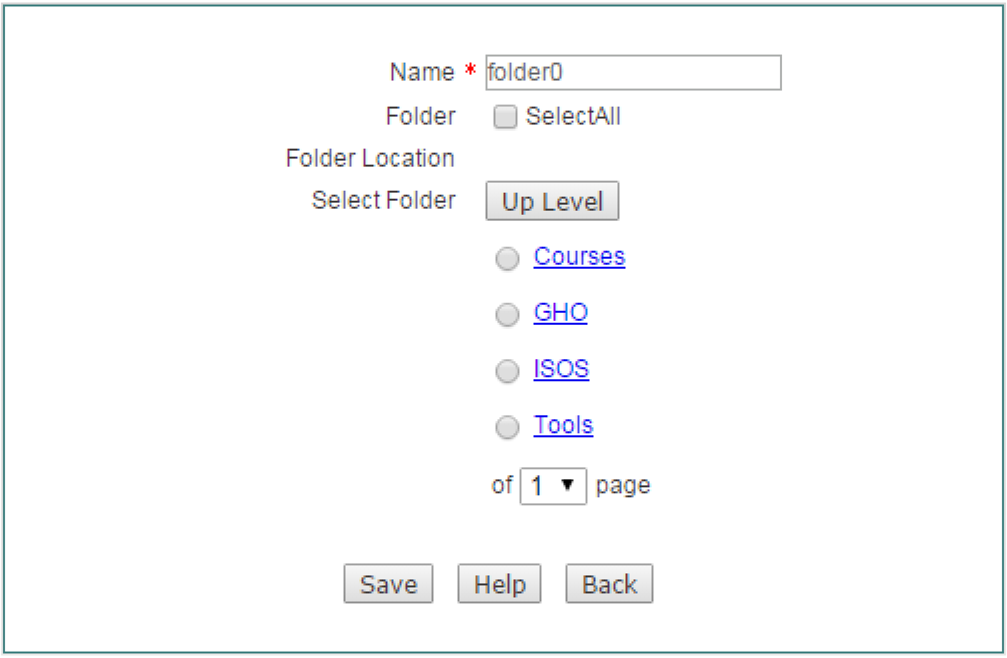
**Figure 5-22 FTP Server**

- **Enable FTP Server:** Select to enable FTP Server.
- **Remote Access:** Select to enable remote access from WAN port.
- **Ftp Port:** Specify the FTP server port for LAN users to access. The default value is 21. We recommend that you do not change the default value unless absolutely necessary.

Click the **Add a new folder** button or ✎ to add a new folder for data sharing or edit

}

the setting of the current folders.



Name * folder0

Folder □ SelectAll

Folder Location

Select Folder

**Figure 5-23 FTP Server Settings**

- **Name:** Specify the name of the folder which will be display on the Shared Directory List.

- **Folder:** Select to share all folders.

- **Select Folder:** Select one of the paths to share.

**Notes:**

1) All the changes you have made will be take effect after restart.

2) There are two ways to access FTP Server:

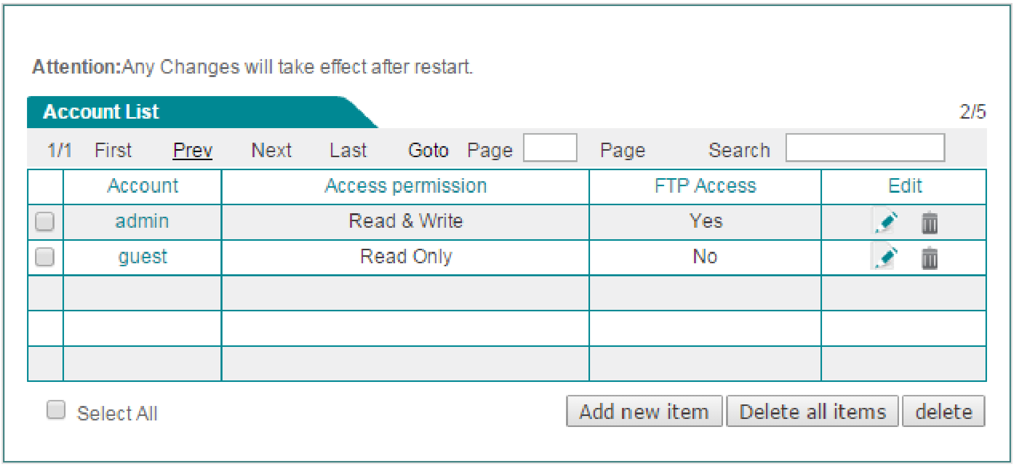
**For local users:** Double-click 'My Computer', enter ftp://xxx.xxx.xxx.xxx:21 (xxx.xxx.xxx.xxx stands for the IP address of the LAN port) in the address bar to open the shared resources folder. Such as: when the IP address of the LAN port is 192.168.1.1, you could enter ftp://192.168.1.1:21.

**For remote users:** First you should ensure that the Remote Access checkbox on the Figure 8- 2 have been selected. Double-click 'My Computer', enter ftp: \\xxx. xxx. xxx. xxx :21 (xxx.xxx.xxx.xxx stands for the IP address of the WAN port) in the address bar to open the shared resources folder. Such as: when the IP address of the WAN port is 172.32.90.1, you could enter ftp:// 172.32.90.1:21.

}

## 5.11 Shared Account

You need to add account for users to access the FTP server before enabling network sharing.



**Attention:**Any Changes will take effect after restart.

Account List 2/5

1/1 First Prev Next Last Goto Page [ ] Page Search [ ]

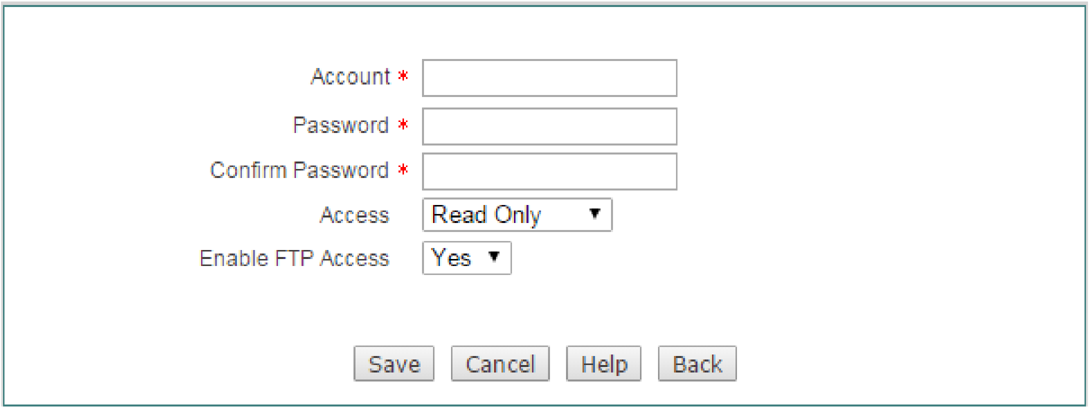
| | Account | Access permission | FTP Access | Edit |
|---|---|---|---|---|
| □ | admin | Read & Write | Yes | ✎ 🗑 |
| □ | guest | Read Only | No | ✎ 🗑 |
| | | | | |
| | | | | |
| | | | | |

□ Select All

**Figure 5-24 Shared Account**

Please setup the username and password for the user account before enabling network sharing. The two default account is **admin** and **guest**. The account of admin has the right to write and read data, and who also can upload the changes on the volume to the server through IE. The account of guest only has the right to read data.

Click the **Add new item** button on the Figure 8-4 to add a new account. You should specify the username and the password for all account.



| | |
|---|---|
| Account * | |
| Password * | |
| Confirm Password * | |
| Access | Read Only ▼ |
| Enable FTP Access | Yes ▼ |

**Figure 5-25 Shared Account Settings**

- **Account:** Specify the unique name of the account.
- **Password:** Specify the password of the account.
- **Confirm Password:** Enter the password again.

}

- **Access:** Grant this account the right to read or read and write. .

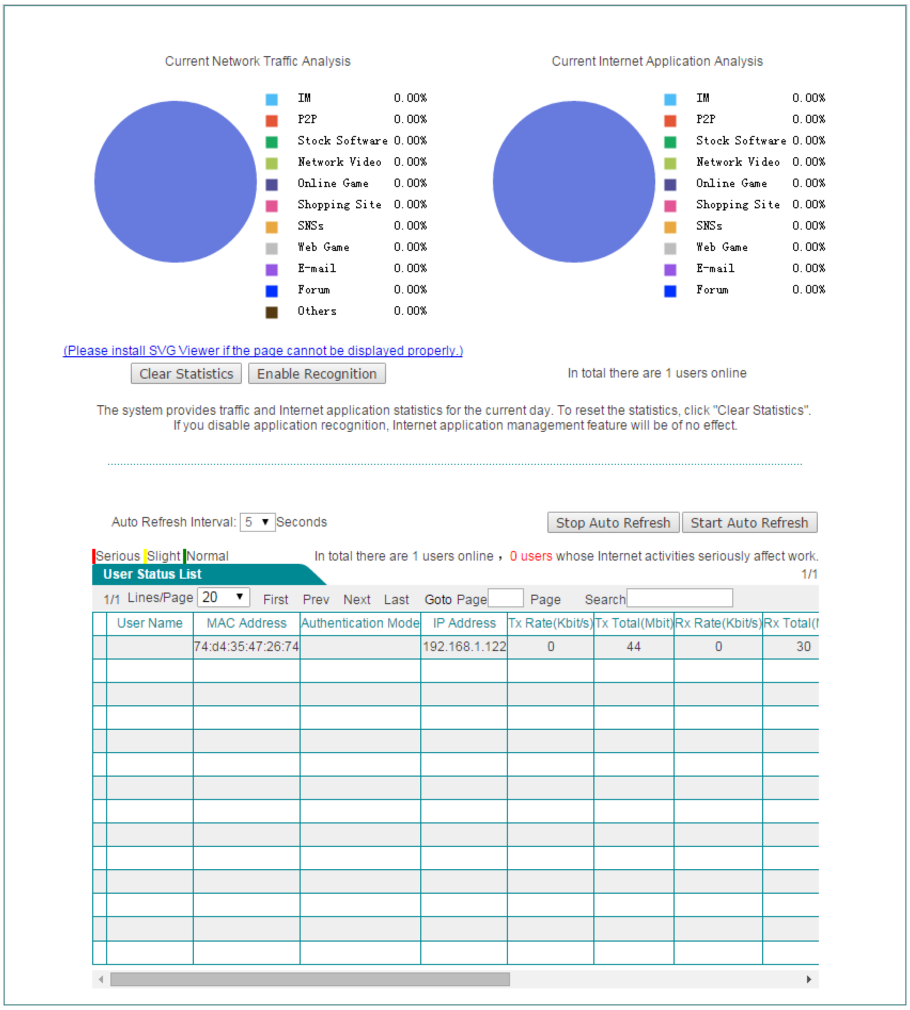
- **Enable FTP Access:** Select **Yes** to allow this account to access FTP server, select **No** to forbid this account to access FTP server.

**}**

# apter 6. User Management Menu

## 6.1 User Status

This section describes **User Management > User Status** page, where you can monitor and analyze network traffic, online behaviors of the LAN users, and current status information of each user, including Rx/Tx rate, Rx/Tx total traffic, Internet behavior, online time, etc.



Current Network Traffic Analysis

| | | |
|---|---|---|
| 🟦 | IM | 0.00% |
| 🟥 | P2P | 0.00% |
| 🟩 | Stock Software | 0.00% |
| 🟩 | Network Video | 0.00% |
| 🟪 | Online Game | 0.00% |
| 🟪 | Shopping Site | 0.00% |
| 🟧 | SNSs | 0.00% |
| ⬜ | Web Game | 0.00% |
| 🟪 | E-mail | 0.00% |
| 🟦 | Forum | 0.00% |
| 🟫 | Others | 0.00% |

Current Internet Application Analysis

| | | |
|---|---|---|
| 🟦 | IM | 0.00% |
| 🟥 | P2P | 0.00% |
| 🟩 | Stock Software | 0.00% |
| 🟩 | Network Video | 0.00% |
| 🟪 | Online Game | 0.00% |
| 🟪 | Shopping Site | 0.00% |
| 🟧 | SNSs | 0.00% |
| ⬜ | Web Game | 0.00% |
| 🟪 | E-mail | 0.00% |
| 🟦 | Forum | 0.00% |

(Please install SVG Viewer if the page cannot be displayed properly.)

Clear Statistics | Enable Recognition

In total there are 1 users online

The system provides traffic and Internet application statistics for the current day. To reset the statistics, click "Clear Statistics". If you disable application recognition, Internet application management feature will be of no effect.

Auto Refresh Interval: 5 ▼ Seconds

Stop Auto Refresh | Start Auto Refresh

Serious Slight Normal

In total there are 1 users online， 0 users whose Internet activities seriously affect work.

User Status List 1/1

1/1 Lines/Page 20 ▼ First Prev Next Last Goto Page Page Search

| | User Name | MAC Address | Authentication Mode | IP Address | Tx Rate(Kbit/s) | Tx Total(Mbit) | Rx Rate(Kbit/s) | Rx Total( |
|---|---|---|---|---|---|---|---|---|
| | | 74:d4:35:47:26:74 | | 192.168.1.122 | 0 | 44 | 0 | 30 |

**Figure 6-1 User Behavior Analysis Pie Charts**

- **Current Network Traffic Analysis:** Displays the percentage of network traffic made up by each application in your network.

- **Current Internet Application Analysis:** Displays the percentage of users engaging in various online activities in your network.

}

- **Clear Statistics:** The system provides network traffic and Internet behavior statistics for the current day. To reset the current statistics, click the **Clear Statistics** button.

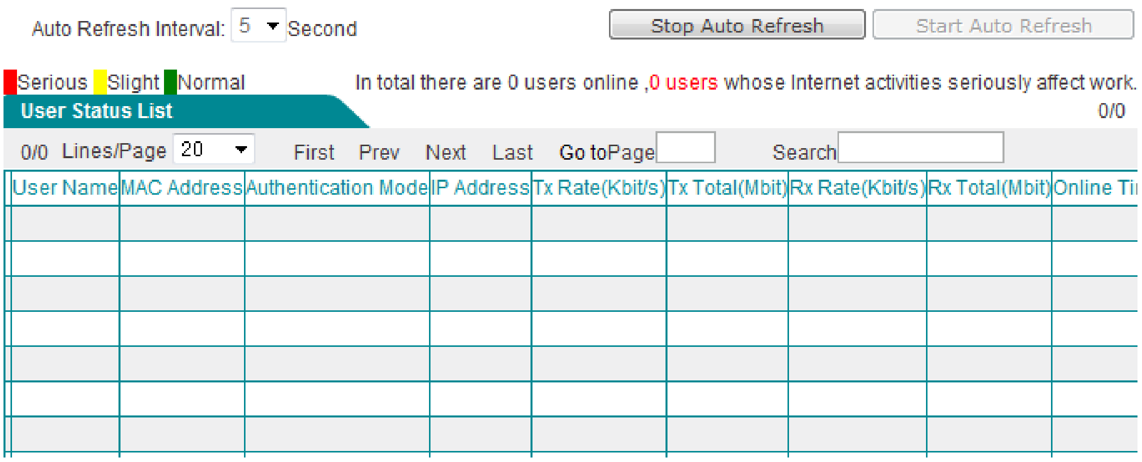
- **Enable Recognition:** Click to enable application recognition. If enabled, the Internet application management feature (set in **App Control > Application Control** page) will take effect.

**Note:**

If the SVG Viewer isn't installed on your PC, the rate chart cannot be displayed properly. To view the rate chart, click the **(Please install SVG Viewer if the page cannot display properly.)** hyperlink to download and install the SVG Viewer.

### 1) User Status List

In **User Status List**, you can view current status of each user, including online time, Rx/Tx rate, Rx/Tx total traffic, Internet behavior, etc.



Auto Refresh Interval: 5 Second

🟥Serious 🟨Slight 🟩Normal

In total there are 0 users online ,0 users whose Internet activities seriously affect work.

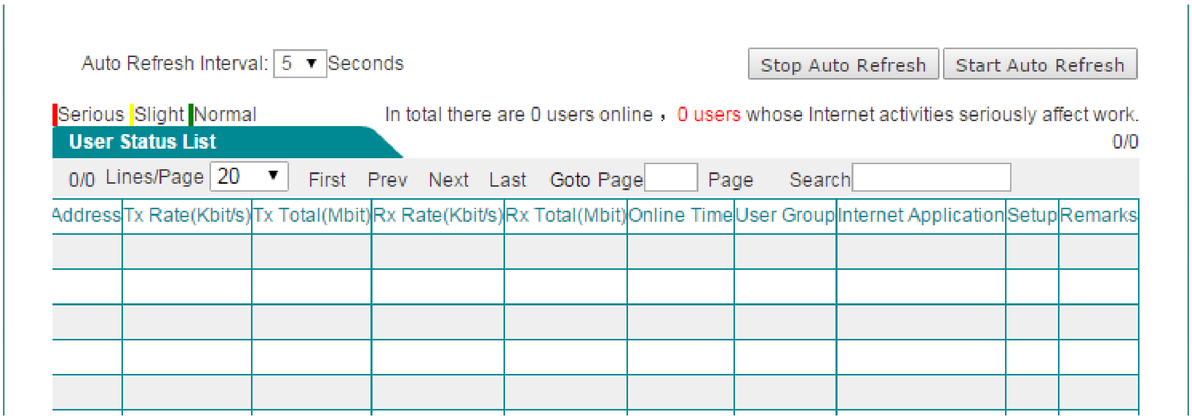
User Status List

0/0

0/0 Lines/Page 20

| User Name | MAC Address | Authentication Mode | IP Address | Tx Rate(Kbit/s) | Tx Total(Mbit) | Rx Rate(Kbit/s) | Rx Total(Mbit) | Online Ti |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**Figure 6-2 User Status List**



Auto Refresh Interval: 5 Seconds

🟥Serious 🟨Slight 🟩Normal

In total there are 0 users online， 0 users whose Internet activities seriously affect work.

User Status List

0/0

0/0 Lines/Page 20

| Address | Tx Rate(Kbit/s) | Tx Total(Mbit) | Rx Rate(Kbit/s) | Rx Total(Mbit) | Online Time | User Group | Internet Application | Setup | Remarks |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Figure 6-3 User Status List (continued)**

The first column in **User Status List** indicates whether a user's online activities affect work. The color of the first column indicates the impact of different degree: Red

}

stands for Serious, Yellow stands for slight, and Green stands for normal. For a user, if the percentage of network traffic made up by accessing shopping sites, social networking sites, using stock software, and playing online/web games is equal to or above 70%, his/her online activities seriously affect work. If the percentage is between 50% and 70% (below 70%), his/her online activities slightly affect work. Else, his/her online activities don't affect work.

- **User Name:** Shows the user name of the user.
- **MAC Address:** Displays the MAC address of the user.
- **Authentication Mode:** Displays the authenticaiton mode of the user.
  - **PPPoE:** The user is a PPPoE user.
  - **WEB:** The user is a Web authentication user.
- **IP Address:** Displays the IP address of the user.
- **Tx/Rx Rate:** Displays the upload/download speed of the user.
- **Tx/Rx Total:** Displays the total traffic transmitted/received by the user.
- **Online Time:** Displays the online time of the user.
- **User Group:** Displays the user group to which the user belongs.
- **Internet Application:** Displays the online activities of the user.
- **Setup:** Click ⬇, and then click the **Clear Statistics** button to clear the Internet behavior statistics of the user.
- **Remarks:** If the user is a PPPoE user or Web authentication user, you can click ♥ icon to modify the description of the user.
- **Auto Refresh Interval:** Specify the value of the interval at which **User Status List** will automatically refresh. The range is 1 to 5 seconds.
- **Stop Auto Refresh:** Click to stop **User Status List** from auto refreshing.
- **Start Auto Refresh:** Click to make **User Status List** automatically refresh at the specified interval.

## 6.2 IP/MAC binding

To achieve network security management, you should firstly implement user identification, and then you should implement user authorization. **Section 12.2 Access Control** describes how to configure and use access control rules to control the Internet behaviors of the LAN users. In this section, we will describe how to implement user identification.

The Device provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Device and your network against IP spoofing attacks. IP spoofing attack refers to that a host attempts to use another trusted host's IP address to connect to or pass through the Device. The host's IP address can easily be changed to a trusted address, but MAC address cannot easily be changed as it is added to the Ethernet card at the factory.

The IP/MAC binding feature allows you to add the IP and MAC address pairs of trusted LAN hosts in the **IP/MAC Binding List**. Note that in the **IP/MAC Binding List**, you can allow or block Internet access for each IP/MAC binding user. After you have added a LAN user's IP and MAC address pair into the **IP/MAC Binding List**, if its **Allow** check box is selected (check mark √ appears), it will allow the user to access the Device and Internet, else block the user.

#### 6.2.1.1 The Operation Principle of IP/MAC Binding

For the sake of convenience, we firstly introduce several related terms including legal user, illegal user and undefined user.

Legal User: A legal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is selected.

Illegal User: A illegal user's IP and MAC address pair matches an IP/MAC binding whose **Allow Internet Access** check box is unselected; or the IP address or MAC address is the same with an IP/MAC binding's, but not both.

Undefined User: An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

It allows the legal users to access the Device and access the Internet through the Device, and denies the illegal users. And the parameter of **Allow Undefined LAN PCs** determines whether it allows the undefined users to access the Device and access the Internet through the Device, that is, it will allow them if the **Allow Undefined LAN PCs** check box is selected, else block them.

IP/MAC binding feature can act on the packets initiated from the LAN hosts to the Device or outside hosts. When receiving a packet initiated from LAN, the Device will firstly determine the sender's identity by comparing the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the sender's identity. The details are as follows:

1) If the sender is a legal user, the packet will be allowed to pass, and then be further processed by the firewall access control function module.

2) If the sender is an illegal user, the packet will be dropped immediately to prevent IP spoofing.

3) If the sender is an undefined user, there are two cases:

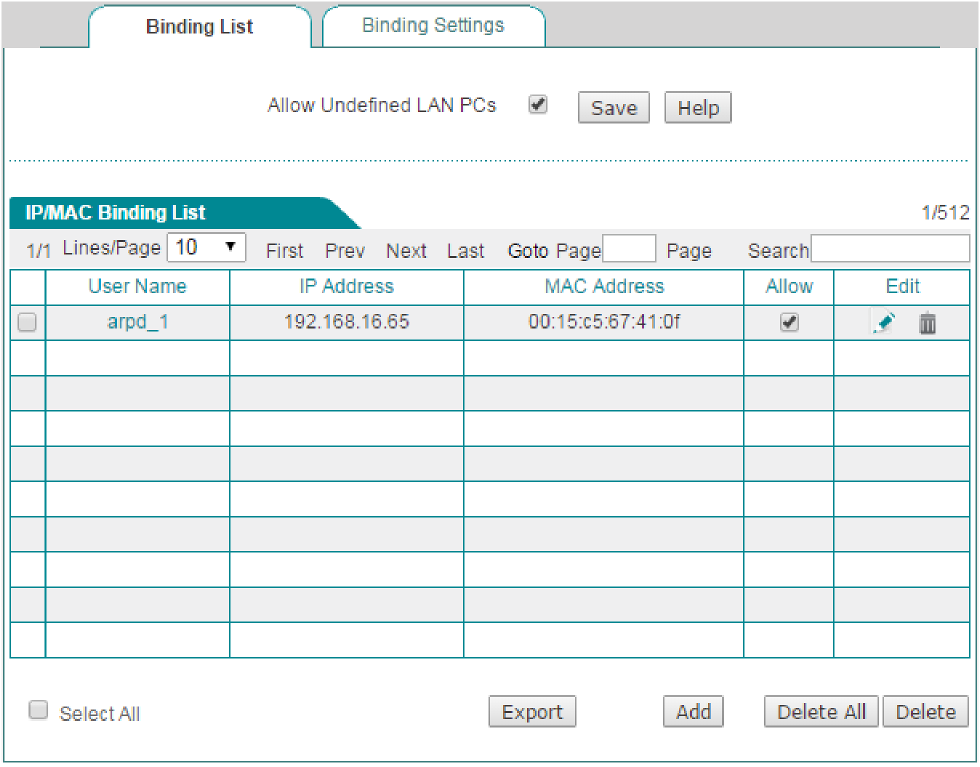
    (1) If the **Allow Undefined LAN PCs** check box is selected, the packet will be

**}**

allowed to pass, and then be further processed by the firewall access control function module.

(2) Else, the packet will be dropped immediately.

For example, if the IP/MAC address pair IP 192.168.16.65 and 00:15:c5:67:41:0f is added to the **IP/MAC Binding List**, and its **Allow** check box is selected, see the following figure.



Binding List | Binding Settings

Allow Undefined LAN PCs ☑ Save Help

IP/MAC Binding List 1/512

1/1 Lines/Page 10 ▾ First Prev Next Last Goto Page Page Search

| | User Name | IP Address | MAC Address | Allow | Edit |
|---|---|---|---|---|---|
| □ | arpd_1 | 192.168.16.65 | 00:15:c5:67:41:0f | ☑ | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

□ Select All Export Add Delete All Delete

**Figure 6-4 IP/MAC Binding List - Example One**

Then, when receiving a packet initiated from LAN, the Device will process it according to the following cases:

1) A packet with IP address 192.168.16.65 and MAC address 00:15:c5:67:41:0f is allowed to pass, and then it will be further processed by the firewall access control function module.

2) A packet with IP address 192.168.16.65 but with a different MAC address is dropped immediately to prevent IP spoofing.

3) A packet with a different IP address but with MAC address 00:15:c5:67:41:0f is dropped immediately to prevent IP spoofing.

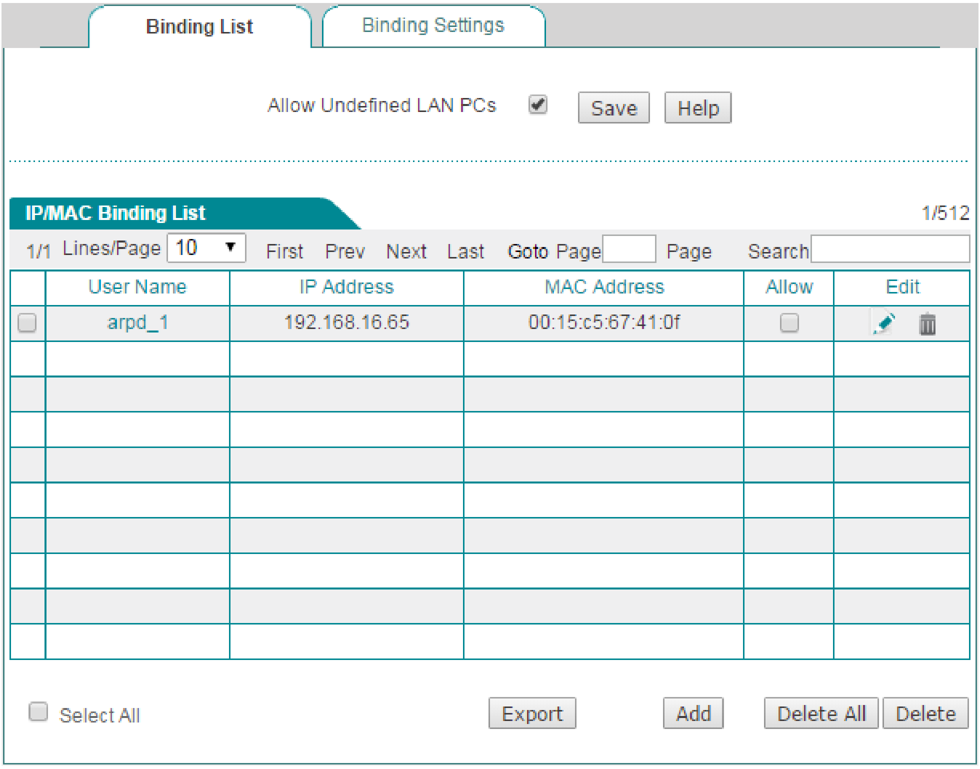
4) A packet's IP address and MAC address both are not defined in the **IP/MAC Binding List**:

**}**

(1) If the **Allow Undefined LAN PCs** check box is selected, the packet is allowed to pass, and then it will be further processed by the firewall access control function module.

(2) Else, the packet is dropped.

If you want to block the user who matches the IP/MAC binding from accessing the Device and Internet, you need unselect **Allow** check box, see the following figure. Then a packet with IP address 192.168.16.65 and MAC address 00:15:c5:67:41:0f will be dropped.



Allow Undefined LAN PCs ☑

IP/MAC Binding List 1/512

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | User Name | IP Address | MAC Address | Allow | Edit |
|---|---|---|---|---|---|
| □ | arpd_1 | 192.168.16.65 | 00:15:c5:67:41:0f | □ | ✎ 🗑 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

□ Select All

**Figure 6-5 IP/MAC Binding List - Example Two**

**Note:**

1) If you have added the IP and MAC address pair of a trusted LAN host in the **IP/MAC Binding List**, and later changed this host's IP address or MAC address, you must also change the corresponding binding in the **IP/MAC Binding List**; otherwise the host cannot access the Device and Internet. If the **Allow Undefined LAN PCs** check box is unselected, you must also add the IP and MAC address pair of any new host that you add to your network, and make sure that its **Allow** check box is selected; otherwise this new host cannot access the Device and Internet.

2) IP/MAC binding feature can only act on the packets initiated from the LAN hosts to the Device or outside hosts, but cannot act on the packets within the LAN. If

}

you change a LAN host's IP address or MAC address, this LAN host will be unable to access the Device and access the Internet through the Device, but it still can communicate with the other LAN hosts, such as, it can browse Network Neighborhood, use windows file and printer sharing services within the LAN, and so on.

### 6.2.1.2 Binding List

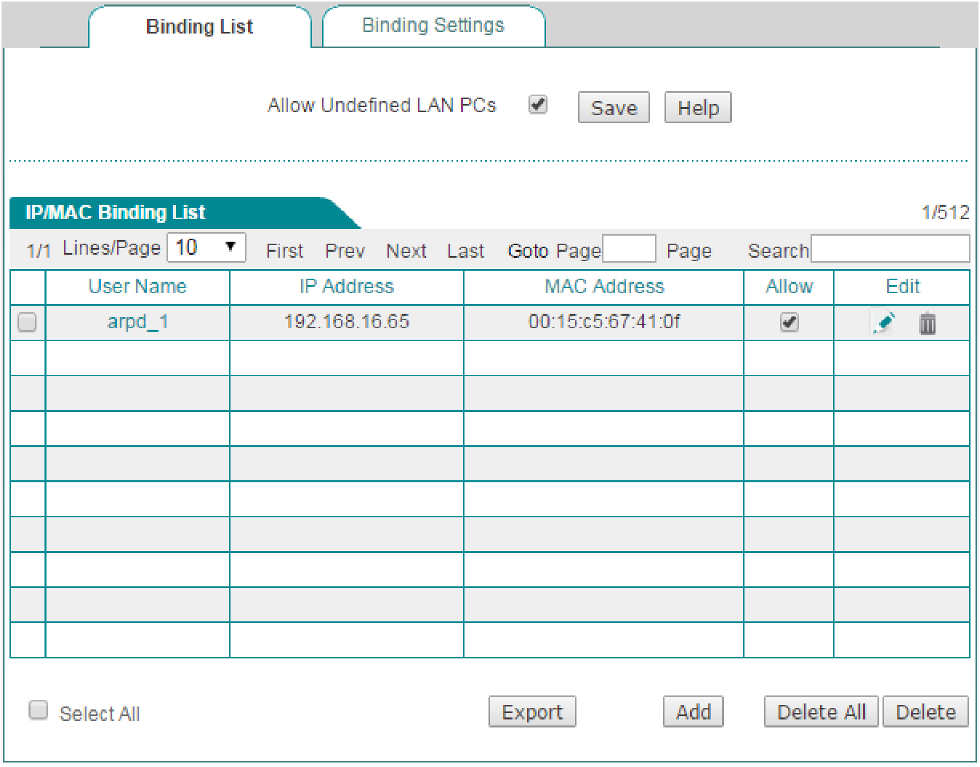
You can view and edit all the IP/MAC Binding entries on **User Management** > **IP MAC binding** > **Binding List** page.

- **Add an IP/MAC Binding:** Click the **Add** button or select the **Binding Settings** tab to go to the setup page, and then configure it, lastly click the **Save** button.

- **Edit an IP/MAC Binding:** Click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button. The **Allow** check box is used to allow or block a user matching an IP/MAC binding from accessing the Device and Internet.

- **Delete IP/MAC Binding(s):** Select the leftmost check boxes, and then click **Delete** on the lower right corner of the **IP/MAC Binding List**.

- **Delete All:** Click **Delete All** on the lower right corner of the list, and then click the **OK** button.



Allow Undefined LAN PCs ☑

1/512

1/1 Lines/Page 10 Goto Page Page Search

| | User Name | IP Address | MAC Address | Allow | Edit |
|---|---|---|---|---|---|
| □ | arpd_1 | 192.168.16.65 | 00:15:c5:67:41:0f | ☑ | ✎ 🗑 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

□ Select All

**Figure 6-6 IP/MAC Binding List**

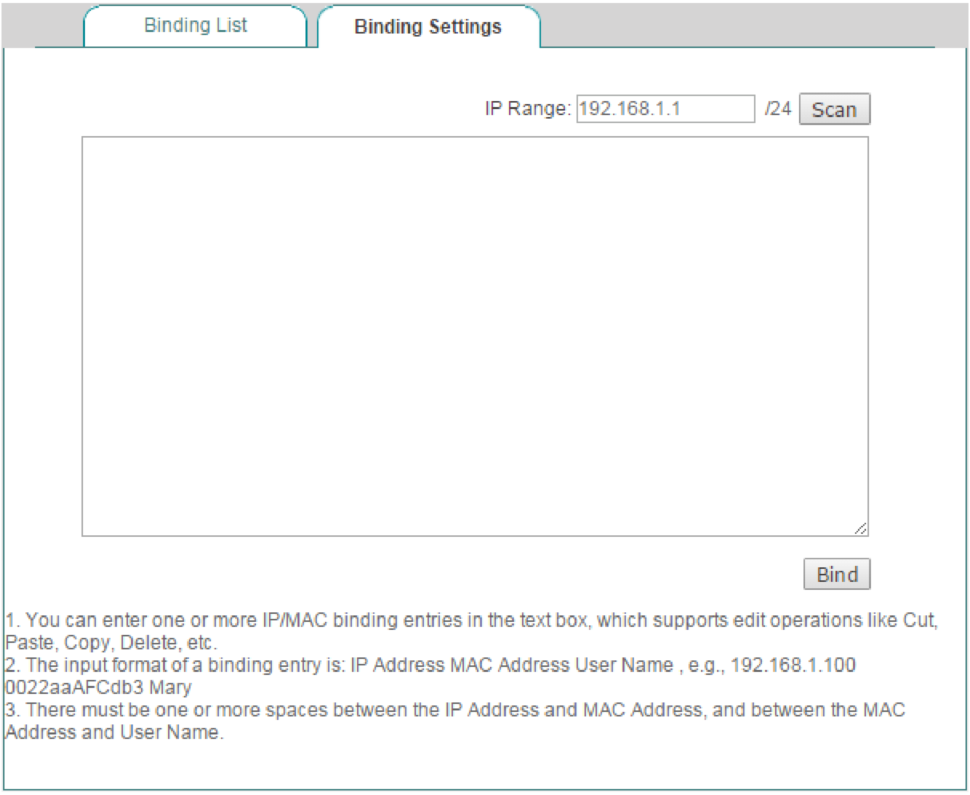
- **Allow Undefined LAN PCs:** Select to allow the undefined LAN hosts from accessing the Device and access the Internet through the Device.

}

- **Export:** Click to download the IP/MAC binding (that is, static ARP binding) script file to the local host. Then run the file and restart the host to add all the static ARP entries to the host to prevent ARP spoofing.

⌖ **Note:** If you want to unselect the **Allow Undefined LAN PCs** check box to block the undefined LAN hosts from accessing or passing through the Device, you should make sure that you have added the IP/MAC address pair of the host that you use to administer the Device into the **IP/MAC Binding List**.

#### 6.2.1.3 Binding Settings



1. You can enter one or more IP/MAC binding entries in the text box, which supports edit operations like Cut, Paste, Copy, Delete, etc.
2. The input format of a binding entry is: IP Address MAC Address User Name , e.g., 192.168.1.100 0022aaAFCdb3 Mary
3. There must be one or more spaces between the IP Address and MAC Address, and between the MAC Address and User Name.

**Figure 6-7 IP/MAC Binding Settings**

- **Scan:** If you click the **Scan** button, the Device will immediately scan the LAN to detect active hosts connected to the Device, learn and display dynamic ARP information (that is, IP and MAC address pairs). Note that if you have added a LAN host's IP and MAC address pair in the **IP/MAC Binding List**, this IP/MAC address pair will not be displayed here.

- **Bind:** Click it to bind all the valid IP and MAC address pairs in the list box.

  Also you can manually create one or more IP/MAC bindings, the operation is as follows: Add one or more IP/MAC address pair entries in the list box, and then click the **Bind** button. The input contents are: IP Address, MAC Address and Description, one address pair entry per line; and the input format of an address pair entry is: IP Address**<Space>**MAC Address**<Space>**Description**<Enter>**. Note that **Description** is an optional parameter.

}

### 6.2.1.4 Internet Whitelist and Blacklist

By utilizing IP/MAC binding feature, you can flexibly configure an Internet whitelist or blacklist for the LAN users.

If you want to allow only a small number of LAN users to access the Internet, you can configure an Internet whitelist for these users. Then only the users that belong to the whitelist can access the Internet, and all the other users can not access.

If you want to block only a small number of LAN users from accessing the Internet, you can configure an Internet blacklist for these users. Then only the users that belong to the blacklist cannot access the Internet, and all the other users can access.

On the Device, a user who belongs to the whitelist is a legal user, that is, the user’s IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is selected.

A user who belongs to the blacklist is an illegal user, that is, the user’s IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is unselected; or the IP address or MAC address is the same with an IP/MAC binding’s, but not both.

### 6.2.1.5 Configure an Internet Whitelist

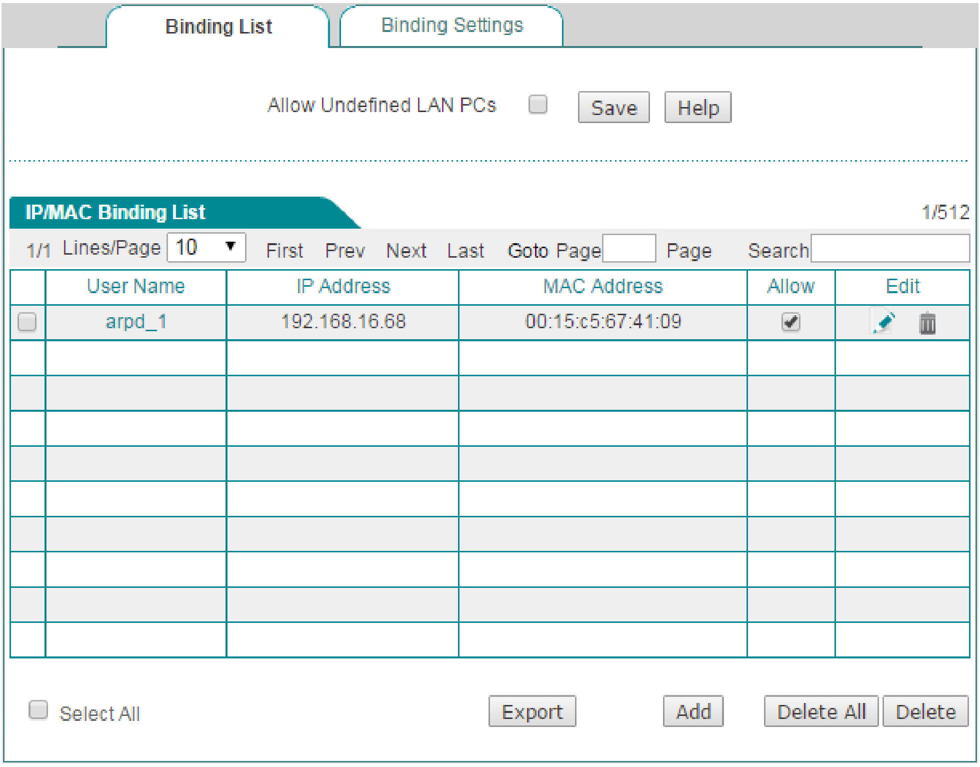
If you want to configure an Internet whitelist, do the following:

**Step 1** Go to the **User Management > IP/MAC Binding** page, and then click the **Add** button or select the **IP/MAC Binding Settings** tab to go to the setup page.

**Step 2** Specify the legal users by creating the IP/MAC bindings: Add these users’ IP and MAC address pairs into the **IP/MAC Binding List**. By default, an IP/MAC binding’s **Allow** check box is selected, which means that the user matching the IP/MAC binding can access the Device and Internet, so please leave it as the default value.

**Step 3** Unselect the **Allow Undefined LAN PCs** check box to block all the undefined users from accessing the Device and Internet.

For example, if you want to allow a LAN user with IP address 192.168.16.68 and MAC address 0015c5674109 to access the Device and Internet, you can add an IP/MAC binding for he/her into the **IP/MAC Binding List**, see the following figure. The binding’s **Allow** check box is selected by default, so please leave it as the default value.



Allow Undefined LAN PCs □

| | User Name | IP Address | MAC Address | Allow | Edit |
|---|---|---|---|---|---|
| □ | arpd_1 | 192.168.16.68 | 00:15:c5:67:41:09 | ☑ | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

□ Select All

**Figure 6-8 IP/MAC Binding List - Example Three**

### 6.2.1.6 Configure an Internet Blacklist

If you want to configure an Internet blacklist, do the following:

**Step 1** Go to the **User Management > IP/MAC Binding** page, and then click the **Add** button or select the **Binding Settings** tab to go to the setup page.

**Step 2** Specify the illegal users by creating the IP/MAC bindings. There are three methods:

**Method One:** Bind each illegal user's IP address to a MAC address which is different from any LAN host's in the **IP/MAC Binding List**.

**Method Two:** Bind an IP address which is different from any LAN host's to each illegal user's MAC address in the **IP/MAC Binding List**.

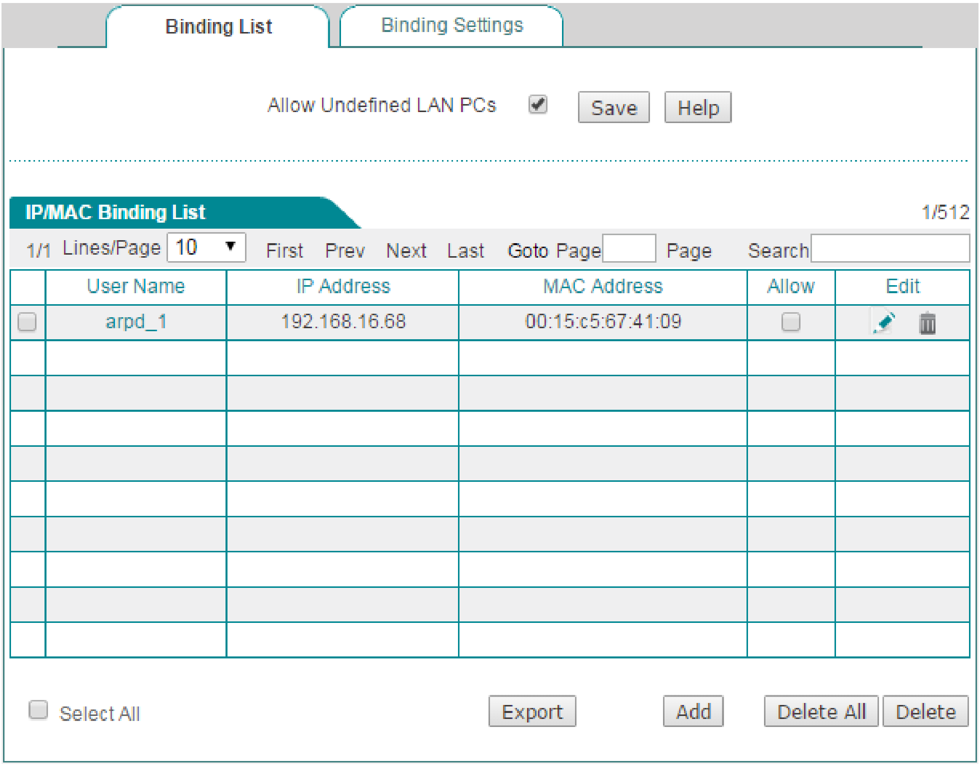
**Method Three:** Add these users' IP and MAC address pairs in the **IP/MAC Binding List**. Unselect each IP/MAC binding's **Allow** check box respectively, then the matched users can not access the Device and Internet.

**Step 3** Select the **Allow Undefined LAN PCs** check box to allow all the undefined users to access the Device and Internet.

For example, if you want to block a LAN user with IP address 192.168.16.68 and MAC address 0015c5674109 from accessing the Device and Internet, you can add the corresponding IP/MAC binding in the **IP/MAC Binding List**. And then unselect

}

the binding's **Allow** check box to block the user's access to the Device and Internet, see the following figure.



Allow Undefined LAN PCs ☑

IP/MAC Binding List 1/512

1/1 Lines/Page 10

| | User Name | IP Address | MAC Address | Allow | Edit |
|---|---|---|---|---|---|
| □ | arpd_1 | 192.168.16.68 | 00:15:c5:67:41:09 | □ | ✎ 🗑 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

□ Select All

**Figure 6-9 IP/MAC Binding List - Example Four**

# 6.3 PPPoE Server

## 6.3.1.1 Introduction to PPPoE

The PPPoE stands for Point-to-Point Protocol over Ethernet, which uses client/server model. The PPPoE provides the ability to connect the Ethernet hosts to a remote Access Concentrator (AC) over a simple bridging access device. And it provides extensive access control management and accounting benefits to ISPs and network administrators.

The PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames to provide point-to-point connection over an Ethernet network.

## 6.3.1.2 PPPoE Stages

As specified in RFC 2516, the PPPoE has two distinct stages: a discovery stage and a PPP session stage. The following describes them respectively.

}

### 6.3.1.3 PPPoE Discovery Stage

In the PPPoE discovery stage, a PPPoE client will find a proper server, and then build the connection. When a client initiates a PPPoE session, it should perform discovery to indentify the PPPoE server's Ethernet MAC address, and establish a PPPoE session ID.

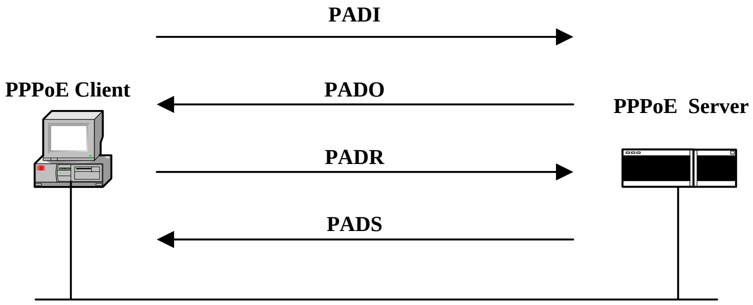


**Figure 6-10 PPPoE Discovery Stage Flows**

The discovery stage includes the following four steps:

1) **PADI (PPPoE Active Discovery Initiation):** At the beginning, a PPPoE client broadcasts a PADI packet to find all the servers that can be connected possibly. Until it receives PADO packets from one or more servers. The PADI packet must contain a service name which indicates the service requested by the client.

2) **PADO (PPPoE Active Discovery Offer):** When a PPPoE server receives a PADI packet in its service range, it will send a PADO response packet. The PADO packet must contain the server's name, and a service name identical to the one in the PADI, and any number of other service names which indicate other services that the PPPoE server can offer. If a PPPoE server receives a PADI packet beyond its service range, it cannot respond with a PADO packet.

3) **PADR (PPPoE Active Discovery Request):** The client may receive more than one PADO packet as the PADI was broadcast. The client chooses one server according to the server's name or the services offered. Then the host sends a PADR packet to the selected server. The PADR packet must contain a service name which indicates the service requested by the client.

4) **PADS (PPPoE Active Discovery Session- confirmation):** When a PPPoE server receives a PADR packet; it prepares to begin a PPP session. It generates a unique PPPoE session ID, and respond to the client with a PADS packet. The PADS packet must contain a service name which indicates the service provided to the client.

When the discovery stage completes successfully, both the server and client know the PPPoE session ID and the peer's Ethernet MAC address, which together define the PPPoE session uniquely.

**}**

## 6.3.1.4 PPP Session Stage

In the PPP session stage, the server and client perform standard PPP negotiation to establish a PPP connection. After the PPP connection is established successfully, the original datagram are encapsulated in PPP frames, and PPP frames are encapsulated in PPPoE session frames, which have the Ethernet type 0x8864. Then these Ethernet frames are sent to the peer. In a PPPoE session frame, the session ID must be the value assigned in the Discovery stage, and cannot be changed in this session.

## 6.3.1.5 PPPoE Session Termination

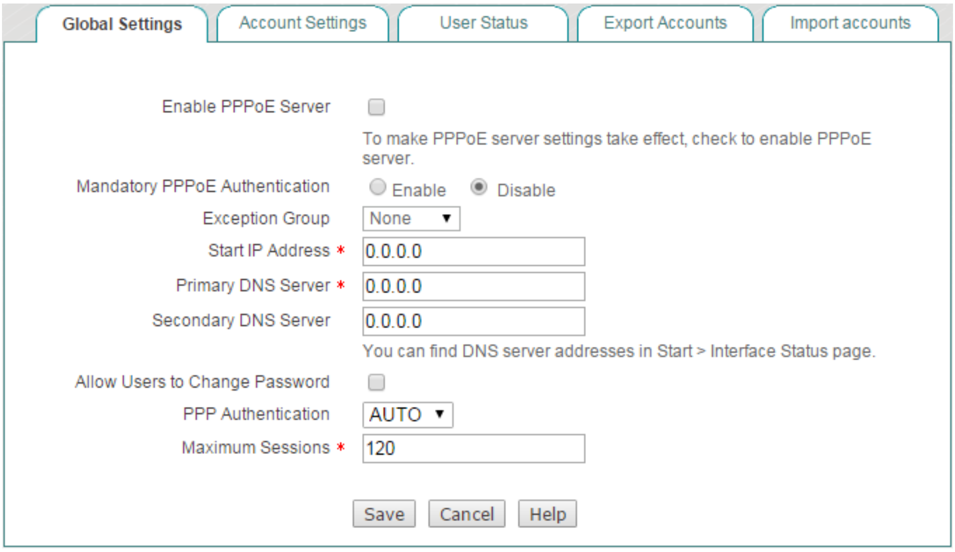
After a session is established, either the server or client may send a PADT (PPPoE Active Discovery Terminate) packet at anytime to indicate the session has been terminated. The PADT packet's SESSION-ID must be set to indicate which session is to be terminated. Once received a PADT, no further PPP packets (even normal PPP termination packets) are allowed to be sent using the specified session. A PPP peer should use the PPP protocol itself to terminate a PPPoE session, but can use the PADT packet to terminate the PPPoE session if PPP cannot be used.

## 6.3.1.6 PPPoE Server Settings

The Device support PPPoE server to allow LAN hosts acting as the PPPoE clients to dial up to the Device.

The Device provide rich PPPoE server features, which include PPPoE global settings, PPPoE account settings, PPPoE User Status, Export PPPoE Accounts, Import PPPoE Accounts and so on.

## 6.3.1.7 Global Settings



Enable PPPoE Server □

To make PPPoE server settings take effect, check to enable PPPoE server.

Mandatory PPPoE Authentication ○ Enable ● Disable

Exception Group None

Start IP Address * 0.0.0.0

Primary DNS Server * 0.0.0.0

Secondary DNS Server 0.0.0.0

You can find DNS server addresses in Start > Interface Status page.

Allow Users to Change Password □

PPP Authentication AUTO

Maximum Sessions * 120

**Figure 6-11 PPPoE Server Global Settings**

}

- **Enable PPPoE Server:** Select to enable PPPoE server.

- **Mandatory PPPoE Authentication:** Select the **Enable** checkbox to let the users access internet only after pass PPPoE authentication.

- **Exception Group:** Select the user group who do not need to pass PPPoE authentication also can access internet. You can configure the user group on **User Management** > **User Group** page.

- **Start IP Address:** Specify the starting IP address that is assigned by the PPPoE server.

- **Primary DNS Server:** Specify the IP address of the primary DNS server that is available to a PPPoE client.

- **Secondary DNS Server:** Specify the IP address of the secondary DNS server that is available to a PPPoE client.

- **Allow Users to Change Password:** Select to allow the PPPoE client to change the password themselves.

- **PPP Authentication:** Specify the PPP authentication mode by which the PPPoE server authenticates a PPPoE client. The available options are **PAP**, **CHAP** and **Auto**. In most cases, please leave the default value of **Auto**, which means that the Device will automatically choose **PAP** or **CHAP** to authenticate the PPPoE client.

- **Max. Sessions:** Specify the maximum number of PPPoE sessions that can be created on the Device. The maximum value of **Max. Sessions** depends on the specific product model.

⌖ **Note:**

The steps of PPPoE client changing password is as following:

1) Open the client and dialing with user name and password.

2) After dialing success, please login to page: http://192.168.1.1/poeUsers.asp (Note the IP address is LAN’s IP).

3) Enter the user name, old password, new password, confirmed password and click the **Save** button to save the changing.

4) Client could change password 5 times every day.

5) Administrator could configure daily routine notification on the **APP Control** > **Notification** page to inform users to change password.

**}**

## 6.3.1.8 Account Settings

### 6.3.1.8.1 PPPoE Account List

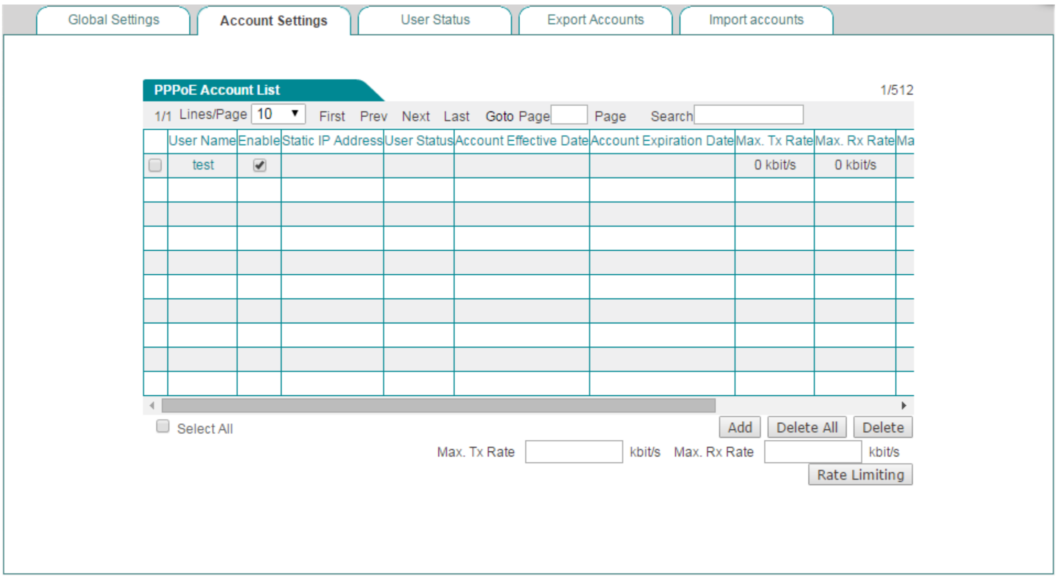
When you have configured some PPPoE accounts, you can view their configuration in the **PPPoE Account List**, including **User Name**, **Enable**, **Static IP Address**, **User Status** and so on.

- **Add a PPPoE Account:** Click the **Add** button to go to the setup page, and then configure it, lastly click the **Save** button.

- **Enable a PPPoE Account:** Select the **Enable** check box to enable the corresponding PPPoE account. If you want to disable the PPPoE account temporarily instead of deleting it, please click it to remove the check mark.

- **Edit a PPPoE Account:** Click the **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete PPPoE Account(s):** Select the leftmost check boxes of them, and then click the **Delete** button.



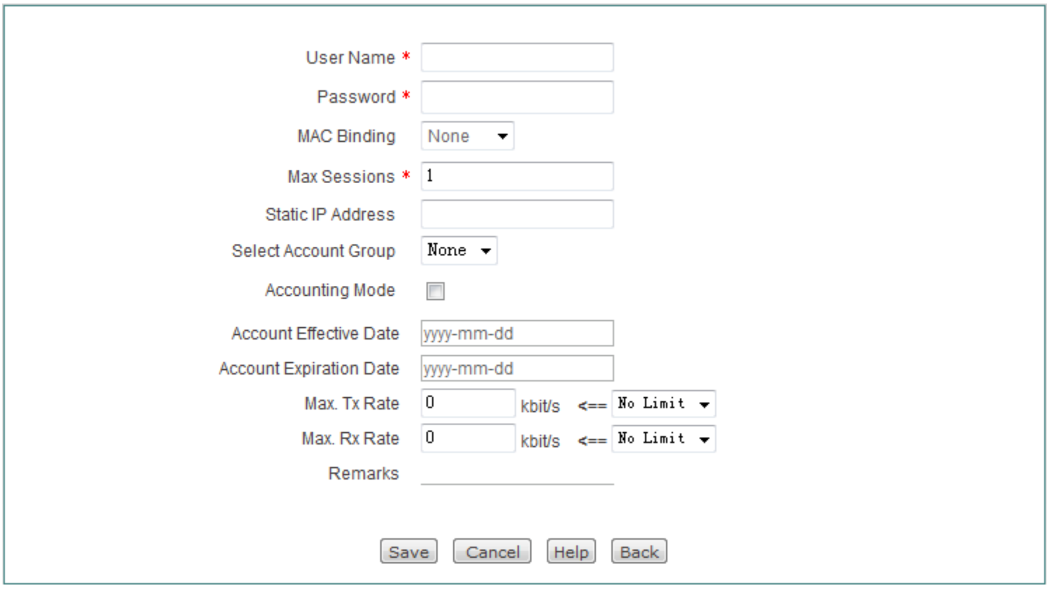
| | User Name | Enable | Static IP Address | User Status | Account Effective Date | Account Expiration Date | Max. Tx Rate | Max. Rx Rate | Ma |
|---|---|---|---|---|---|---|---|---|---|
| □ | test | ☑ | | | | | 0 kbit/s | 0 kbit/s | |

**Figure 6-12 PPPoE Account List**

### 6.3.1.8.2 PPPoE Account Settings

In the **PPPoE > Account Settings** page, you can configure PPPoE account related parameters, which include basic parameters, rate limit parameters and so on.

}



| | |
|---|---|
| User Name * | |
| Password * | |
| MAC Binding | None |
| Max Sessions * | 1 |
| Static IP Address | |
| Select Account Group | None |
| Accounting Mode | □ |
| Account Effective Date | yyyy-mm-dd |
| Account Expiration Date | yyyy-mm-dd |
| Max. Tx Rate | 0 kbit/s <== No Limit |
| Max. Rx Rate | 0 kbit/s <== No Limit |
| Remarks | |

**Figure 6-13 PPPoE Account Settings**

- **User Name:** Specify a unique user name of the PPPoE account. It should be between 1 and 31 characters long. The PPPoE server will use **User Name** and **Password** to identify the PPPoE client.

- **Password**: Specify the password of the PPPoE account.

- **MAC Binding:** Specify the type of PPPoE account and MAC address binding. The available options are **None**, **Auto** and **Manual**.

  - **None:** If selected, a PPPoE client with any MAC address can use the current PPPoE account to dial up.

  - **Auto:** If selected, the Device will automatically bind the PPPoE account to the MAC address of the user who uses this account to establish a PPPoE session firstly. After that only this user can use the account.

  - **Manual:** If selected, you can configure up to four MAC addresses that are bound to the account. Only the users with one of these MAC addresses can use the account.

- **MAC Address:** Specify the MAC address that is bound to the current PPPoE account. If you select **Manual** from the **MAC Binding** drop-down list, this parameter will be displayed. In this case, you should enter a MAC address that is bound to the account in the text box.

- **Max. Sessions:** Specify the maximum number of PPPoE sessions that can be created by using the current PPPoE account.

- **Static IP Address:** Specify a static IP address that is assigned to the user who uses the current PPPoE account. It must be a valid IP address in the range of address pool configured in the **PPPoE > Global Settings** page.

}

- **Select Account Group:** Add the account to the selected account group. The account group should be set on the **User Management** > **User Group** page.

- **Accounting Mode:** The Device support Account Billing of PPPoE Server. It offers account billing based on time. You can configure account expiration notice on the **APP Control** > **Notification** > **Account Expiration Notification** page.

- **Account Effective Date:** Select the day of account take effect.

- **Account Expiration Date:** Select the day of account expire.

- **Max. Tx Rate:** Specify the maximum upload bandwidth of a PPPoE dial-in user that uses the current PPPoE account.

- **Max Rx Rate:** Specify the maximum download bandwidth of a PPPoE dial-in user that uses the current PPPoE account.

- **Remarks:** Specify the description of the PPPoE account.

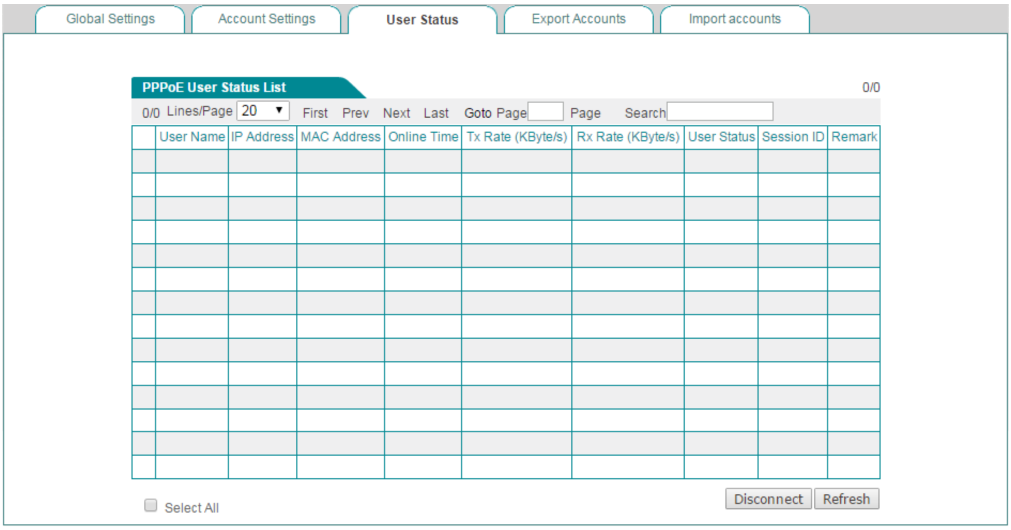
**Note:**

1) If you want to assign a static IP address to the user that uses a PPPoE account to establish a PPPoE session, you should enter the IP address in the**Static IP Address** text box, and should set the **Max. Sessions** to 1.

2) Fixed Rate Limiting is no effect to PPPoE account after you have configure Tx/Rx Rate.

### 6.3.1.9 User Status

In the **PPPoE > User Status** page, you can view the status and usage information of each online PPPoE dial-in user. If a PPPoE dial-in user has established the PPPoE session to the Device successfully, you can view the assigned IP address, MAC address, Rx Rate and Tx Rate of the user, online time and session ID of the PPPoE session.



PPPoE User Status List 0/0

0/0 Lines/Page 20

| | User Name | IP Address | MAC Address | Online Time | Tx Rate (KByte/s) | Rx Rate (KByte/s) | User Status | Session ID | Remark |
|---|---|---|---|---|---|---|---|---|---|

□ Select All

}

Figure 6-14 PPPoE User Status List

- **User Name:** Displays the PPPoE user name. The PPPoE dial-in user uses it to dial-up and establish the PPPoE session to the Device.
- **IP Address:** Displays the PPPoE dial-in user’s IP address that is assigned by the PPPoE server.
- **MAC Address:** Displays the PPPoE dial-in user’s MAC address.
- **Online Time:** Displays the elapsed time since the PPPoE session was established successfully.
- **Rx Rate:** Displays the real-time download rate (in kilobytes per second) of the PPPoE dial-in user.
- **Tx Rate:** Displays the real-time upload rate (in kilobytes per second) of the PPPoE dial-in user.
- **User Status:** Displays the PPPoE account status. If a PPPoE dial-in user has established the PPPoE session to the Device successfully with the PPPoE account, it displays Connected; Else, it displays Disconnected.
- **Session ID:** Displays the session ID of the PPPoE Session, which uniquely identifies a PPPoE session.
- **Remark:** Displays the description of the PPPoE user status.
- **Disconnect:** If you want to hang the established PPPoE session up manually, select the leftmost check box of this PPPoE session, and then click the **Disconnect** button.
- **Refresh:** Click to view the latest information in the list.

## 6.3.1.10 Export Accounts

The **PPPoE > Export Accounts** page provides PPPoE accounts export function to simplify operation. Click the Export Accounts button to export accounts in txt format.

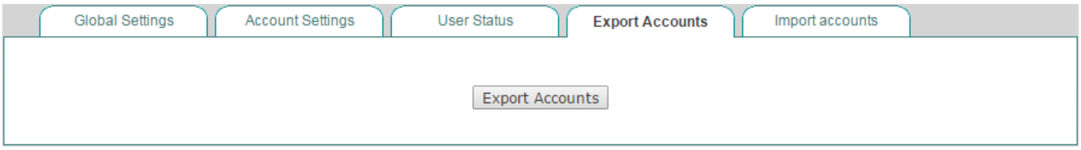
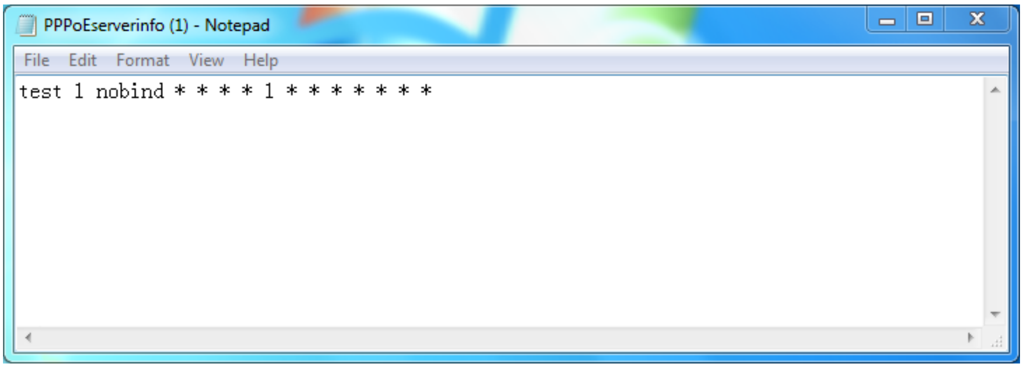


Figure 6-15 Export PPPoE accounts

}

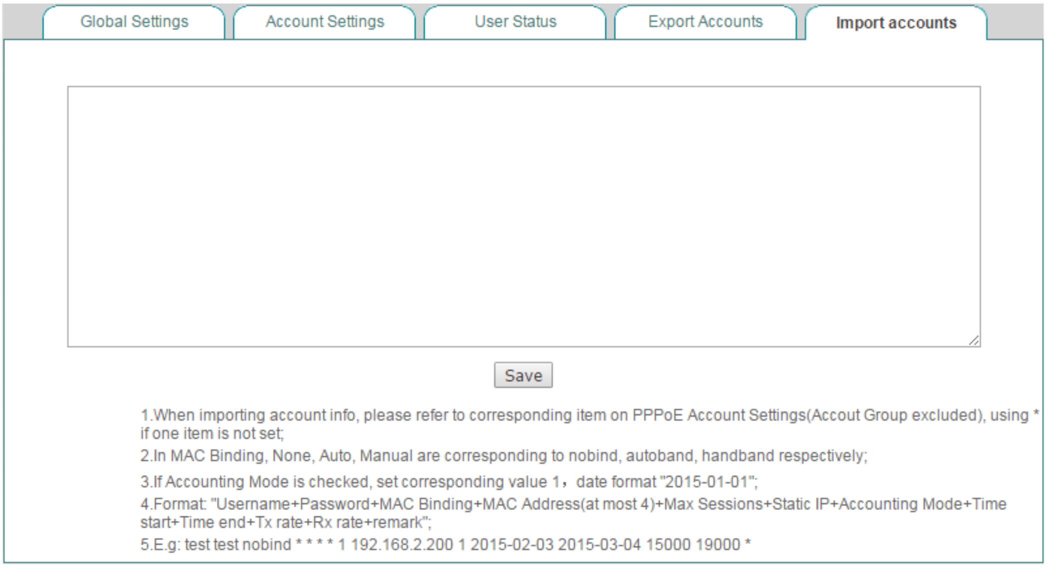


```
test 1 nobind * * * * 1 * * * * * * *
```

Figure 6-16 Export PPPoE accounts

### 6.3.1.11 Import Accounts

The **PPPoE > Import Accounts** page provides PPPoE accounts import function to simplify operation. When you want to create a great deal of PPPoE accounts, you can import them at a time in the page. You can edit them in Notepad, and then copy them to the **Import Accounts** list box; also you can directly enter them in the **Import Accounts** list box. The import contents are: User Name, Password, and Description of each PPPoE account, one PPPoE account per line; and the import format of a PPPoE account is: User Name**<Space>**Password**<Space>**Description**<Enter>**.



1.When importing account info, please refer to corresponding item on PPPoE Account Settings(Accout Group excluded), using * if one item is not set;

2.In MAC Binding, None, Auto, Manual are corresponding to nobind, autoband, handband respectively;

3.If Accounting Mode is checked, set corresponding value 1，date format "2015-01-01";

4.Format: "Username+Password+MAC Binding+MAC Address(at most 4)+Max Sessions+Static IP+Accounting Mode+Time start+Time end+Tx rate+Rx rate+remark";

5.E.g: test test nobind * * * * 1 192.168.2.200 1 2015-02-03 2015-03-04 15000 19000 *

Figure 6-17 Import PPPoE accounts

- **Save:** After you have entered the PPPoE accounts in the **Import Accounts** list box, click the **Save** button to save them to the Device, and then you can view them in the **PPPoE Account List**.

**Note:** To avoid unnecessary data loss due to computer crashes, you can copy the entered PPPoE accounts to a Notepad file in your local PC before saving them to the Device.

}

## 6.3.1.12 Example for PPPoE

### 1) Requirements

In this example, an organization's administrator wants the LAN users to act as the PPPoE clients to dial up to the Device. And it only allows the PPPoE dial-in users to access the Internet through the Device. The exception is the CEO with IP address **192.168.16.2**.

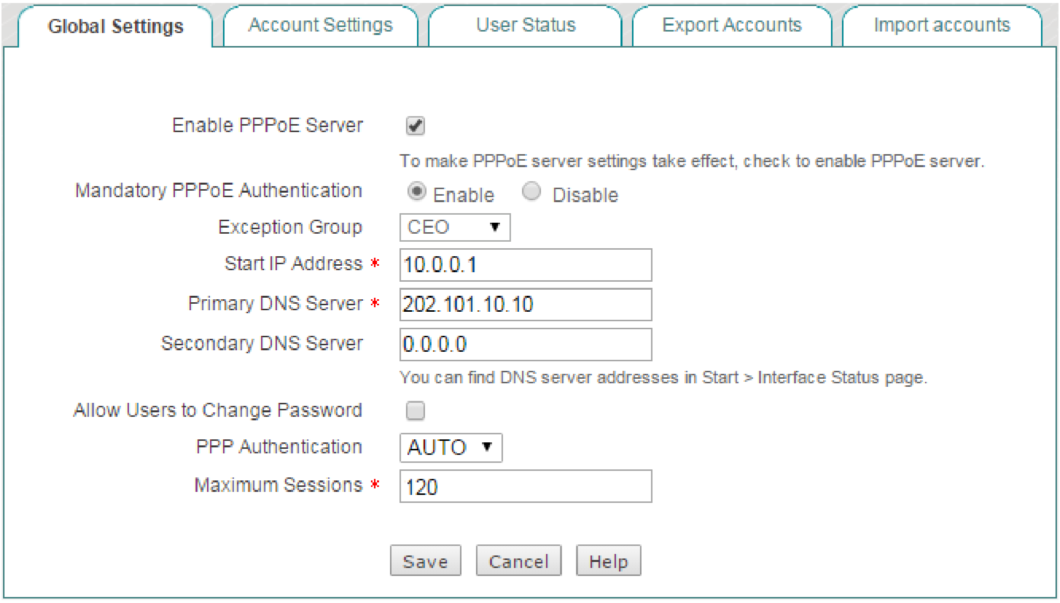
When acting as a PPPoE server, the Device dynamically will assign the IP addresses to the LAN users. The start IP address assigned to the dial-in user is 10.0.0.1, the primary DNS server IP address is 202.101.10.10, and the maximum number of PPPoE sessions that can be created on the Device is 100.

The administrator need to create two PPPoE accounts: one is universal account which is used by the normal employees, and its **Rx** and **Tx bandwidth** are both 512 Kbit/s, its **Max. Sessions** is 90; the other is advanced account which is used only for MAC address 0021859b4544 with a static IP address 10.0.0.50.

### 2) Configuration Procedure

#### (1) Configuring PPPoE Server Global Parameters

Go to the **PPPoE > Global Settings** page. Select the **Enable PPPoE Server** check box, select the **Mandatory PPPoE Authentication** check box, and select **CEO** from the **Exception Group** drop-down list. The **CEO** address group only includes one IP address: 192.168.16.2, which is configured in the **User Management > User Group** page. Enter **10.0.0.1** in the **Start IP Address**, enter **202.101.10.10** in the **Primary DNS Server**, and enter **100** in the **Max. Sessions** text box. Leave the default values for the other parameters. Then click the **Save** button to save the settings.



Enable PPPoE Server ☑

To make PPPoE server settings take effect, check to enable PPPoE server.

Mandatory PPPoE Authentication ● Enable ○ Disable

Exception Group CEO

Start IP Address * 10.0.0.1

Primary DNS Server * 202.101.10.10

Secondary DNS Server 0.0.0.0

You can find DNS server addresses in Start > Interface Status page.

Allow Users to Change Password □

PPP Authentication AUTO

Maximum Sessions * 120

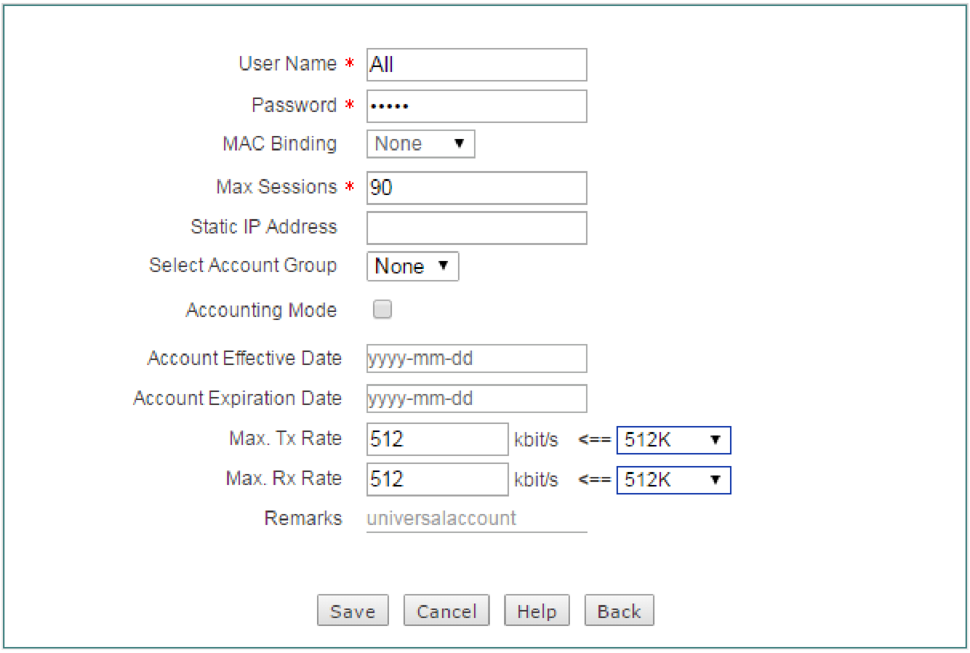
**Figure 6-18 PPPoE Server Global Settings - Example**

#### (2) Configuring PPPoE Accounts

}

**Step 1** Go to the **PPPoE > PPPoE Account > PPPoE Account Settings** page.

**Step 2** Creating the universal PPPoE Account whose user name is All. See the following figure, enter **All** in the **User Name**, enter **test** in the **Password**, enter **universalaccount** in the **Remarks**, enter **512** in the **Tx Bandwidth** and **Rx Bandwidth**, and enter **90** in the **Max. Sessions** text box. Leave the default values for the other parameters. Then click the **Save** button to save the settings.

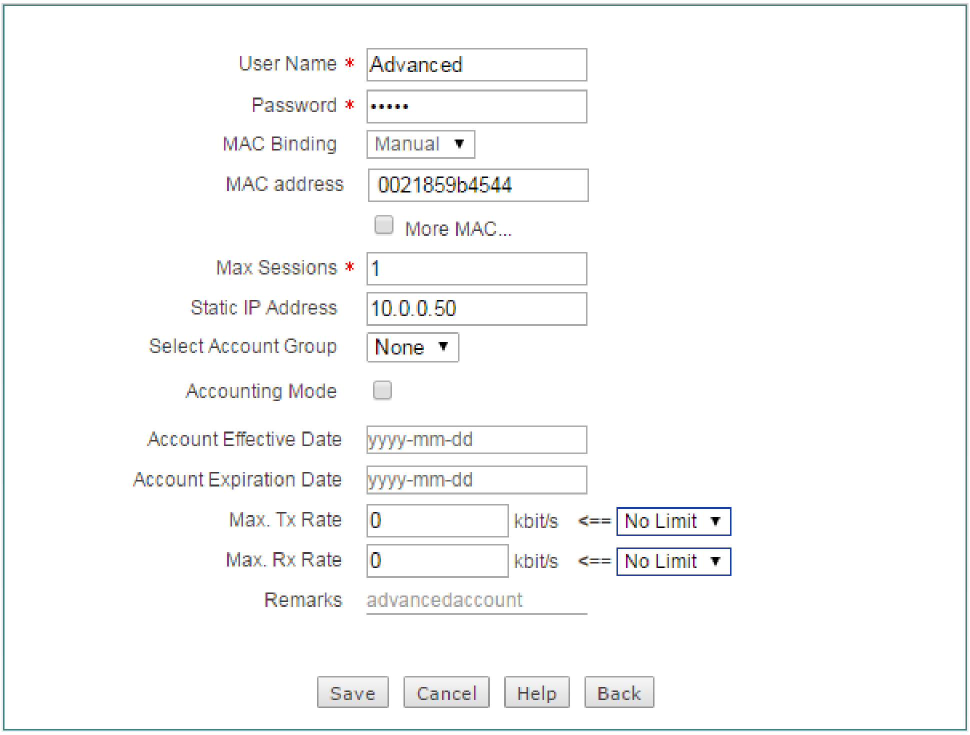


| | | | |
|---|---|---|---|
| User Name * | All | | |
| Password * | ••••• | | |
| MAC Binding | None ▼ | | |
| Max Sessions * | 90 | | |
| Static IP Address | | | |
| Select Account Group | None ▼ | | |
| Accounting Mode | □ | | |
| Account Effective Date | yyyy-mm-dd | | |
| Account Expiration Date | yyyy-mm-dd | | |
| Max. Tx Rate | 512 | kbit/s <== | 512K ▼ |
| Max. Rx Rate | 512 | kbit/s <== | 512K ▼ |
| Remarks | universalaccount | | |

**Figure 6-19 Configuring the Universal PPPoE Account - Example**

**Step 3** Creating the advanced PPPoE Account whose user name is Advanced. See the following figure, enter **Advanced** in the **User Name**, enter **test2** in the **Password**, enter **advanced account** in the **Remarks**, and enter **0021859b4544** in the **MAC Address**, enter **1** in the **Max. Sessions** text box, enter **10.0.0.50** in the **Static IP Address**. Leave the default values for the other parameters. Then click the **Save** button to save the settings.

}



User Name * Advanced

Password * •••••

MAC Binding Manual ▼

MAC address 0021859b4544

□ More MAC...

Max Sessions * 1

Static IP Address 10.0.0.50

Select Account Group None ▼

Accounting Mode □

Account Effective Date yyyy-mm-dd

Account Expiration Date yyyy-mm-dd

Max. Tx Rate 0 kbit/s <== No Limit ▼

Max. Rx Rate 0 kbit/s <== No Limit ▼

Remarks advancedaccount

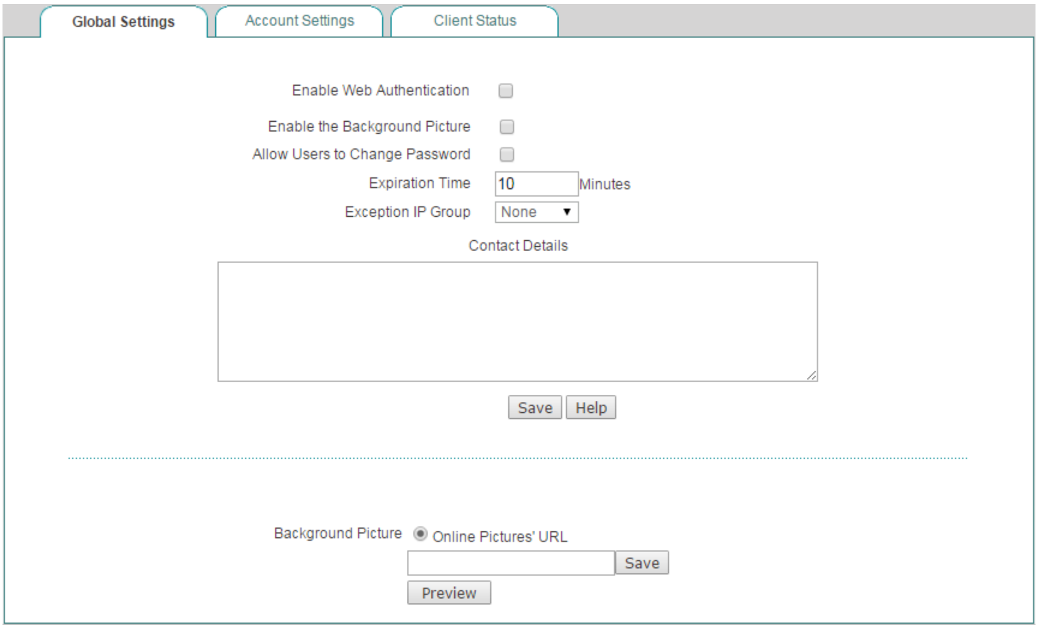
**Figure 6-20 Configuring the Advanced PPPoE Account - Example**

## 6.4 Web Authentication

The Device provide Web authentication feature. This new feature will enhance network security. If you enable the Web authentication on the Device, those non-PPPoE dial-in users cannot access the Internet through the Device unless they are authenticated successfully through Web browser.

}

### 6.4.1.1 Global Settings



Enable Web Authentication □

Enable the Background Picture □

Allow Users to Change Password □

Expiration Time 10 Minutes

Exception IP Group None

Contact Details

Background Picture ● Online Pictures' URL

Figure 6-21 Global Settings

- **Enable Web Authentication:** If selected, non-PPPoE dial-in users cannot access the Internet through the Device unless they are authenticated successfully.

- **Enable the Background Picture:** Select to enable setting a background picture on the web authentication page.

- **Allow Users to Change Password:** Select to enable users change password themselves. You can set the user group on **User Management** > **User Group** page.

- **Expiration Time:** Specify how long the user will be log off, if there is no traffic after the user logging in.

- **Exception IP Group:** Select the user groups that don’t need web authentication also can access internet.

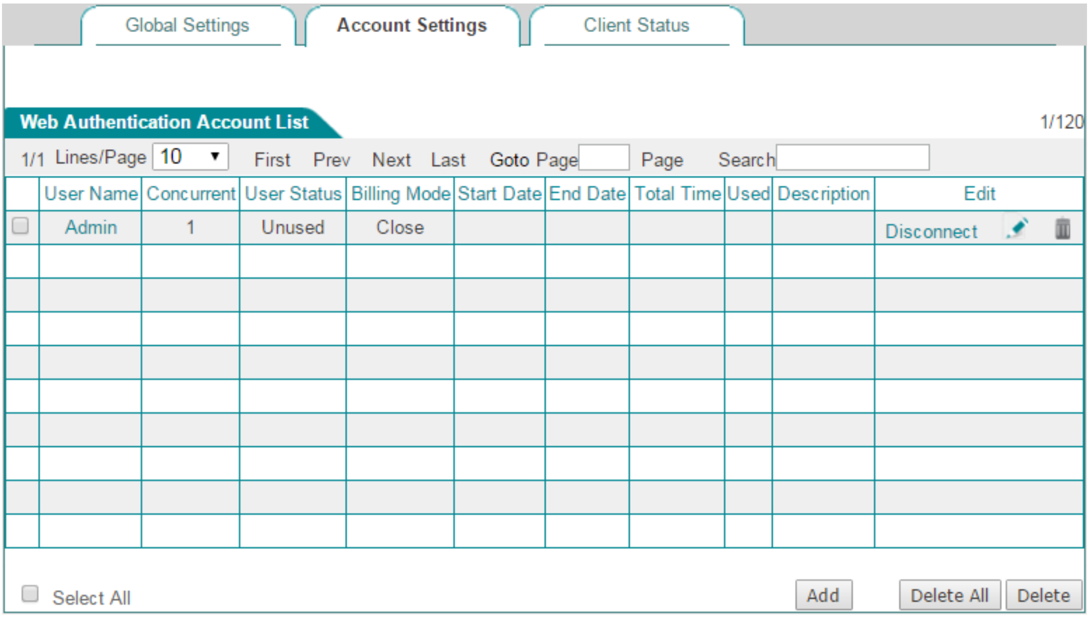
- **Contact Details:** Enter the contact information you want to put at the below web authentication page.

- **Background Picture:** Paste the background picture’s URL on the text box and click the **Save** button to save the settings. You can click the Preview button to preview the web authentication page.

### 6.4.1.2 Account Settings

All the web authentication account you have set will be displayed on this page.

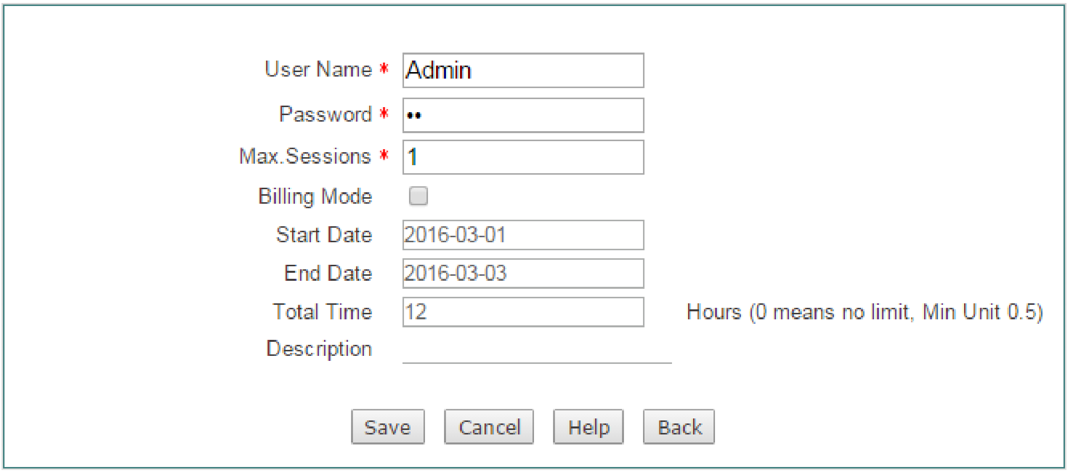
}



| | User Name | Concurrent | User Status | Billing Mode | Start Date | End Date | Total Time | Used | Description | Edit |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Admin | 1 | Unused | Close | | | | | | Disconnect |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

**Figure 6-22 Web Authentication Account List**

Click the **Add** button on the Figure 9-22 to go to setup page, and then configure it, lastly click the **Save** button.



User Name * Admin

Password * ••

Max.Sessions * 1

Billing Mode □

Start Date 2016-03-01

End Date 2016-03-03

Total Time 12 Hours (0 means no limit, Min Unit 0.5)

Description

**Figure 6-23 Web Authentication Account Settings**

- **User Name:** Specify a unique user name of the web authentication account. It should be between 1 and 31 characters long. The Device will use the **User Name** and **Password** to authenticate a user.
- **Password**: Specify the password of the web authentication account.
- **Billing Mode**: Select the check to allow billing of Web Authentication based on time.
- **Start Date:** Select the day of account take effect.

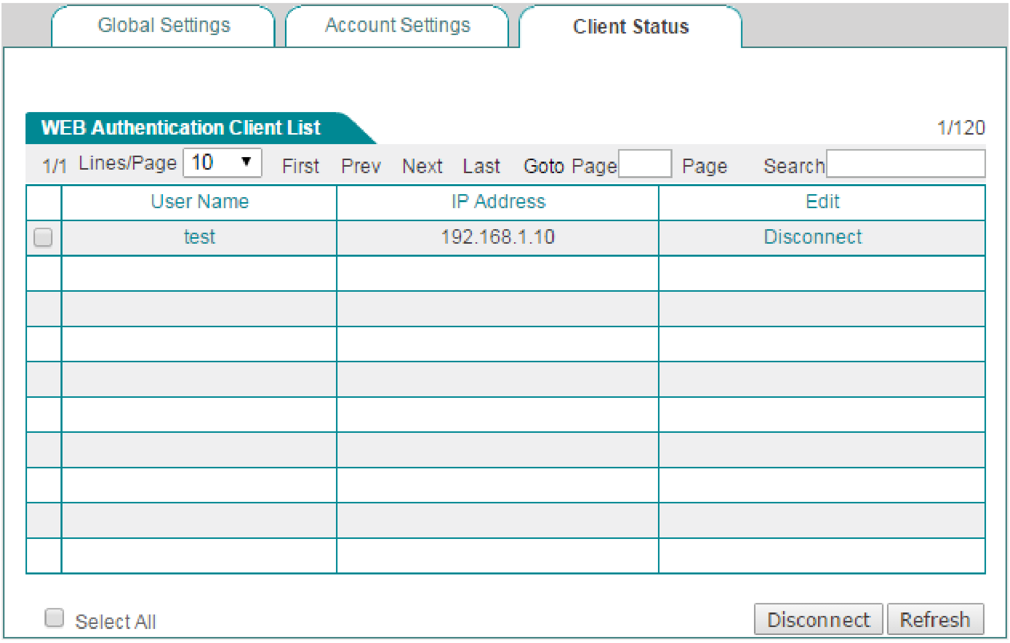
}

- **End Date:** Select the day of account expire.
- **Total Time:** Enter the total time for this account take effect.
- **Description:** Specify the description of the web authentication account.

### 6.4.1.3 Client Status

On the **Web Authentication > Client Status** page, you can view the current status of the web authentication accounts which have been used.

Select the leftmost checkbox of the users, and then click the **Disconnect** button to let the users log off manually.



| | User Name | IP Address | Edit |
|---|---|---|---|
| □ | test | 192.168.1.10 | Disconnect |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Figure 6-24 Web Authentication Client Status**

### 6.4.1.4 The steps for using Web Authentication

If you want to use web authentication for a non-PPPoE dial-in user, do the following:

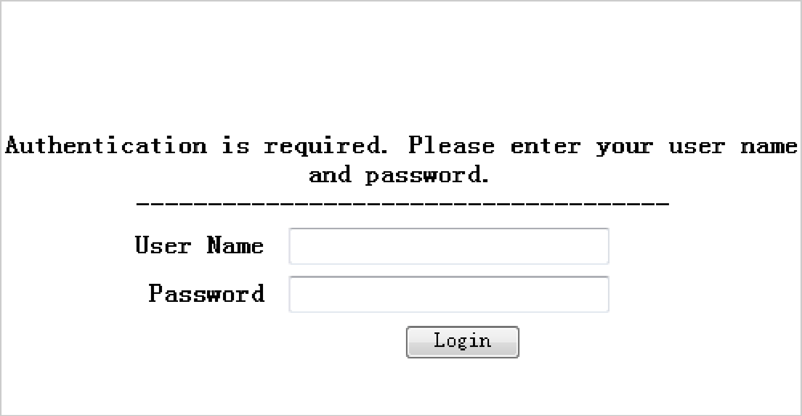
**Step 1** Go to the **User Management** > **Web Authentication** > **Global Settings** page, and then select the **Enable Web Authentication** checkbox and **Allow Users to Change Password** checkbox.

**Step 2** Go to **User Management > Web Authentication > Account Settings** page to configure a new web authentication user account, and then click the **Save** button to save the settings.

**Step 3** Launch a web browser, enter an Internet domain name or IP address in the address bar, and then press **<Enter>**, the Device will automatically pop up

}

an authentication login page, see the figure as following.



Authentication is required. Please enter your user name and password.

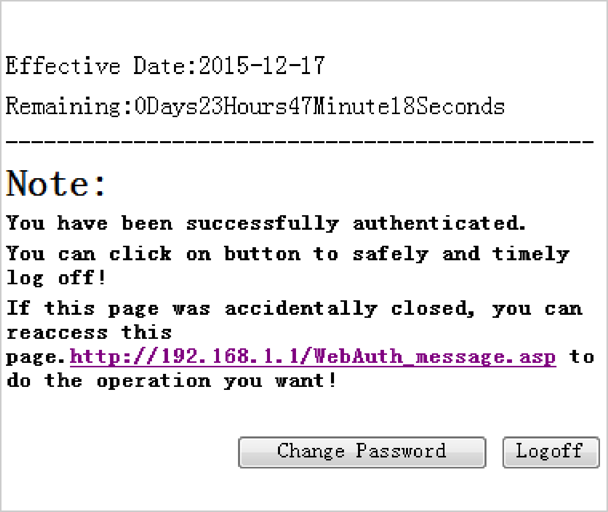
----------------------------------------

User Name

Password

Figure 6-25 Web Authentication Login Page

**Step 4** Enter the correct user name and password in the text boxes, and then click the **Save** button, the system will pop up a prompt page.



Effective Date:2015-12-17

Remaining:0Days23Hours47Minute18Seconds

--------------------------------------------

Note:

You have been successfully authenticated.

You can click on button to safely and timely log off!

If this page was accidentally closed, you can reaccess this page.http://192.168.1.1/WebAuth_message.asp to do the operation you want!

Figure 6-26 Web Authentication Prompt Page

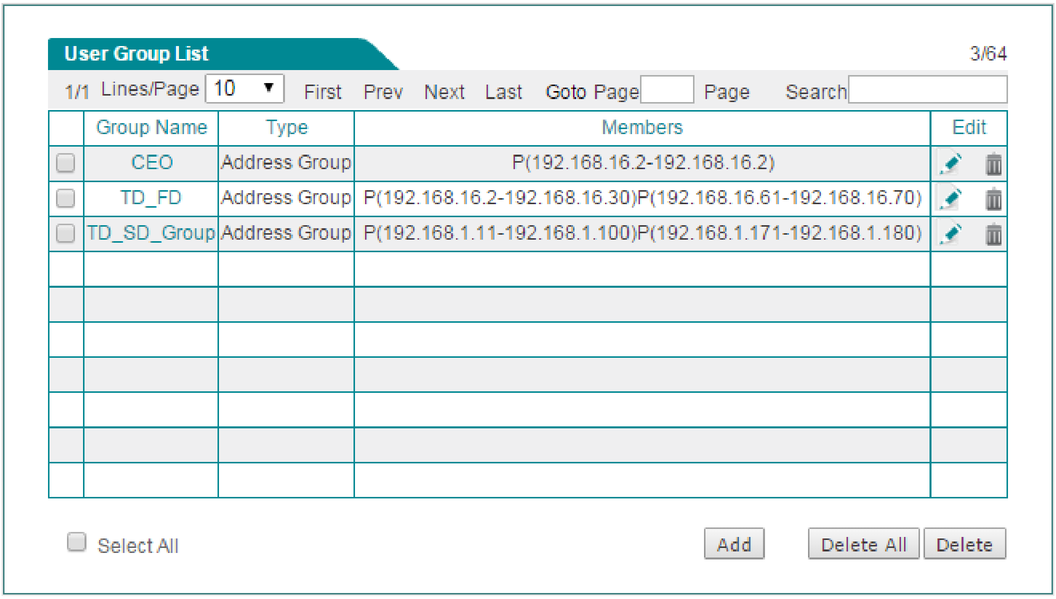
## 6.5 User Group

This section describes **User Management > User Group** page. You can group users that have similar needs. There are two types of groups: Address Group and Account Group.

### 1) User Group List

In **User Group List**, you can add, view, modify and delete the user groups.

}



User Group List 3/64

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

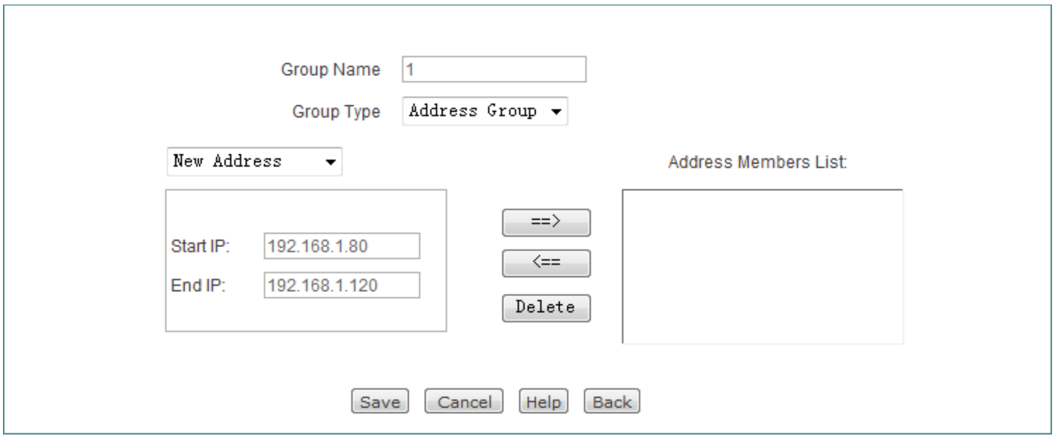
| □ | Group Name | Type | Members | Edit |
|---|---|---|---|---|
| □ | CEO | Address Group | P(192.168.16.2-192.168.16.2) | ✎ 🗑 |
| □ | TD_FD | Address Group | P(192.168.16.2-192.168.16.30)P(192.168.16.61-192.168.16.70) | ✎ 🗑 |
| □ | TD_SD_Group | Address Group | P(192.168.1.11-192.168.1.100)P(192.168.1.171-192.168.1.180) | ✎ 🗑 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

□ Select All

**Figure 6-27 User Group List**

## 2) User Group Settings

To add a new user group, go to **User Management > User Group** page, next click **Add** to go to **User Group Settings** page, and then configure it, lastly click **Save**.



Group Name: 1

Group Type: Address Group ▼

New Address ▼

Start IP: 192.168.1.80

End IP: 192.168.1.120

Address Members List:

**Figure 6-28 User Group Settings**

- **Group Name:** Specify the unique name for the user group.

- **Group Type:** Select the type of the user group, Address Group or Account Group.

- **Note:** The user groups cannot be nested deeper than 2. For example, if the address group A contains the address group B, then the address group A cannot be added to any other address group.

}

# Chapter 7. App Control Menu

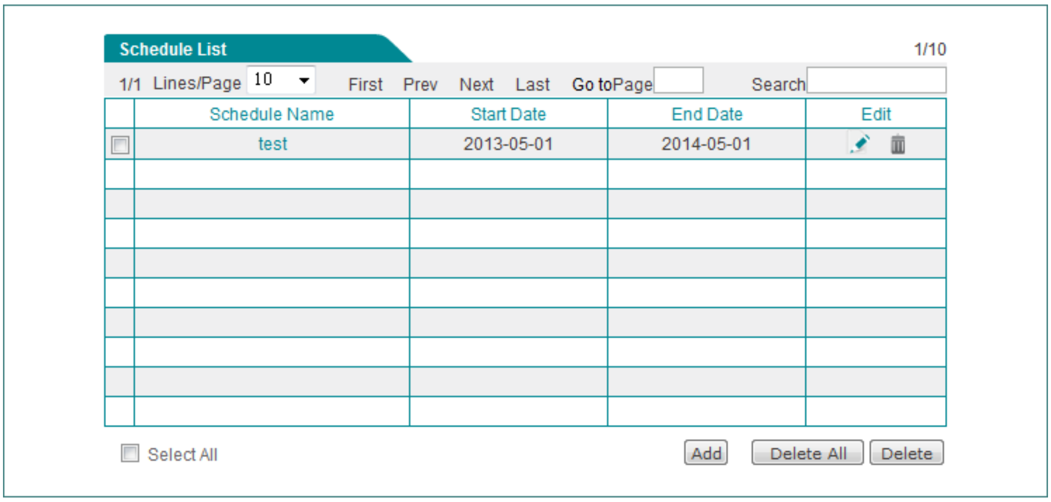
This chapter describes how to configure schedule, application control, QQ whitelist, MSN whitelist, TradeManager, notification, application audit, and policy database.

## 7.1 Schedule

This section describes **APP Control > Schedule** page, you can configure and view schedules. A schedule consists of a start date, an end date, and optional time periods.

### 1) Schedule List

In **Schedule List**, you can add, view, modify and delete schedules.



Schedule List 1/10

1/1 Lines/Page 10 First Prev Next Last Go toPage Search

| | Schedule Name | Start Date | End Date | Edit |
|---|---|---|---|---|
| □ | test | 2013-05-01 | 2014-05-01 | ✎ 🗑 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

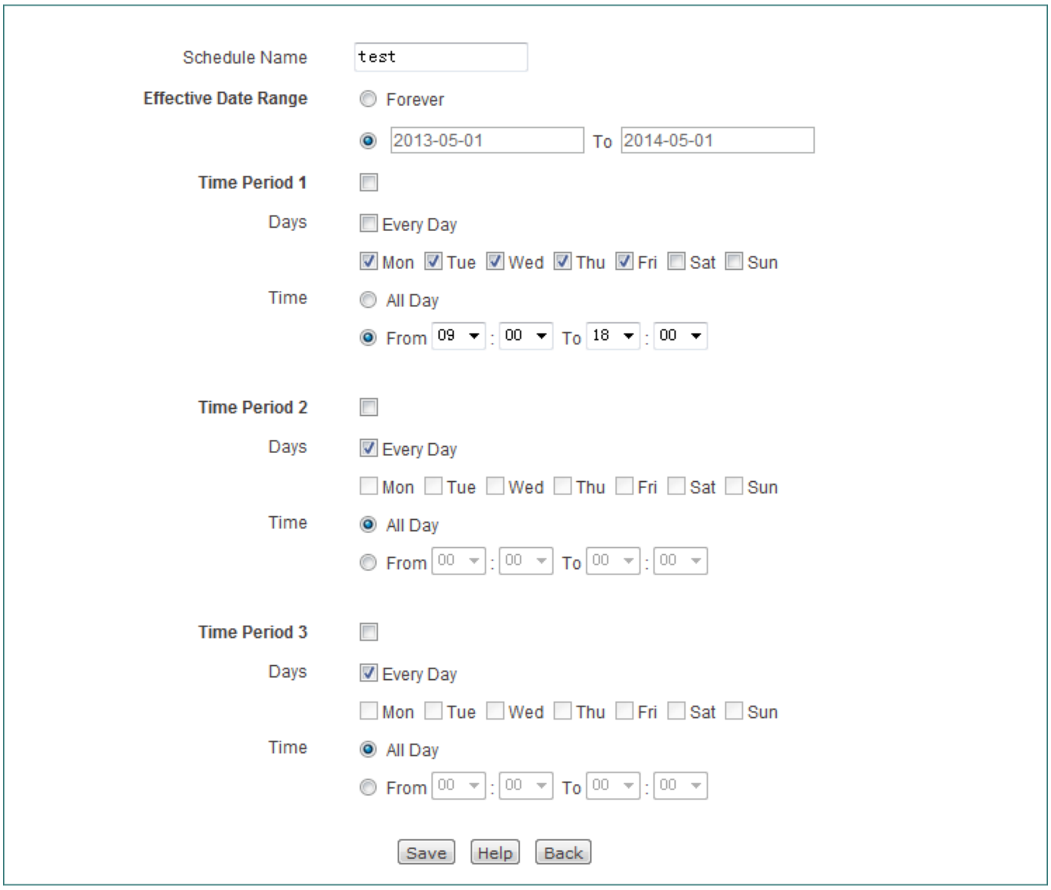
□ Select All

**Figure 7-1 Schedule List**

### 2) Schedule Settings

To add a new schedule entry, go to **App Control > Schedule** page, next click **Add** to go to **Schedule Settings** page, and then configure it, lastly click **Save**.

}



| | |
|---|---|
| Schedule Name | test |
| Effective Date Range | ○ Forever |
| | ● 2013-05-01 To 2014-05-01 |
| Time Period 1 | □ |
| Days | □ Every Day |
| | ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun |
| Time | ○ All Day |
| | ● From 09 : 00 To 18 : 00 |
| Time Period 2 | □ |
| Days | ☑ Every Day |
| | □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun |
| Time | ● All Day |
| | ○ From 00 : 00 To 00 : 00 |
| Time Period 3 | □ |
| Days | ☑ Every Day |
| | □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun |
| Time | ● All Day |
| | ○ From 00 : 00 To 00 : 00 |

**Figure 7-2 Schedule Settings**

- **Schedule Name:** Specify a unique name for the schedule.

- **Effective Date Range:** Specify the effective date range for the schedule.

- **Time Period 1** ~ **Time Period 3:** Specify further constraints of active time within the specified date range.

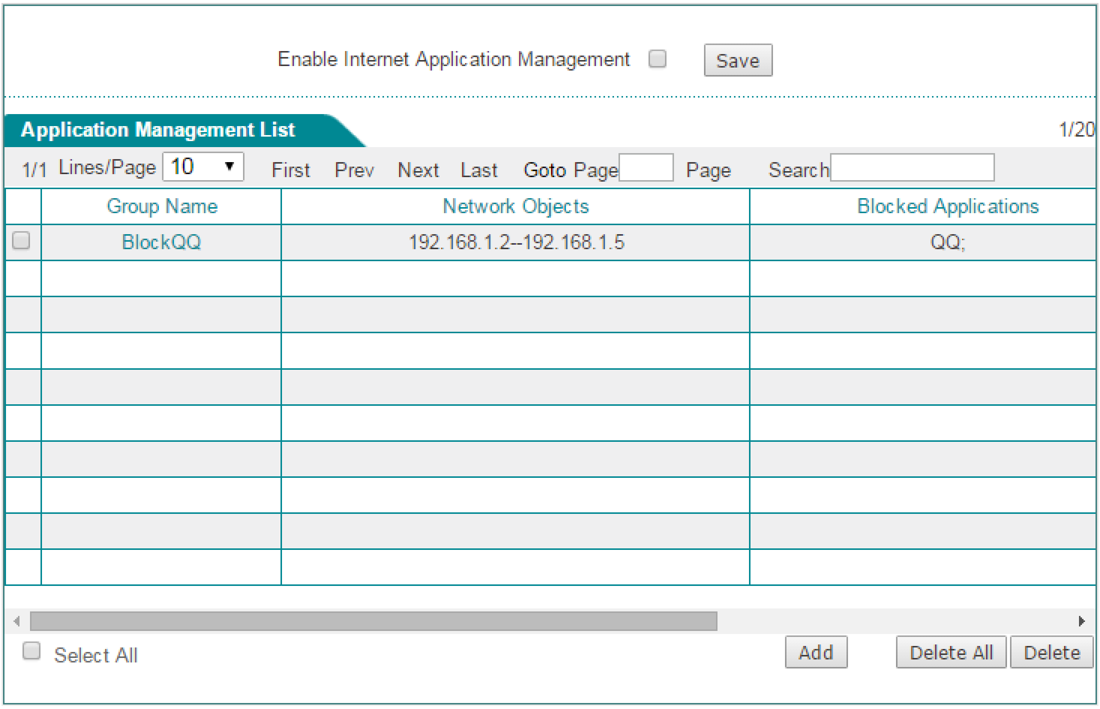
## 7.2 Application Control

This section describes **APP Control > Application Control** page, you can configure and view application management list. An application control entry consists of a date, and application.

### 1) Application Management List

In **App Control> Application Control** page, you can enable or disable Internet application management, and you can add, view, modify, and delete Internet application management policies in **Application Management List**.

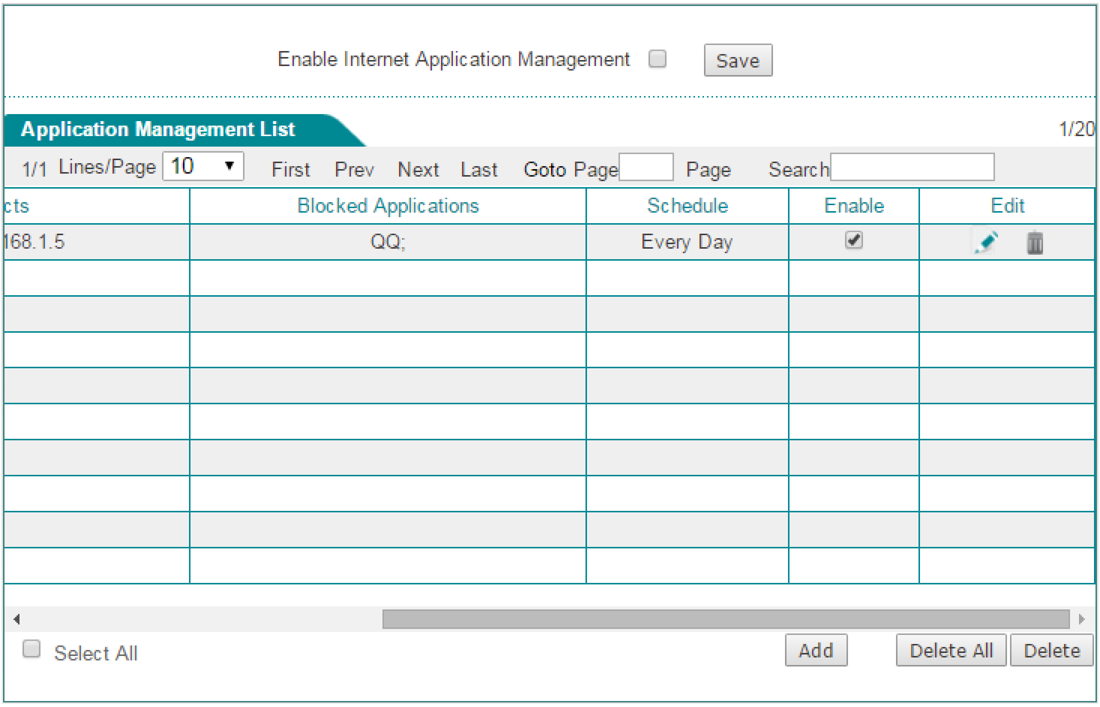
}



Enable Internet Application Management □ Save
Application Management List
1/20
1/1 Lines/Page 10 ▾ First Prev Next Last Goto Page Page Search
□ Select All
Add
Delete All
Delete

| | Group Name | Network Objects | Blocked Applications |
|---|---|---|---|
| □ | BlockQQ | 192.168.1.2--192.168.1.5 | QQ; |

**Figure 7-3 Application Management List**



Enable Internet Application Management □ Save
Application Management List
1/20
1/1 Lines/Page 10 ▾ First Prev Next Last Goto Page Page Search
□ Select All
Add
Delete All
Delete

| cts | Blocked Applications | Schedule | Enable | Edit |
|---|---|---|---|---|
| 168.1.5 | QQ; | Every Day | ☑ | ✎ 🗑 |

**Figure 7-4 Application Management List (continued)**

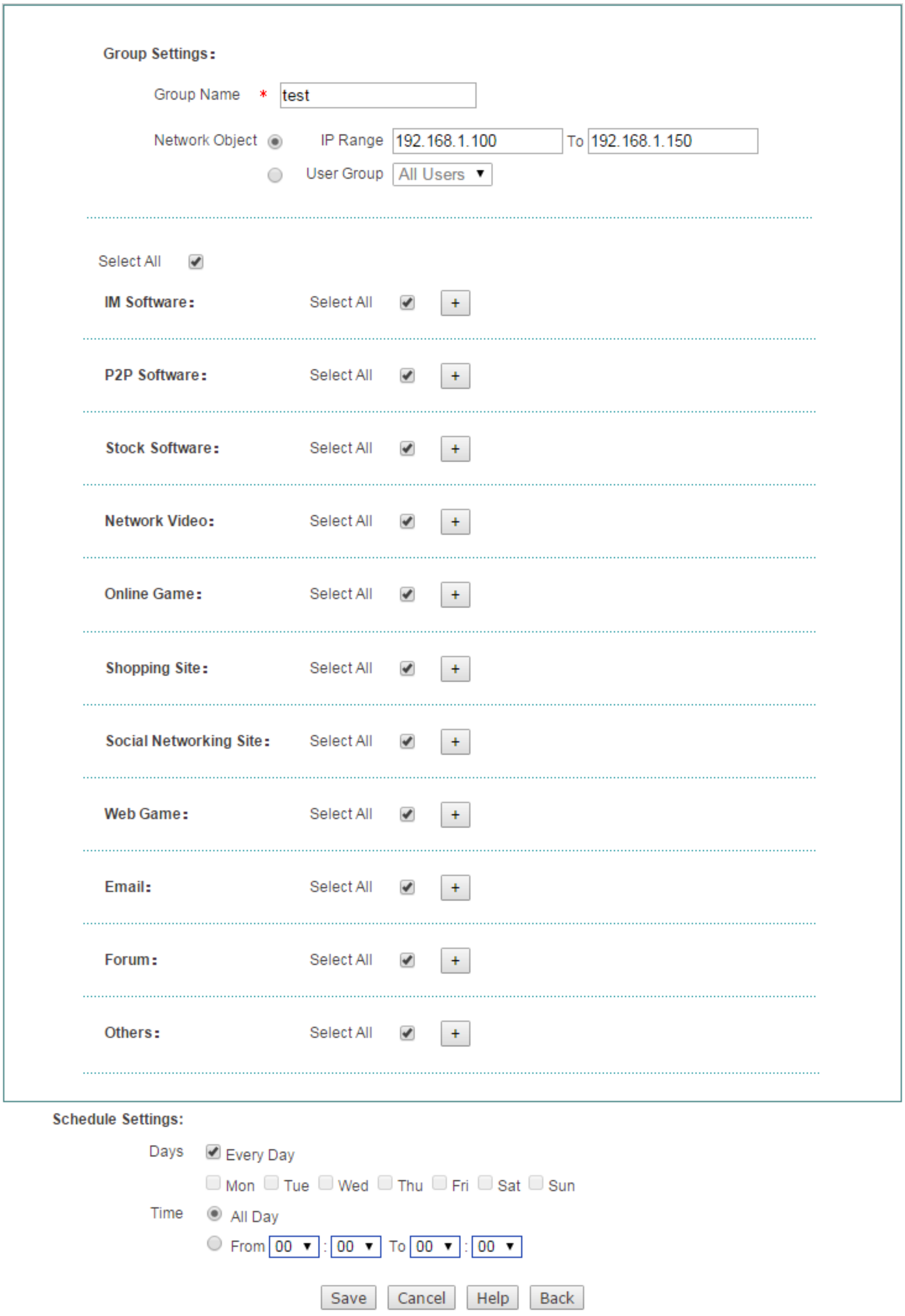
- **Enable Internet Application Management:** Select the check box to enable Internet application management.

**Notes:** To use this feature, you need to enable application recognition in **User Management > User Status** page.

}

## 2) Internet Application Management Settings

To add a new application management policy, go to **App Control > Application Control** page, next click **Add** to go to **Internet Application Management Settings** page, and then configure it, lastly click **Save**.



Group Settings:

Group Name * test

Network Object ● IP Range 192.168.1.100 To 192.168.1.150

○ User Group All Users ▼

Select All ☑

IM Software: Select All ☑ +

P2P Software: Select All ☑ +

Stock Software: Select All ☑ +

Network Video: Select All ☑ +

Online Game: Select All ☑ +

Shopping Site: Select All ☑ +

Social Networking Site: Select All ☑ +

Web Game: Select All ☑ +

Email: Select All ☑ +

Forum: Select All ☑ +

Others: Select All ☑ +

Schedule Settings:

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

**Figure 7-5 Internet Application Management Settings**

- **Group Name:** Enter a unique name for the group to which the Internet application management policy applies.

}

- **Network Object:** Select the members of the group. You can select the **IP Range** button to specify a range of IP addresses, or select the **User Group** button to select a user group. The members in the group are subject to the Internet application management policy.

- **IM Software, P2P Software, Block Stock Software, Network Video, Online Game, Shopping Site, Social Networking Site, Web Game, Email, Forum and Others**: Select the applications or services that you want to block under each category.

- **Schedule Settings:** Select the days and times when the Internet application management policy is in effect. By default, the policy is always in effect.

**Note:**

If a function option in **Application Control** page doesn't have the desired effect, please go to **App Control > Policy Database** page to check whether the corresponding policy is the latest. See **Section10.8 Policy Database** for more information about how to update policy.

### 3) Example for Application Control

### Requirements

In this example, a company has four departments:

- Technology Department: 192.168.1.11~192.168.1.100
- Customer Service Department: 192.168.1.101~192.168.1.140
- Sales Department: 192.168.1.141~192.168.1.170
- Financial Department: 192.168.1.171~192.168.1.180

Now the company wants to manage employee online application. It is required that all the Internet applications provided in **Internet Application Management Settings** page are blocked during working hours (Monday to Friday, 09:00 to 18:00), and permitted at other times including weekends. But there are two exceptions:

- The CEO and vice CEO can access the Internet without any restrictions. Their IP addresses are 192.168.16.5 and 192.168.16.9 respectively.
- The Customer Service and Sales Departments' employees need to use IM applications to communicate with customers during working hours.

### Analysis

We need to create two Internet application management policies to meet the requirements:

}

- Policy 1: It is used to allow the Customer Service and Sales Departments' employees to use IM applications, and block all other applications during working hours.

- Policy 2: It is used to block the Technology and Financial Departments' employees from accessing all the Internet applications during working hours.

## Configuration Procedure

### (1) Adding Policy 1

**Step 1** Go to **App Control > Application Control** page, and click **Add** to go to **Internet Application Management Settings** page.

**Step 2** Make the following settings.

- Enter **CSD_SD** in the **Group Name** text box.

- Select the **IP Range** radio button, and enter **192.168.1.101** and **192.168.1.170** in the two text boxes.

- Select the first **Select All** check box in the page, and then clear the **Select All** check box next to **IM Software**.

- In the **Schedule Settings** section, clear the **Every Day** check box, and select the **Mon**, **Tue**, **Wed**, **Thu** and **Fri** check boxes. Next, choose **09:00** and **18:00** as the daily start time and end time.

**Step 3** Click the **Save** button to add this policy to Application Management List.

### (2) Adding Policy 2

**Step 1** Go to **User Management > User Group** to add a user group for the Customer Service and Sales Departments' employees: **Group Name** is **TD_SD_Group**, **Group Type** is **Address Group**, and it contains two IP address ranges: from 192.168.1.11 to 192.168.1.100, and from 192.168.1.171 to 192.168.1.180.

**Step 2** Go to **App Control > Application Control** page, and click **Add** to go to **Internet Application Management Settings** page.

**Step 4** Make the following settings.

- Enter **TD_SD** in the **Group Name** text box.

- Select the **User Group** radio button, and select **TD_SD_Group** from the drop-down list.

**}**

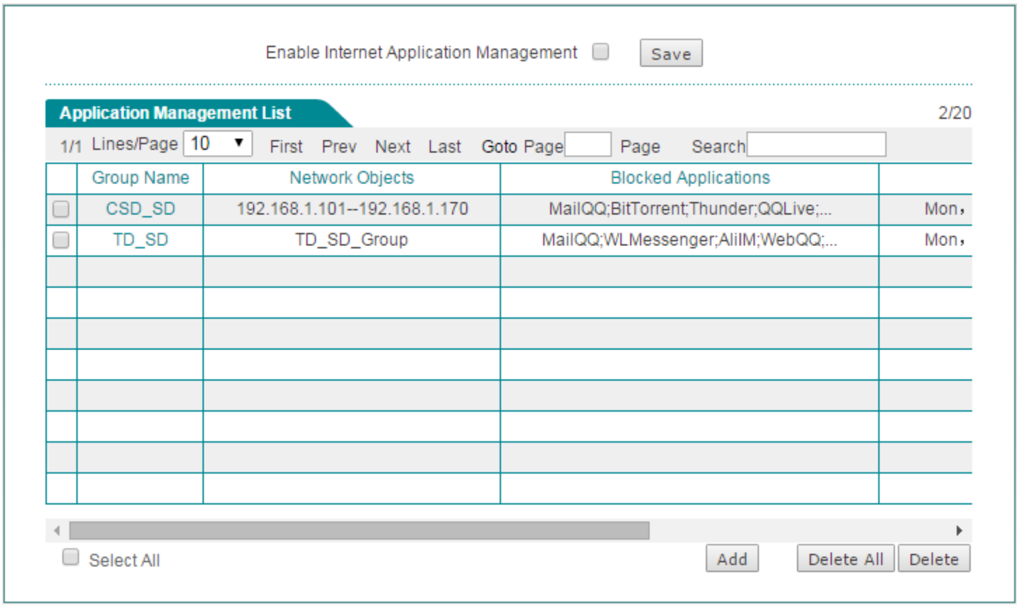
- Select the first **Select All** check box in the page.
- In the **Schedule Settings** section, do the same as the policy 1.

**Step 5** Click the **Save** button to add this policy to Application Management List.

### (3) Enabling Internet Application Management

Lastly, you need to enable Internet application management to make the policies take effect.

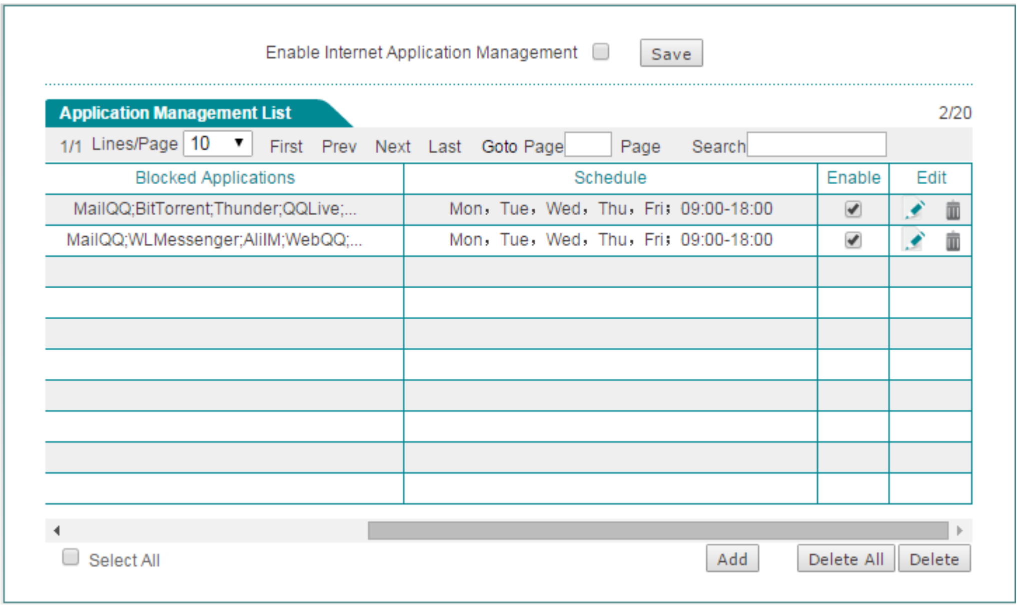
The configuration is now complete. You can veiw the two policies in **Application Management List**.


Enable Internet Application Management □
Save
Application Management List
2/20
1/1 Lines/Page 10
First Prev Next Last Goto Page Page Search
□ Select All
Add
Delete All
Delete

| | Group Name | Network Objects | Blocked Applications | |
|---|---|---|---|---|
| □ | CSD_SD | 192.168.1.101--192.168.1.170 | MailQQ;BitTorrent;Thunder;QQLive;... | Mon, |
| □ | TD_SD | TD_SD_Group | MailQQ;WLMessenger;AliIM;WebQQ;... | Mon, |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Figure 7-6 Internet Application Management List – Example**

}



Enable Internet Application Management ☐ Save

Application Management List 2/20

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

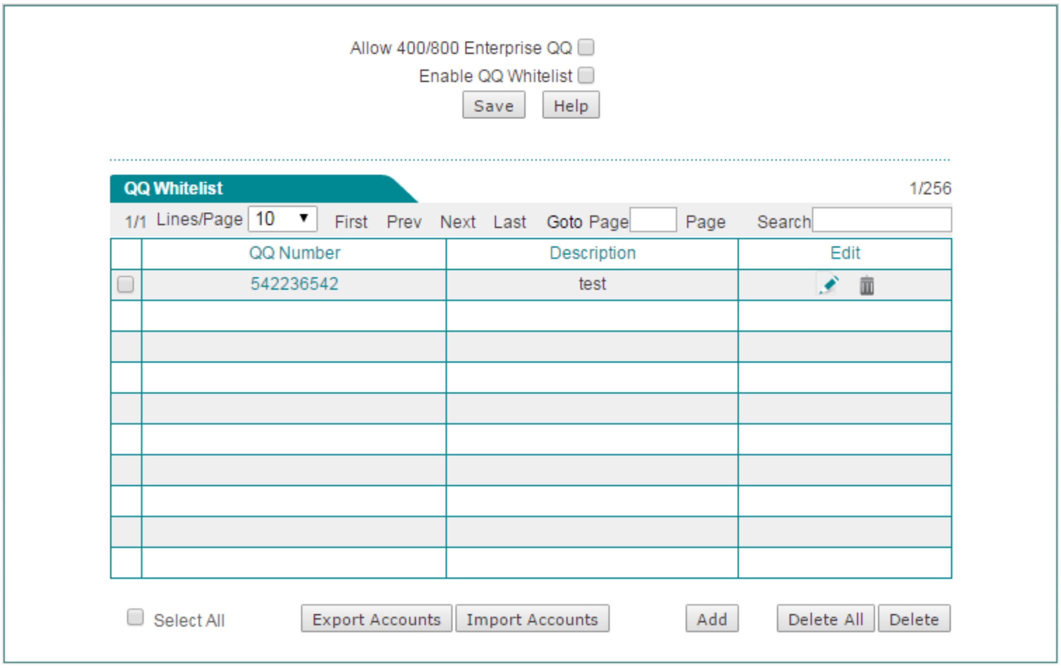
| Blocked Applications | Schedule | Enable | Edit |
|---|---|---|---|
| MailQQ;BitTorrent;Thunder;QQLive;... | Mon，Tue，Wed，Thu，Fri；09:00-18:00 | ☑ | ✎ 🗑 |
| MailQQ;WLMessenger;AliIM;WebQQ;... | Mon，Tue，Wed，Thu，Fri；09:00-18:00 | ☑ | ✎ 🗑 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

☐ Select All Add Delete All Delete

**Figure 7-7 Internet Application Management List – Example (continued)**

## 7.3 QQ Whitelist

This section describes **App Control > QQ Whitelist** page. This feature allows you to add a list of QQ numbers that are exempt from the Internet application management policies (set in **App Control > Application Control** page).



Allow 400/800 Enterprise QQ ☐

Enable QQ Whitelist ☐

Save Help

QQ Whitelist 1/256

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | QQ Number | Description | Edit |
|---|---|---|---|
| ☐ | 542236542 | test | ✎ 🗑 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

☐ Select All Export Accounts Import Accounts Add Delete All Delete

**Figure 7-8 QQ Whitelist**

}

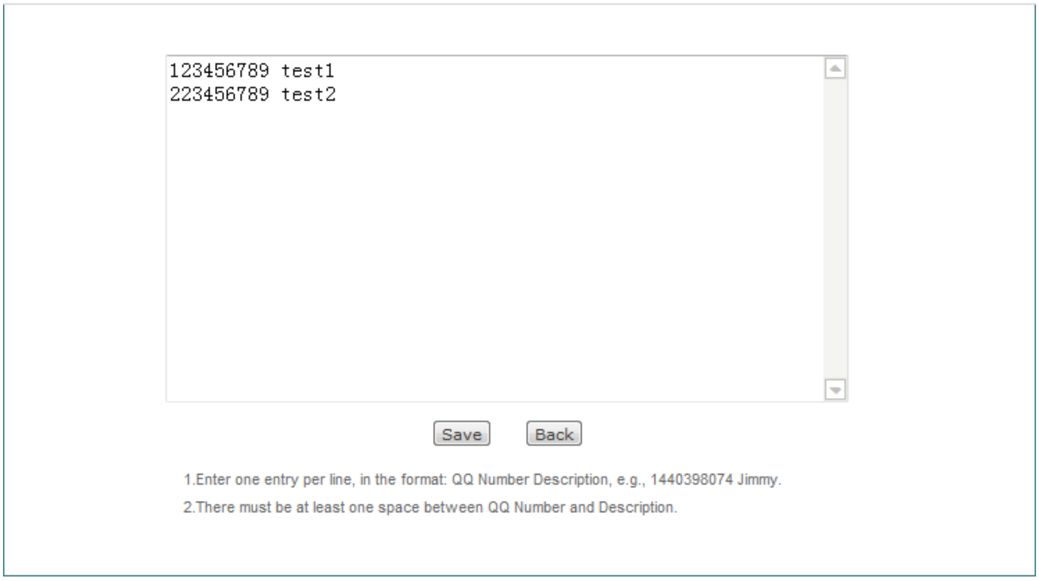
- **Allow 400/800 Enterprise QQ:** Select to allow 400/800 enterprise QQ. If selected, 400/800 enterprise QQ numbers are exempt from the Internet application management policies.

- **Enable QQ Whitelist**: Select to enbale QQ whitelist. If enabled, the QQ numbers in **QQ Whitelist** are exempt from the Internet application management policies.

- **Add:** To add a new QQ number, click **Add** to go to **QQ Whitelist Settings** page, and then configure it, lastly click **Save**.

- **Export Accounts:** You can click **Export Accounts** export all QQ numbers with description to a text file.

- **Import Accounts:** To add multiple QQ numbers at once, click **Import Accounts** to go to **Import QQ Numbers** page, and then enter them in the text box, lastly click **Save**. Enter one entry per line in this format: **QQ Number** <Space> **Description**, e.g., 1440398074 Jimmy. Be sure to leave at least one space between QQ Number and Description.



```
123456789 test1
223456789 test2
```

1.Enter one entry per line, in the format: QQ Number Description, e.g., 1440398074 Jimmy.

2.There must be at least one space between QQ Number and Description.

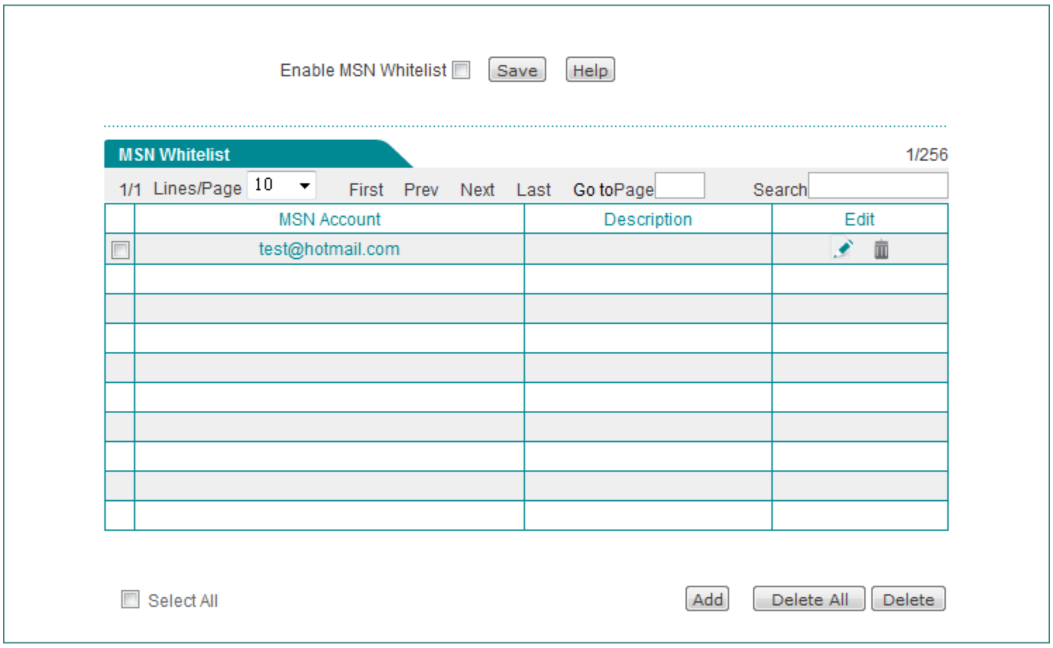
**Figure 7-9 Import QQ Numbers**

**Note:** The maximum QQ number that can be entered is 4294967295.

## 7.4 MSN Whitelist

This section describes **App Control > MSN Whitelist** page. This feature allows you to add a list of MSN accounts that are exempt from the Internet application management policies (set in **App Control > Application Control** page).

}



Enable MSN Whitelist □

MSN Whitelist 1/256

1/1 Lines/Page 10 Go toPage Search

| | MSN Account | Description | Edit |
|---|---|---|---|
| □ | test@hotmail.com | | ✎ 🗑 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

□ Select All

**Figure 7-10 MSN Whitelist**

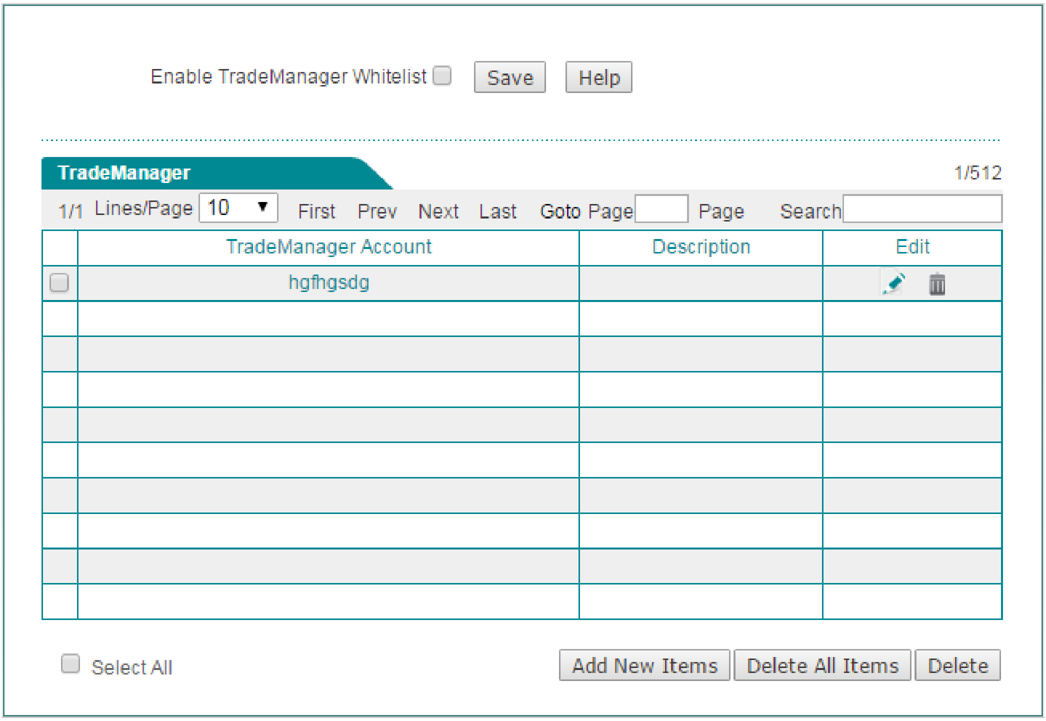
- **Enable MSN Whitelist**: Select the check box to enbale MSN whitelist. If enabled, the MSN accounts in **MSN Whitelist** are exempt from the Internet application management policies.

- **Add:** To add a new MSN account, click **Add** to go to **MSN Whitelist Settings** page, and then configure it, lastly click **Save**.

## 7.5 TradeManager

This section describes **App Control > TradeManager** page. This feature allows you to add a list of TradeManager accounts that are exempt from the Internet application management policies (set in **App Control > Application Control** page).

}



Enable TradeManager Whitelist ☐

| | TradeManager Account | Description | Edit |
|---|---|---|---|
| ☐ | hgfhgsdg | | ✎ 🗑 |

Figure 7-11 TradeManager

- **Enable TradeManager Whitelist**: Select the check box to enbale TradeManager whitelist. If enabled, the accounts in TradeManager list are exempt from the Internet application management policies.

- **Add:** To add a new TradeManager account, click **Add New Items** to go to **TradeManager Account** page, and then configure it, lastly click **Save**.

## 7.6 Notification

The Device provides notice feature which is used to push notice messages to the specified LAN users. After you enable notice feature, if a specified LAN user accesses the Internet via a web browser (e.g., IE, Firefox), the Device will automatically push a notice message to the user.

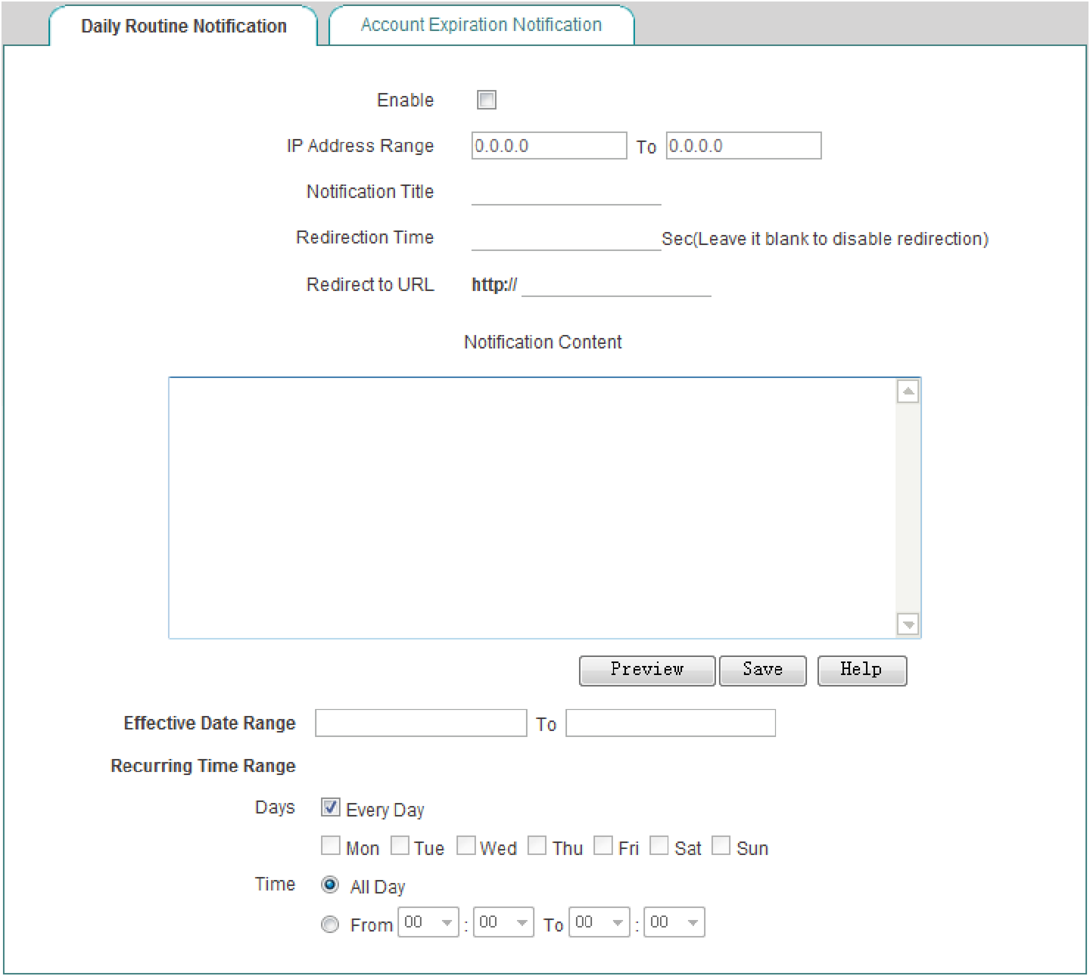
The Device provides daily routine notice and account expiration notice. If you enable daily routine notice feature and specify a notice message, and then when a specified LAN user accesses the Internet via a web browser, the Device will automatically push the notice message to the user on the specified time. If you enable account expiration notice feature and specify a notice message, and when a specified LAN user accesses the Internet via a web browser, the Device will automatically push the notice message to the user before the account expire.

Besides notice feature in this page, the Device also provide domain blocking notice feature. Please refer to the section: 12.3 Domain Filtering for detailed information.

}

### 7.6.1.1 Daily Routine Notification

When using daily routine notice, the Device will automatically push the notice message to the LAN users that belong to the specified address group at the specified time.



Enable □

IP Address Range 0.0.0.0 To 0.0.0.0

Notification Title

Redirection Time Sec(Leave it blank to disable redirection)

Redirect to URL http://

Effective Date Range To

Days ☑ Every Day

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

Time ● All Day

○ From 00 : 00 To 00 : 00

Figure 7-12 Daily Routine Notification

- **Enable:** Select the check box to enable Daily Routine Notification.

- **IP Address Range:** Specify the range of IP addresses to which the notification will be sent.

- **Notification Titile:** Specify the title of the notice message.

- **Redirection Time:** Specify the time you stay on the notice page. After that time, the web page will jump to the page you setup on **Redirect to URL**. Leave it blank means disable redirection

- **Redirect to URL:** Specify the URL you want the web page jump to after **Redirection Time** you setup.

}

- **Notification Content:** Specify the content of the notice message.

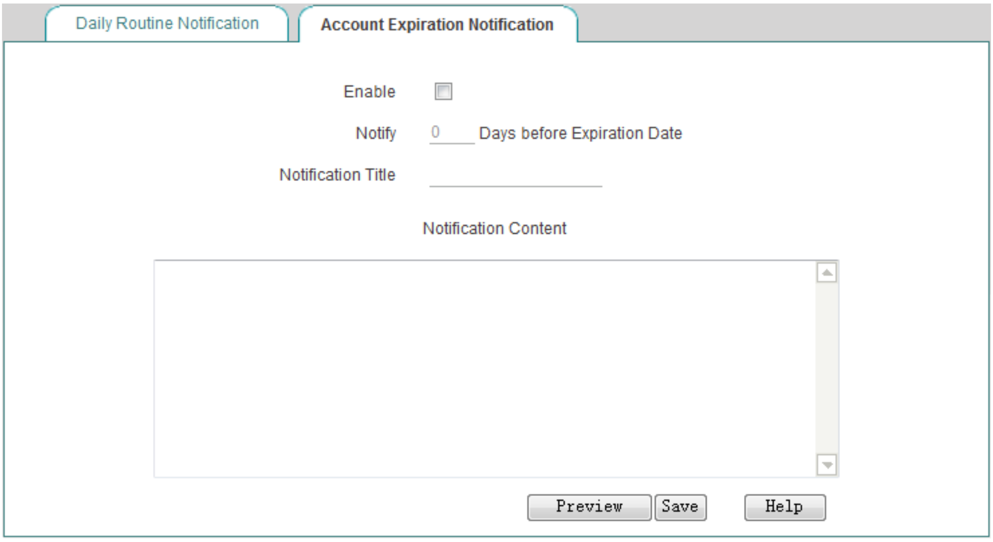
- **Effective Date Range:** Specify the effective date range of the notification.

- **Recurring Time Range:** Specify the days and times during which the notification will be sent.

**Note:** Only modifying the content of notification title and notification content and then clicking the **Save** button will not take effect.

### 7.6.1.2 Account Expiration Notification

When using account expiration notice, the Device will automatically push the notice message to the LAN users before the PPPoE account expire.



Enable □

Notify 0 Days before Expiration Date

Notification Title

Notification Content

Figure 7-13 Account Expiration Notification

- **Enable:** Select the check box to enable account expiration notification feature.

- **Notify** “X” **Days before Expiration Date:** Specify the number of days before the account expiration date so that the notification will be sent to the users from that day onwards. Each time a PPPoE user or Web authentication user connects to the Device, the notification appears the first time the user attempts to access a web page.

- **Notification Title:** Specify the title of the notification.

- **Notification Content:** Specify the content of the notification.

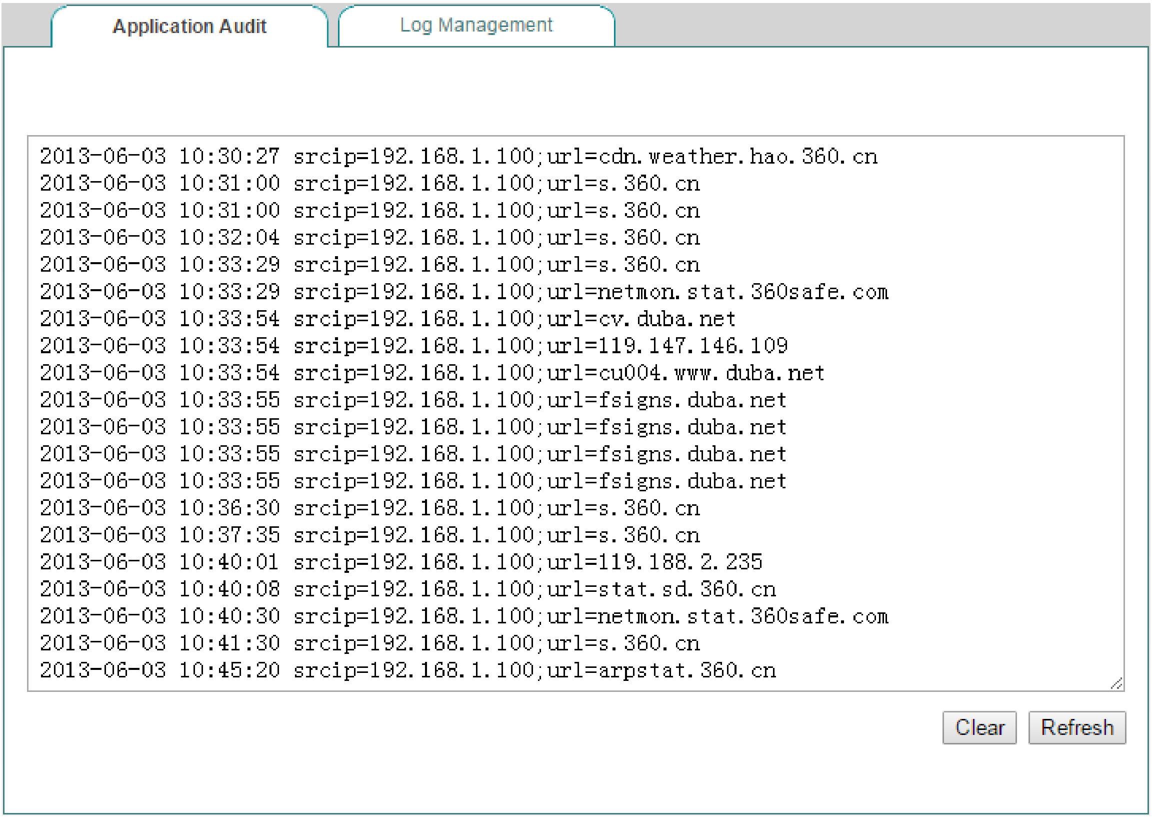
**Note:** After a PPPoE or web authentication user account expires, the user the user can still dial in and connect to the Device, but cannot access the Internet through the Device; and when the user attempts to access a Web site, the expiration notification appears in the Web browser.

}

# 7.7 Application Audit

This section describes **App Control > Application Audit** page. On the Device, auditing is the process of tracking user online activities. When an audited event occurs, the Device stores a record of the event to the audit log.

### 1) View Audit Log



```
2013-06-03 10:30:27 srcip=192.168.1.100;url=cdn.weather.hao.360.cn
2013-06-03 10:31:00 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:31:00 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:32:04 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:33:29 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:33:29 srcip=192.168.1.100;url=netmon.stat.360safe.com
2013-06-03 10:33:54 srcip=192.168.1.100;url=cv.duba.net
2013-06-03 10:33:54 srcip=192.168.1.100;url=119.147.146.109
2013-06-03 10:33:54 srcip=192.168.1.100;url=cu004.www.duba.net
2013-06-03 10:33:55 srcip=192.168.1.100;url=fsigns.duba.net
2013-06-03 10:33:55 srcip=192.168.1.100;url=fsigns.duba.net
2013-06-03 10:33:55 srcip=192.168.1.100;url=fsigns.duba.net
2013-06-03 10:33:55 srcip=192.168.1.100;url=fsigns.duba.net
2013-06-03 10:36:30 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:37:35 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:40:01 srcip=192.168.1.100;url=119.188.2.235
2013-06-03 10:40:08 srcip=192.168.1.100;url=stat.sd.360.cn
2013-06-03 10:40:30 srcip=192.168.1.100;url=netmon.stat.360safe.com
2013-06-03 10:41:30 srcip=192.168.1.100;url=s.360.cn
2013-06-03 10:45:20 srcip=192.168.1.100;url=arpstat.360.cn
```

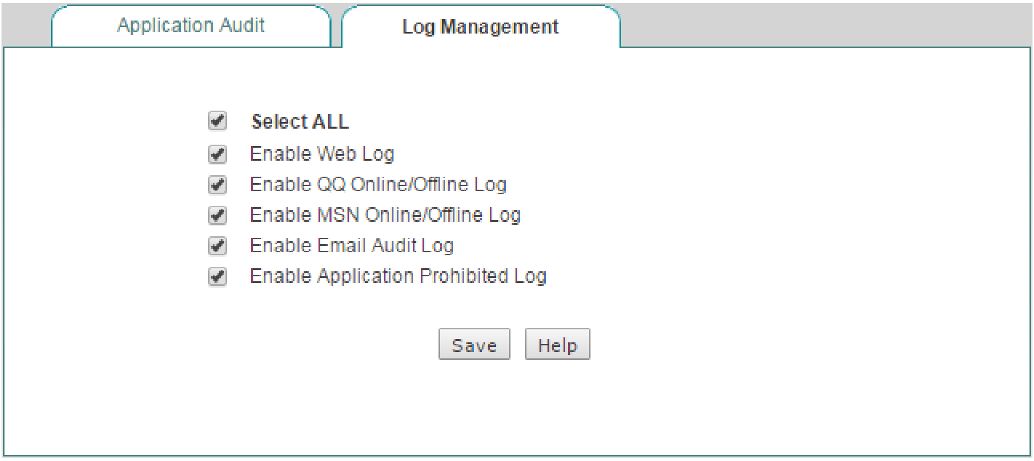
**Figure 7-14 Internet Application Audit**

**Note:** The Device can record the last 400 audit log messages.

### 2) Log Management

You can go to **App Control > Application Audit > Log Management** to specify the types of events to audit.

}



☑ Select ALL
☑ Enable Web Log
☑ Enable QQ Online/Offline Log
☑ Enable MSN Online/Offline Log
☑ Enable Email Audit Log
☑ Enable Application Prohibited Log

**Figure 7-15 Log Management**

- **Enable Web Log:** Select the check box to enable web log. If enabled, you can view the records of website visits in **Application Audit** page. E.g., "2012-07-09 09:36:41 srcip=200.200.202.127;url=www.paipai.com" means that the user with IP address 200.200.202.127 accessed www.paipai.com on July 09, 2012 at 09:36:41.

- **Enable QQ Online/Offline Log:** Select the check box to enable QQ online/offline log. If enabled, you can view QQ online and offline activities of internal users in **Application Audit** page.

- **Enable MSN Online/Offline Log:** Select the check box to enable MSN online/offline log. If enabled, you can view MSN online and offline activities of internal users in **Application Audit** page.

- **Enable Email Audit Log:** Select the check box to enable email audit log. If enabled, you can view emails sending and receiving activities of internal users in **Application Audit** page.

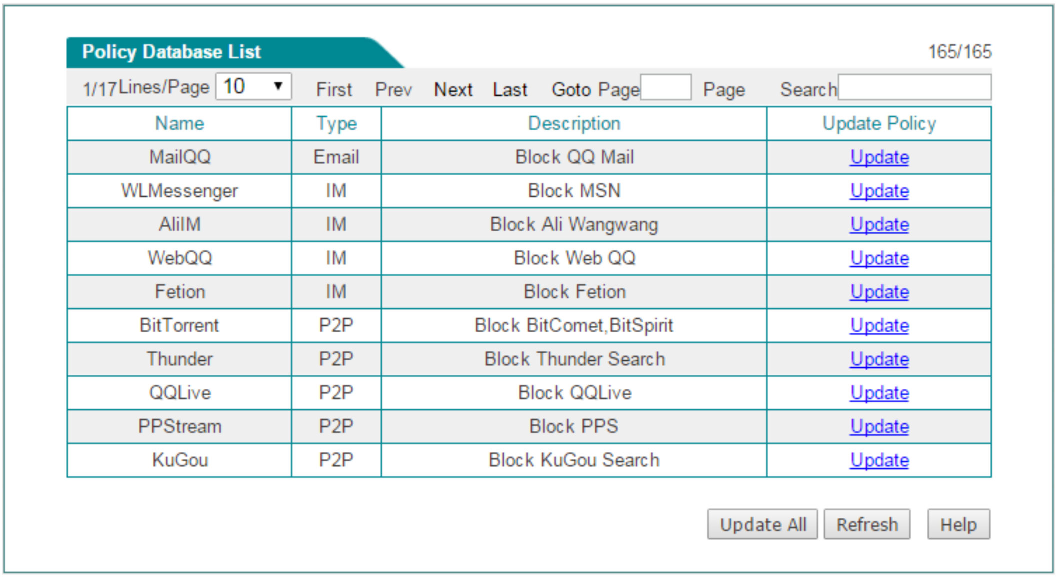
- **Enable Application Prohibited Log:** Select the check box to enable application prohibited log. If enabled, you can view the events blocked by Internet application management policies (set in **App Control > Application Control** page) in **Application Audit** page.

## 7.8 Policy Database

This section describes **App Control** > **Policy Database** page.

In this page, you can not only view the policies in **Policy Database List**, but also update them online. The Device currently provides eleven types of policies, including: Email, IM, P2P, Stock, Network Video, Online Game, Shopping Site, SNS, Web Game, Forum and Others. These policies are referenced by Internet application management function (set in **App Control > Application Control** page).

}



| Name | Type | Description | Update Policy |
|---|---|---|---|
| MailQQ | Email | Block QQ Mail | Update |
| WLMessenger | IM | Block MSN | Update |
| AliIM | IM | Block Ali Wangwang | Update |
| WebQQ | IM | Block Web QQ | Update |
| Fetion | IM | Block Fetion | Update |
| BitTorrent | P2P | Block BitComet,BitSpirit | Update |
| Thunder | P2P | Block Thunder Search | Update |
| QQLive | P2P | Block QQLive | Update |
| PPStream | P2P | Block PPS | Update |
| KuGou | P2P | Block KuGou Search | Update |

**Figure 7-16 Policy Database**

- **Name:** Displays the name of the policy.
- **Type:** Displays the type of the policy.
- **Description:** Displays the description of the policy. It is usually used to describe the purpose of the policy.
- **Update:** Click to update the policy over the Internet.
- **Update All:** Click to update all policies in the list over the Internet.

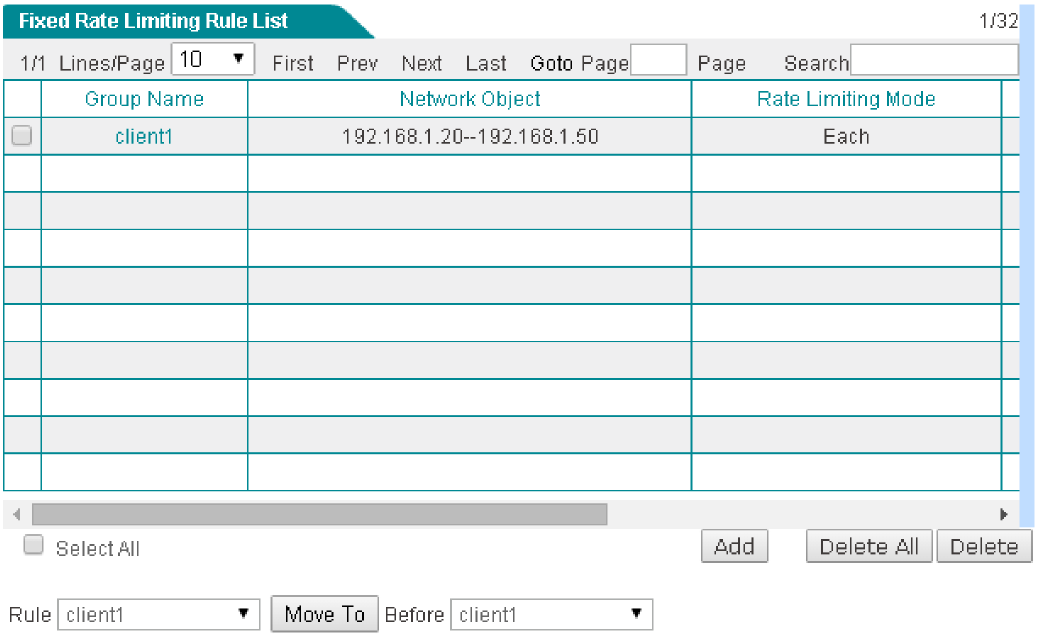
}

# Chapter 8. QoS Menu

This chapter mainly describe fixed rate limiting, flexible bandwidth, p2p rate limit, session limiting.

## 8.1 Fixed Rate Limiting

On the **QoS** > **Fixed Rate Limiting** page, you can specify the upload/download limiting value for each LAN host, in order to allocate bandwidth equally and avoid few hosts occupying too much bandwidth.



Fixed Rate Limiting Rule List 1/32

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | Group Name | Network Object | Rate Limiting Mode |
|---|---|---|---|
| □ | client1 | 192.168.1.20--192.168.1.50 | Each |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

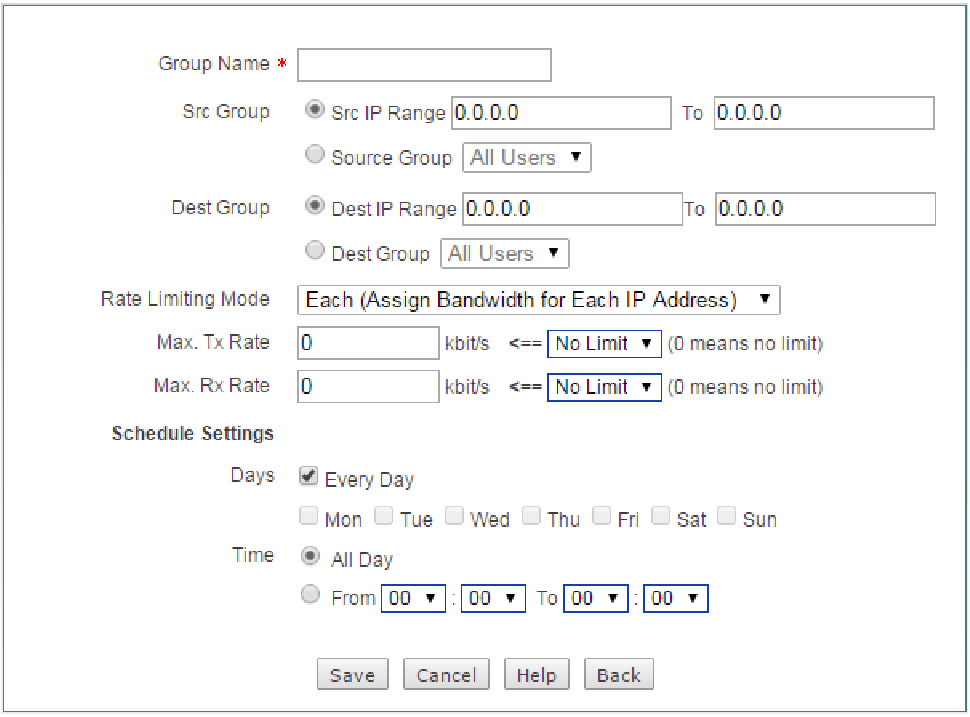
□ Select All

Rule client1 ▼ Move To Before client1 ▼

**Figure 8-1 Fixed Rate Limiting Rule List**

Click the **Add** button in the up figure to add a fixed rate limiting rule entry.

}



Group Name *

Src Group ● Src IP Range 0.0.0.0 To 0.0.0.0

○ Source Group All Users ▼

Dest Group ● Dest IP Range 0.0.0.0 To 0.0.0.0

○ Dest Group All Users ▼

Rate Limiting Mode Each (Assign Bandwidth for Each IP Address) ▼

Max. Tx Rate 0 kbit/s <== No Limit ▼ (0 means no limit)

Max. Rx Rate 0 kbit/s <== No Limit ▼ (0 means no limit)

Schedule Settings

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

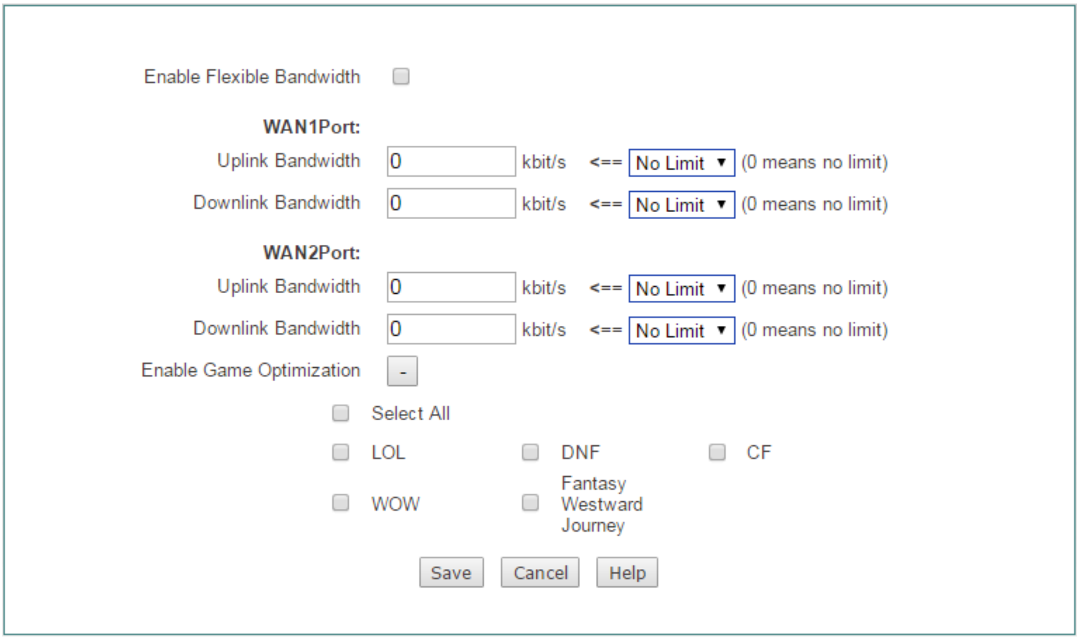
**Figure 8-2 Fixed Rate Limiting Setup**

- **Group Name:** Specify group name.
- **Src Group:** Specify the range of IP addresses in local network to which the fixed rate limiting rule applies.
- **Dest Group:** Specify the range of destination IP addresses to which the fixed rate limiting rule applies.
- **Rate Limiting Mode - Each:** The specified Max. Tx/Rx rate is assigned to each IP address that matches the rule.
- **Rate Limiting Mode - Share:** The specified Max. Tx/Rx rate is shared by all IP addresses that match the rule.
- **Max. Tx/Rx Rate:** Specify the maximum upload rate and download rate.
- **Schedule Settings:** Apply a schedule to the fixed rate limiting rule to specify when it is in effect.

## 8.2 Flexible Bandwidth

On the **QoS > Flexible Bandwidth** page, you can enable game boost and set uplink/downlink bandwidth. When the network is busy, the game will get the uplink/downlink bandwidth you set, which ensure the game running smoothly.

}



Enable Flexible Bandwidth □

**WAN1Port:**

Uplink Bandwidth 0 kbit/s <== No Limit ▼ (0 means no limit)

Downlink Bandwidth 0 kbit/s <== No Limit ▼ (0 means no limit)

**WAN2Port:**

Uplink Bandwidth 0 kbit/s <== No Limit ▼ (0 means no limit)

Downlink Bandwidth 0 kbit/s <== No Limit ▼ (0 means no limit)

Enable Game Optimization -

□ Select All

□ LOL □ DNF □ CF

□ WOW □ Fantasy Westward Journey

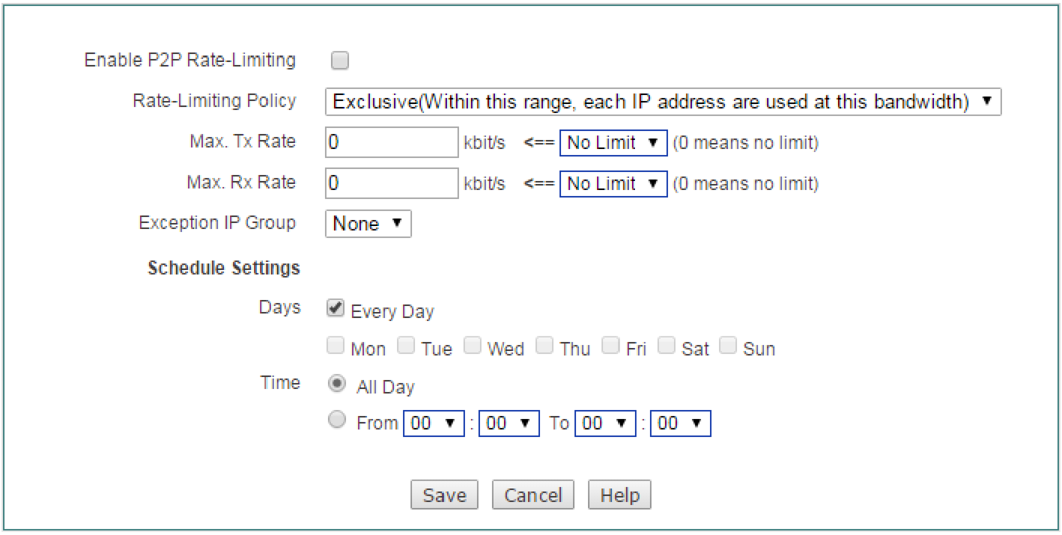
**Figure 8-3 Flexible Bandwidth**

- **Enable Game Boost:** Select to enable game boost.
- **Uplink Bandwidth:** Specify the upload speed of Internet connection. 0 means unlimited rate.
- **Downlink Bandwidth:** Specify the download speed of Internet connection. 0 means unlimited rate.
- **Game Settings:** Select the game you want to boost.

## 8.3 P2P Rate Limit

P2P software usually occupies too much bandwidth, which lead to the network very busy. You can limit the speed of P2P users by setting its maximum upload and download speed. On the **QoS > P2P Rate Limit** page, you can enable this function.

}



Enable P2P Rate-Limiting □

Rate-Limiting Policy: Exclusive(Within this range, each IP address are used at this bandwidth) ▼

Max. Tx Rate: 0 kbit/s <== No Limit ▼ (0 means no limit)

Max. Rx Rate: 0 kbit/s <== No Limit ▼ (0 means no limit)

Exception IP Group: None ▼

Schedule Settings

Days: ☑ Every Day

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

Time: ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

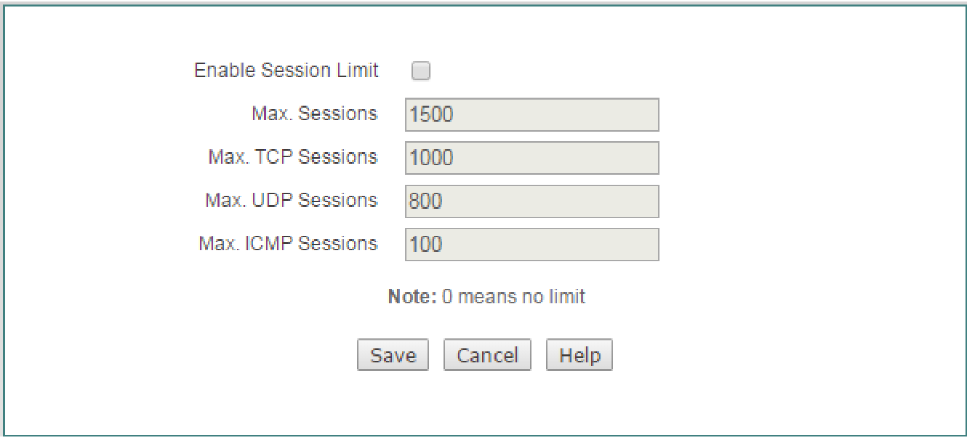
**Figure 8-4 P2P Rate Limit**

- **Enable P2P Rate-Limiting:** Select to enable P2P Rate-Limiting.
- **Rate-Limiting Policy:** The options are **Exclusive** and **Share**.
  - **Exclusive:** The specified **Max. Tx/Rx Rate** is assigned to each member in the group.
  - **Share:** The specified **Max. Tx/Rx Rate** is shared by all members in the group.
- **Max. Tx Rate:** Specify the maximum upload speed for the members in the group. 0 means unlimited rate.
- **Max. Rx Rate:** Specify the maximum download speed for the members in the group. 0 means unlimited rate.
- **Exception IP Group:** Specify the group which is out of the P2P Rate limiting.
- **Schedule Settings:** Specify the schedule of this P2P Rate Limiting taking effect.

## 8.4 Session Limiting

On the **QoS > Session Limiting** page, you can set the maximum number of concurrent sessions, concurrent TCP sessions, concurrent UDP sessions, concurrent ICMP sessions per restricted host..

}



Enable Session Limit □

Max. Sessions 1500

Max. TCP Sessions 1000

Max. UDP Sessions 800

Max. ICMP Sessions 100

**Note:** 0 means no limit

**Figure 8-5 Session Limiting**

- **Enable Session Limit:** Select to enable session limiting.

- **Max. Sessions:** Specify the maximum number of concurrent sessions per restricted host. 0 means no restriction.

- **Max. TCP Sessions:** Specify the maximum number of concurrent TCP sessions per restricted host. 0 means no restriction.

- **Max. UDP Sessions:** Specify the maximum number of concurrent UDP sessions per restricted host. 0 means no restriction.

- **Max. ICMP Sessions:** Specify the maximum number of concurrent ICMP sessions per restricted host. 0 means no restriction.

**Notes:**

1) If some applications (such as online games) performance is degraded due to the maximum sessions limiting, you can increase the **Max. Sessions** and **Max. TCP sessions** (or **Max. UDP sessions**) properly. Note that if they are too large, it will lower or lose the Device’s ability to prevent DDoS attacks.

2) In most cases, to ensure that the LAN users surf the Internet normally, the maximum NAT sessions cannot be too small. It is suggested that both the **Max. Sessions** and **Max. TCP sessions** should be larger than or equal to 100, the **Max. UDP sessions** should be larger than or equal to 50, and **Max. ICMP sessions** should be larger than or equal to 10.

}

# Chapter 9. Firewall Menu

This chapter mainly describe attack prevention, access control, domain filtering, MAC Address Filtering.

## 9.1 Attack Prevention

This section describes the **Firewall > Attack Prevention** page, which includes internal attack prevention and external attack prevention.

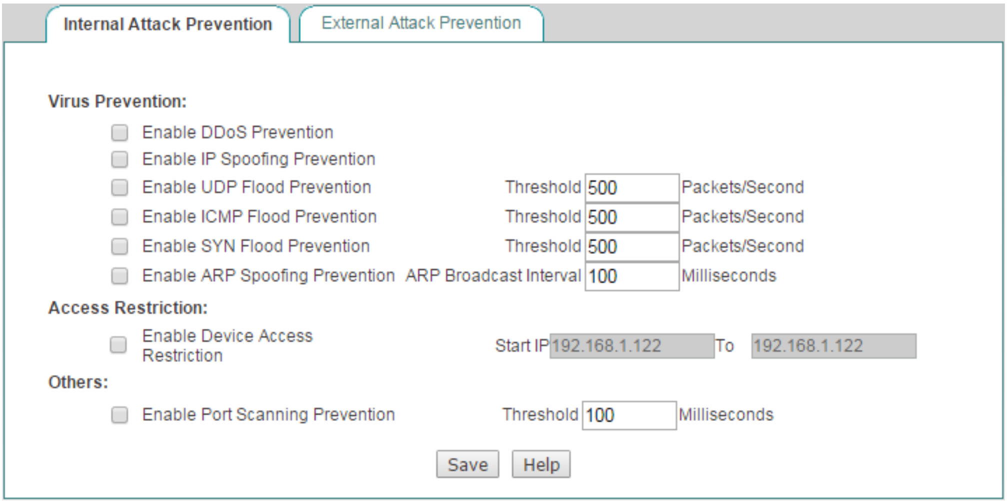
### 9.1.1.1 Internal Attack Prevention

In this page, you can do basic internal attack defense settings to enhance network security. The internal attack defense includes three parts:

- **Virus Prevention:** It can effectively protect the Device against popular virus attacks, such as, DDoS attack, UDP/ICMP/SYN flood attack, ARP spoofing attack, and so on.

- **Access Restriction:** It can effectively protect the Device by only allow the specified IP address host access to the Device.

- **Others:** It can effectively protect the Device against port scanning attack.



Virus Prevention:

☐ Enable DDoS Prevention

☐ Enable IP Spoofing Prevention

☐ Enable UDP Flood Prevention Threshold 500 Packets/Second

☐ Enable ICMP Flood Prevention Threshold 500 Packets/Second

☐ Enable SYN Flood Prevention Threshold 500 Packets/Second

☐ Enable ARP Spoofing Prevention ARP Broadcast Interval 100 Milliseconds

Access Restriction:

☐ Enable Device Access Restriction Start IP 192.168.1.122 To 192.168.1.122

Others:

☐ Enable Port Scanning Prevention Threshold 100 Milliseconds

**Figure 9-1 Internal Attack Defense Settings**

1) **Virus Prevention**

◈ **Enable DDoS Prevention:** If selected, the Device will be effectively protected against popular DoS/DDoS attacks.

}

- **Enable IP Spoofing Prevention:** If selected, the Device will be effectively protected against IP spoofing attack. The Device will only forward the packets whose source IP address is in the same subnet as the Device LAN IP address.

- **Enable UDP Flood Prevention:** If selected, the Device will be effectively protected against UDP flood attack. If the number of UDP packets from one source IP address (e.g., 192.168.16.66) to a single port on a remote host exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.66 is performing UDP flood attack, and then randomly discard the further UDP packets from that source to that destination. In most cases, leave **Threshold** the default value.

- **Enable ICMP Flood Prevention:** If selected, the Device will be effectively protected against ICMP flood attack. If the number of ICMP packets from one source IP address (e.g., 192.168.16.16) to a single port on a remote host exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.16 is performing ICMP flood attack, and then randomly discard the further ICMP packets from that source to that destination. In most cases, leave **Threshold** the default value.

- **Enable SYN Flood Prevention:** If selected, the Device will be effectively protected against SYN flood defense. If the number of SYN packets from one source IP address (e.g., 192.168.16.36) to a single port on a remote host exceeds the threshold, the Device will consider that the LAN host with IP address 192.168.16.36 is performing SYN flood attack, and then randomly discard the further SYN packets from that source to that destination. In most cases, leave **Threshold** the default value.

- **Enable ARP Spoofing Prevention:** If selected, and then bind all the IP/MAC address pairs of the LAN hosts (configured in the **User Management > IP/MAC Binding** page), it will effectively protect the Device against ARP spoofing attack.

- **ARP Broadcast Interval:** Specify the time interval at which the Device periodically broadcasts gratuitous ARP packets. These gratuitous ARP packets are used to inform the LAN hosts the correct MAC address of the Device's LAN interface, so the LAN hosts can effectively defense ARP spoofing attack. It should be multiple of 10 between 100 and 5000 milliseconds.

### 2) Access Restriction

- **Enable Device Access Restriction**: If selected, LAN hosts' access to the Device through LAN interface will be restricted, so it will protect the Device against internal DDoS attacks.

- **Start IP:** Specify an address range of the allowed LAN hosts. When **Enable Device Access Restriction** is selected, only the LAN hosts that belong to this range can access the web or telnet service provided by the Device.

### 3) Others

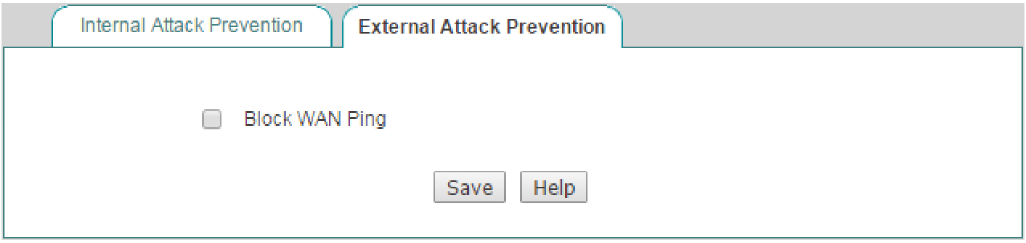
- **Enable Port Scanning Prevention:** If selected, the Device will be effectively protected against port scanning attack. After you enable this feature, if a LAN

}

host continuously sends the SYN packets to different ports on a remote host, and the number of ports exceeds 10 at the specified time interval (set by the **Threshold)**, the Device will consider that the LAN host is performing port scanning attack, and then randomly discard the further SYN packets from it to that destination host. In most cases, leave the **Threshold** the default value.

#### 9.1.1.2 External Attack Prevention

In this page you can enable or disable WAN ping respond. As ping is often used by malicious Internet users to locate active networks or hosts, in most cases, it is recommended that you disable WAN ping respond for added security. Only in some special cases, such as network debugging, you need enable this feature.



□ Block WAN Ping

**Figure 9-2 External Attack Defense Settings**

- **Block WAN Ping:** It allows you to enable or disable WAN ping respond. If you select the check box to block WAN ping respond, all the Device's WAN interfaces will not respond to ping requests from the outside hosts.

## 9.2 Access Control

The development of Internet has brought some side effects, such as the emergence of gambling, pornography, and other illegal websites which are contrary to the state laws and regulations; broadband network provide fast surfing to the Internet users, while fast spreading worms cause great threat to the Internet users. So if an organization wants to access the Internet, it needs specific Internet access rules. Such as, a government organization wants to block the civil servants from accessing stock websites, using IM messenger applications; a business wants to block the employees from accessing game websites and other services which are unrelated to work during working time; parents want to control their children's online time; an network administrator wants to block the worms and hacker attacks.

To achieve these purposes, we develop and implement access control feature on the Device. By utilizing access control feature flexibly, you can not only assign different Internet access privileges to different LAN users, but also assign different Internet access privileges to the same users based on schedules. In practice, you can set appropriate access control rules according to the actual requirements of your organization. Such as, for a school, you can block the students to access game websites; for a family, you can only allow your children to access the Internet during the specified period of time; for a business, you can block the Financial Department's employees from accessing the Internet.

}

### 9.2.1.1 The Operation Principle of Access Control

By default, as no access control rule exists on the Device, the Device will forward all the valid packets received by the LAN interface. After you have enabled access control, the Device will examine each packet received by the LAN interface to determine whether to forward or drop the packet, based on the criteria you specified in the access control rules.

When receiving a packet initiated from LAN, the Device will analyze the packet by extracting its source MAC address, source IP address, destination IP address, protocol type (TCP, UDP or ICMP), port number, content, and the date and time at which the packet was received, and then compare them with each rule in the Access Control Rule List in order, from top to bottom. The first rule that matches the packet will be applied to the packet, and the Device will forward or drop it according to this rule's action. Note that after a match is found, no further rules will be checked; and if no match is found, the Device will drop the packet to ensure security.

The access control rules are applied to the packets that are received by the Device's LAN interface, that is, those packets that arrive on the LAN interface and then go through the Device. If a packet matches a rule whose **Action** is **Allow**, the packet will be allowed to pass, and then be further processed by route, NAT and other modules. Else, if the packet matches a rule whose **Action** is **Drop**, or doesn't match any rule, the packet will be dropped immediately. As these dropped packets are no longer further processed by route, NAT and other modules, it will reduce CPU load and improve the Device performance.

The action of an access control rule is either **Allow** or **Deny**. When receiving a packet that matches a rule in the **Access Control Rule List**, the Device will forward the packet if the rule's action is **Allow**; else the Device will drop it.

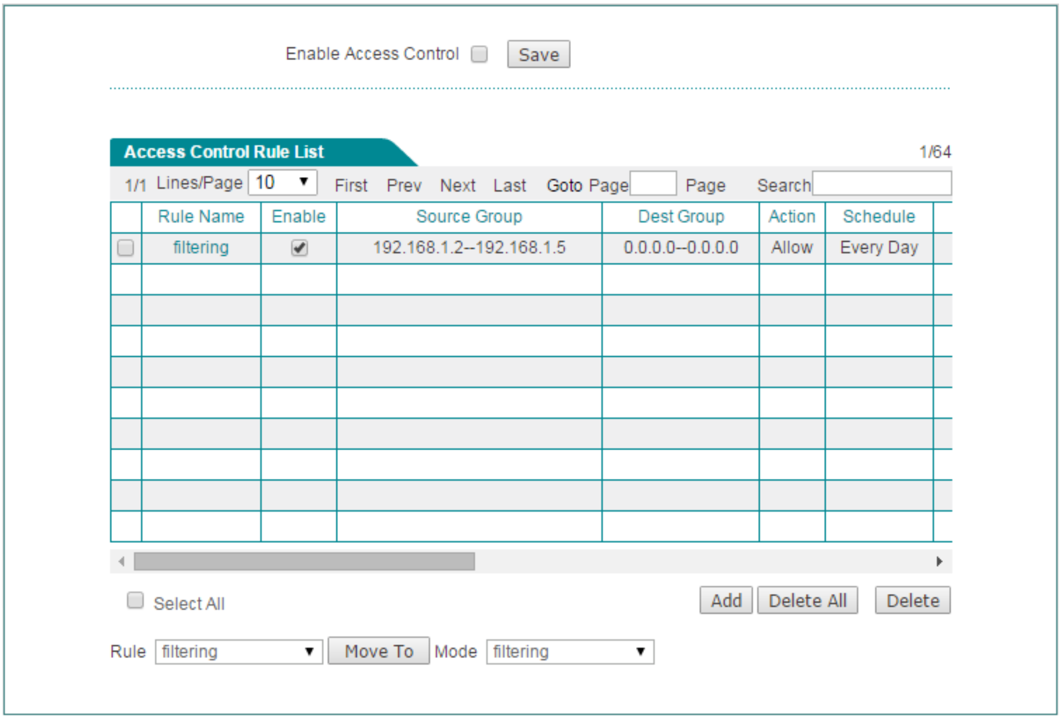
### 9.2.1.2 The Execution Order of Access Control Rules

The order of access control rules is very important. When receiving a packet initiated from LAN, the Device will search Access Control Rule List to find out if there is a rule that matches the packet. It will check the packet against each rule in the Access Control Rule List in order. After a match is found, no further rules will be checked. If no match is found, the Device will drop the packet to ensure security. Note that by default the rules are listed in reverse chronological order of creation, the later the rule is created, the upper the rule is listed; and the Device allows you to manually move a rule to a different position in the list.

Because the Device will allow or deny a packet to pass according to the first rule that matches the packet, you should arrange the rules in Access Control Rule List from specific to general. For example, if you create an access control rule at the beginning that explicitly allows all packets to pass, no further rules are ever checked. Another example is that if you only allow a LAN user to access Web service, and block any other service, then the rule that allows the user to access Web service should be listed above the rule that denies the user to access any other service.

}

### 9.2.1.3 Access Control Rule List



Enable Access Control □

Access Control Rule List 1/64

1/1 Lines/Page 10

| | Rule Name | Enable | Source Group | Dest Group | Action | Schedule |
|---|---|---|---|---|---|---|
| □ | filtering | ☑ | 192.168.1.2--192.168.1.5 | 0.0.0.0--0.0.0.0 | Allow | Every Day |

□ Select All

Rule filtering Mode filtering

Figure 9-3 Access Control List

- **Add an Access Control Rule:** Click the **Add** button to go to the setup page, and then configure it, lastly click the **Save** button.

- **Edit an Access Control Rule:** Click its **Edit** hyperlink, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Move an Access Control Rule:** The Device allows you to move an access control rule to above another rule in the list, the operation is as follows: Select the ID of a rule that you want to move from the **Rule** drop-down list, and another rule's ID from the **Mode** drop-down list, lastly click the **Move To** button.

- **Delete Access Control Rule(s):** Select the leftmost check boxes of rules, and then click the **Delete** button.

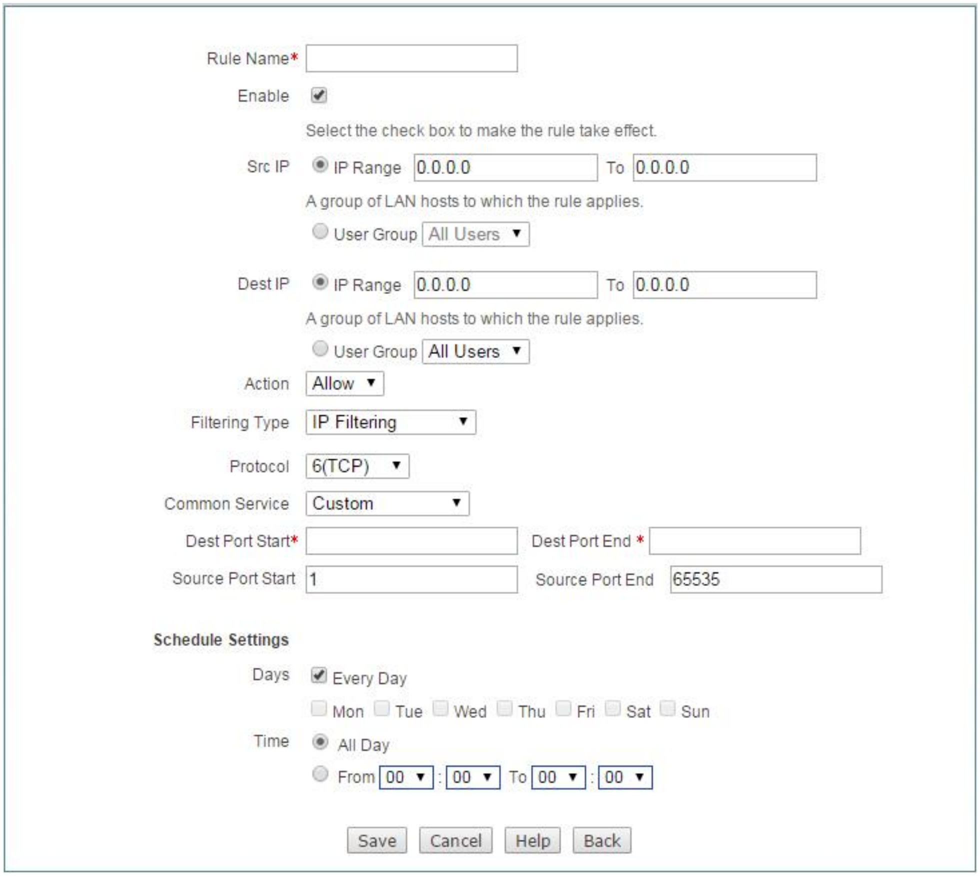
**Note:** The execution order of access control rule list you added is from up to down.

### 9.2.1.4 Access Control Rule Settings

We will introduce every parameter's meaning for four filtering type (IP Filtering, URL Filtering, Keyword Filtering, DNS Filtering).

}

### 9.2.1.4.1 IP Filtering



Rule Name*

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users

Dest IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users

Action Allow

Filtering Type IP Filtering

Protocol 6(TCP)

Common Service Custom

Dest Port Start* Dest Port End *

Source Port Start 1 Source Port End 65535

**Schedule Settings**

Days ☑ Every Day

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

Time ● All Day

○ From 00 : 00 To 00 : 00

**Figure 9-4 Access Control Rule Settings_IP Filtering**

- **Rule Name:** Specify the name of this rule.

- **Enable:** Select to enable Access Control.

- **Src IP:** Specify the source IP addresses of the packets to which the access control rule applies. There are two options:

  - **IP Range:** Specify the start and the end addresses.

  - **User Group:** Select it to choose an address group.

- **Dest IP:** Specify the destination IP addresses of the packets to which the access control rule applies. There are two options:

  - **IP Range:** Specify the start and end addresses.

  - **User Group:** Select it to choose an address group.

- **Action:** It determines the action of the access control rule. There are two available options:

}

  - **Allow:** If selected, the Device will allow the packets that match the rule to pass, that is, the Device will forward these packets.

  - **Deny:** If selected, the Device will deny the packets that match the rule to pass, that is, the Device will drop these packets.

- **Filtering Type:** here please select **IP Filtering**.

- **Protocol:** The protocol type of access control, with five options: **1(ICMP)**, **6(TCP)**, **17(UDP)**, **51(AH)**, and **all (All)**.

- **Common Service:** Provides the common service port of TCP protocol and UDP protocol. You also can choose **Custom** from the drop-down list to set Dest Port and Source Port for yourself.

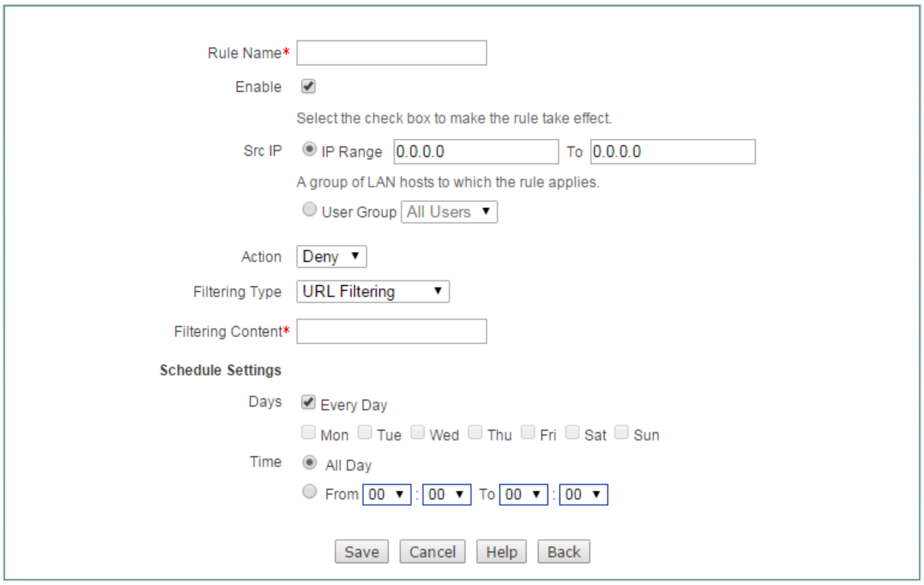
- **Dest Port:** Specify a range of destination ports to which the access control rule applies.

- **Source Port:** Specify a range of source ports to which the access control rule applies.

- **Schedule Settings:** Specify a schedule to restrict when the access control rule take effect. The default value is **Every Day** and **All Day**, which means the access control rule take effect always. Note that after the selected schedule has expired, the rule will be in effect always.

⌖ **Note:** The default addresses is 0.0.0.0 to 0.0.0.0 which means access control is effective for all users. There is no limitation for destination.

### 9.2.1.4.2 URL Filtering



Rule Name*

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▾

Action Deny ▾

Filtering Type URL Filtering ▾

Filtering Content*

**Schedule Settings**

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▾ : 00 ▾ To 00 ▾ : 00 ▾

**Figure 9-5 Access Control Rule Settings_URL Filtering**

}

The setting of Rule Name, Enable, Src IP, Action, Schedule Settings is the same with IP Filtering, please refer to the section: 12.2.1.4.1 IP Filtering.

- **Filtering Type:** Here please select **URL Filtering**.

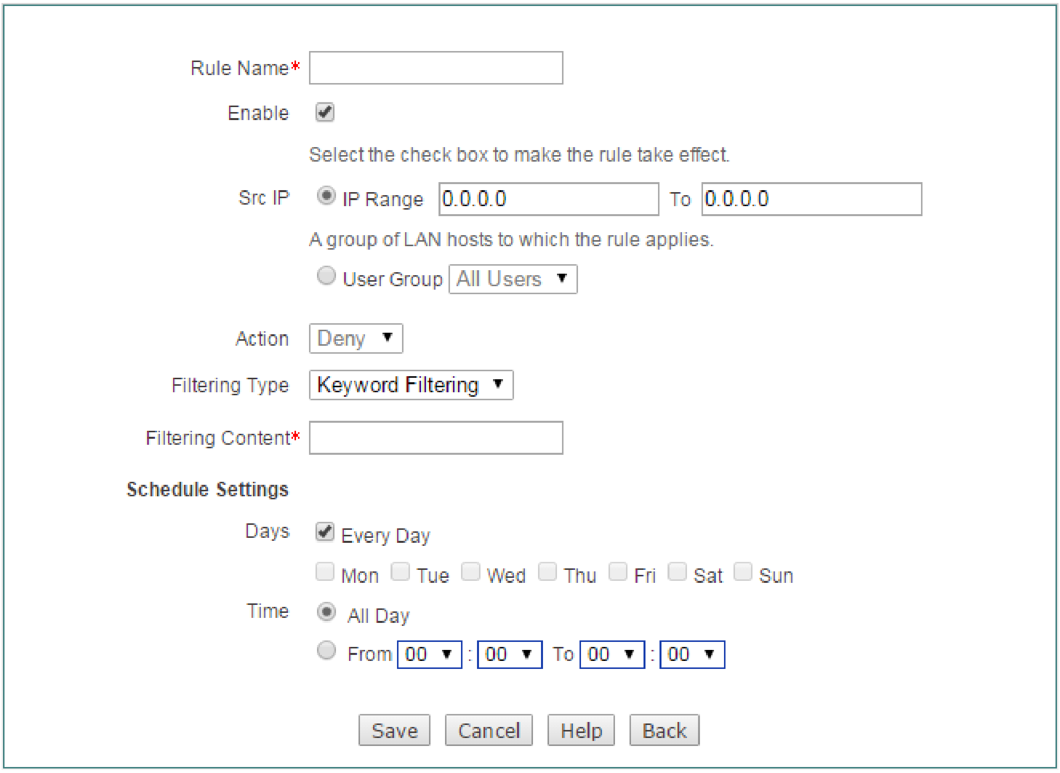
- **Filtering Content:** Enter the URL address you want the access control rule applies.

URL Filtering is filtering based on the URL keyword. When the URL of accessing webpage completely matches with the content of **Filtering Content** textbox, it will be consider matching the strategy. When inputting a full domain, the URL contains the full domain of all web pages are match. When inputting a substring of domain, the URL contains the substring of all web pages are match. **Note:**

1) The URL address is not case sensitive. Please don't input **http://** when entering URL content.

2) URL Filtering is not suitable for applications users use web browser to access. Such as: URL Filtering is not suitable for the visiting of ftp://ftp.niveoprofesional.com. In this case, you can configure IP Filtering to allow or forbidden the FTP connecting.

### 9.2.1.4.3 Keyword Filtering



Rule Name*

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Deny ▼

Filtering Type Keyword Filtering ▼

Filtering Content*

Schedule Settings

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

**Figure 9-6 Access Control Rule Settings_Keyword Filtering**

The setting of Rule Name, Enable, Src IP, Action, Schedule Settings is the same with IP Filtering, please refer to the section: 12.2.1.4.1 IP Filtering.

}

- **Filtering Type:** Here please select **Keyword Filtering**.

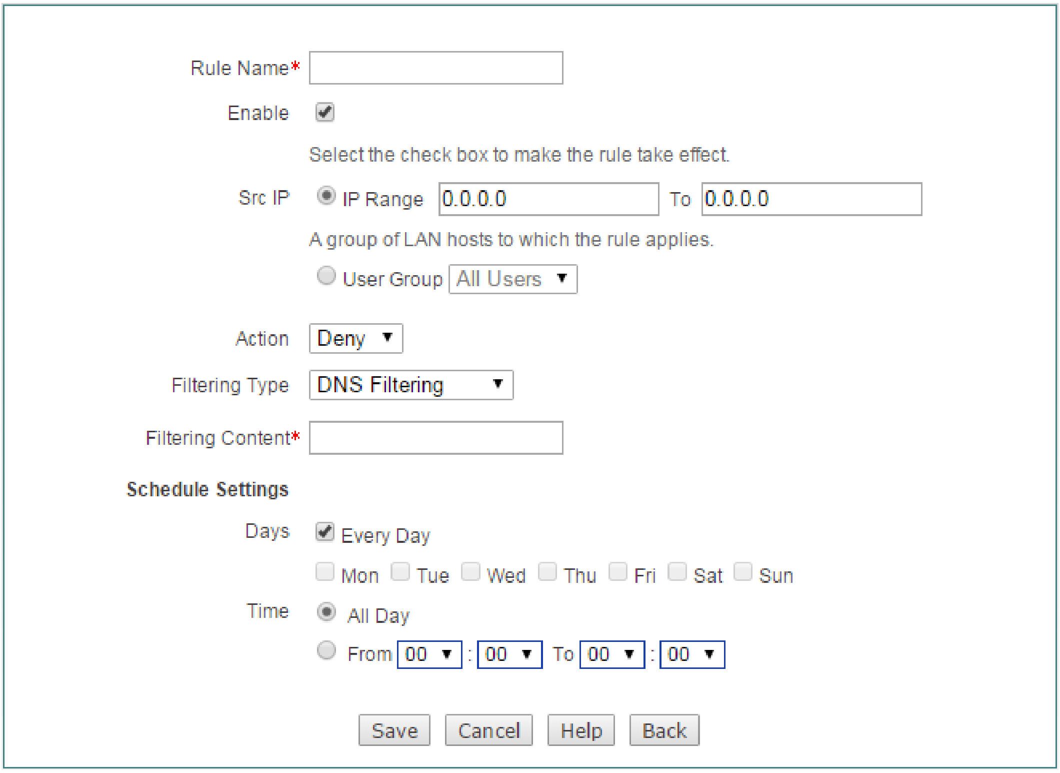
- **Filtering Content:** Specify the keywords you want the access control rule applies.

**Note:**

1) For Keyword Filtering, there is only **Deny** action you can choose.

2) The filtering content couldn't contain < > , % ' \ " & ; and blank space.

### 9.2.1.4.4 DNS Filtering



Rule Name*

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Deny ▼

Filtering Type DNS Filtering ▼

Filtering Content*

**Schedule Settings**

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

**Figure 9-7 Access Control Rule Settings_DNS Filtering**

The setting of Rule Name, Enable, Src IP, Action, Schedule Settings is the same with IP Filtering, please refer to the section: 12.2.1.4.1 IP Filtering.

- **Filtering Type:** Here please select **DNS Filtering**.

- **Filtering Content:** Specify the Domain's full name you want access control rule applies.

**Note:** Wildcard asterisk * is suitable for DNS Filter. For example, when inputting ***.163.*** on the Filtering Content, and choose Deny on the Action drop-down checkbox, users will not access to the URL which contains **.163.** of all the web pages.

}

## 9.2.1.5 Examples for Access Control

### 9.2.1.5.1 Example One

#### Requirements

In this example, a business allows the IP address between 192.168.1.9 to192.168.1.20 accesses to Internet at working time (From Monday to Friday 9:00~18:00).

#### Analysis

We need to use three user-defined access control rules to meet requirements:

(1) User-defined rule 1: Allow them to access DNS during working time.

(2) User-defined rule 2: Allow them to access WEB during working time.

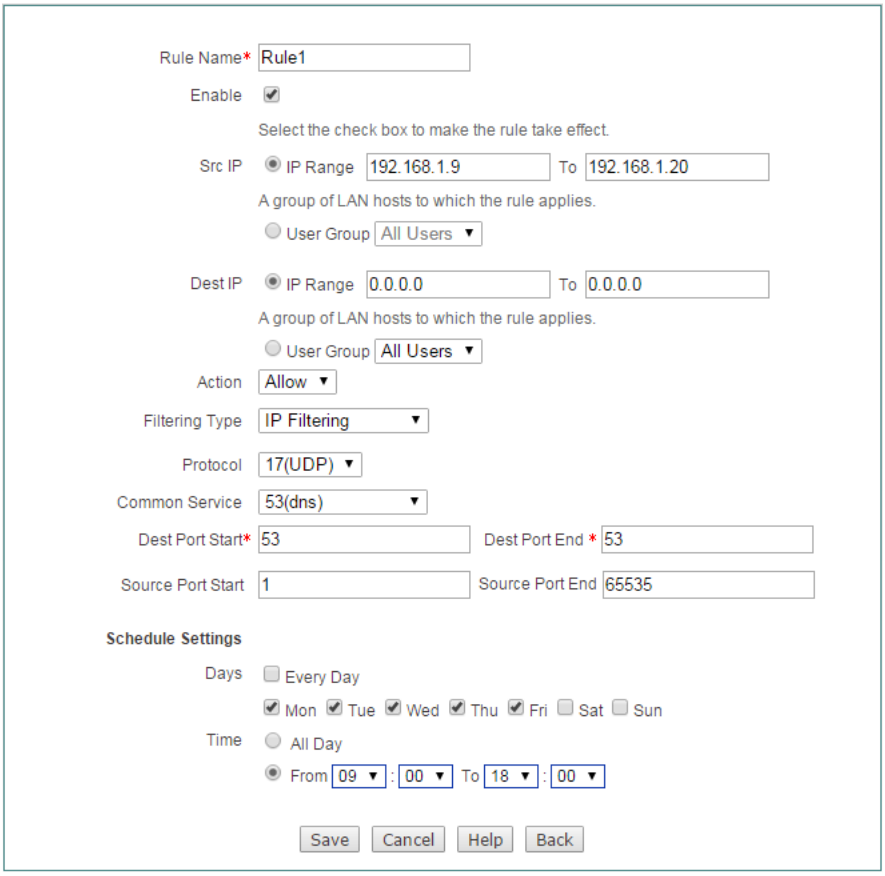
(3) User-defined rule 3: Deny them to access all other services during working time.

#### Configuration Procedure

**Step 1** Configuring Access Control Rule 1

Go to **Firewall** > **Access Control** page. Set the Src IP from 192.168.1.9 to 192.168.1.20, select **Allow** from the Action, select IP Filtering from Filtering Type, select 17(UDP) from Protocol , select 53(dns) from Common Service, select **Mon** to **Fri** from the Days, select **9:00** to **18:00** from Time, lastly click the **Save** button to save the settings.

**}**



Rule Name* Rule1

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 192.168.1.9 To 192.168.1.20

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Dest IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Allow ▼

Filtering Type IP Filtering ▼

Protocol 17(UDP) ▼

Common Service 53(dns) ▼

Dest Port Start* 53 Dest Port End * 53

Source Port Start 1 Source Port End 65535

Schedule Settings

Days □ Every Day

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

Time ○ All Day

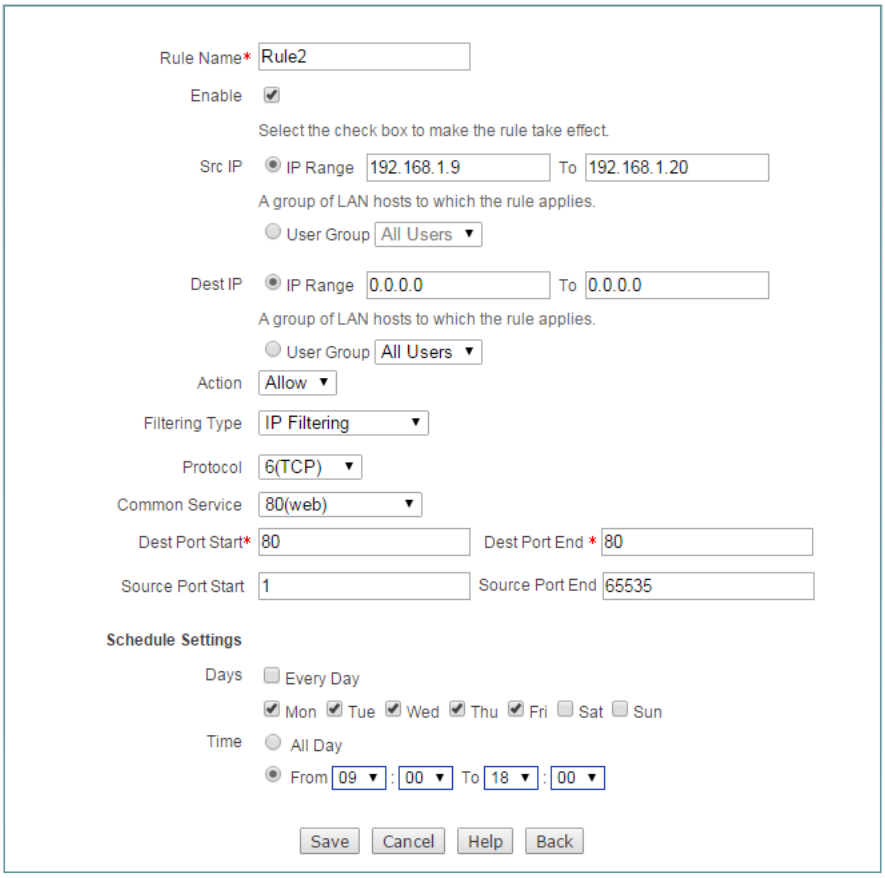
● From 09 ▼ : 00 ▼ To 18 ▼ : 00 ▼

**Figure 9-8 Access Control _Example 1_step 1**

**Step 2** Configuring Access Control Rule 2

Go to **Firewall** > **Access Control** page. Set the Src IP from 192.168.1.9 to 192.168.1.20, select **Allow** from the Action, select **IP Filtering** from Filtering Type, select 6(TCP) from Protocol , select 80(web) from Common Service, select **Mon** to **Fri** from the Days, select **9:00** to **18:00** from Time, lastly click the **Save** button to save the settings.

}



Rule Name* Rule2

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 192.168.1.9 To 192.168.1.20

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Dest IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Allow ▼

Filtering Type IP Filtering ▼

Protocol 6(TCP) ▼

Common Service 80(web) ▼

Dest Port Start* 80 Dest Port End * 80

Source Port Start 1 Source Port End 65535

Schedule Settings

Days □ Every Day

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

Time ○ All Day

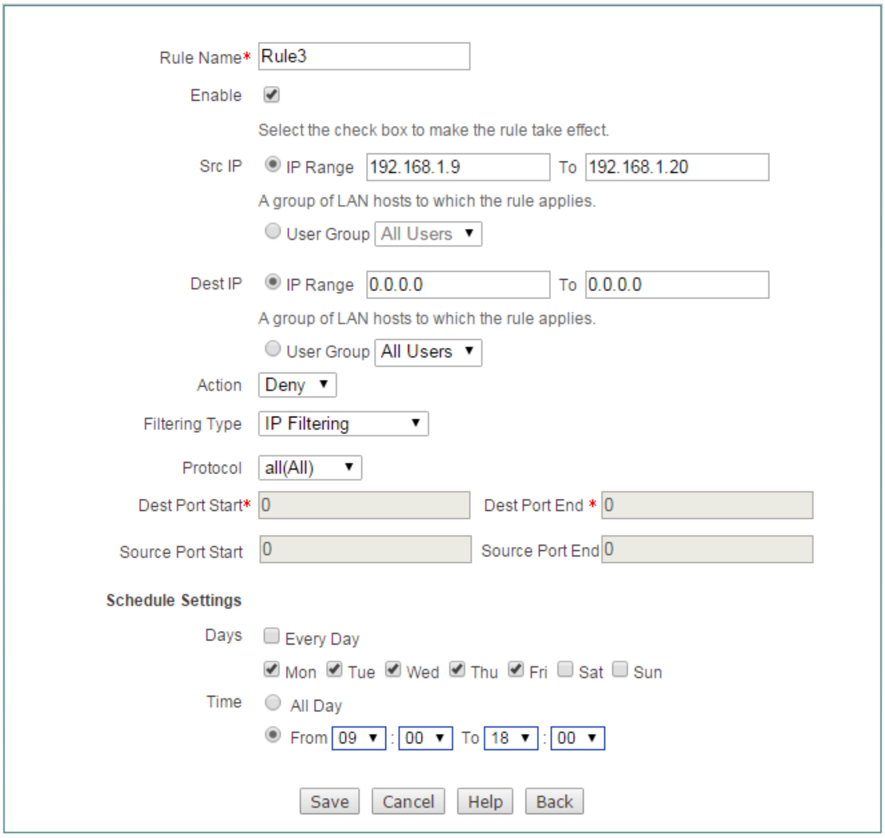
● From 09 ▼ : 00 ▼ To 18 ▼ : 00 ▼

**Figure 9-9 Access Control _Example 1_step 2**

**Step 3** Configuring Access Control Rule 3

Go to **Firewall** > **Access Control** page. Set the Src IP from 192.168.1.9 to 192.168.1.20, select **Deny** from the Action, select IP Filtering from Filtering Type, select all(All) from Protocol , select **Mon** to **Fri** from the Days, select **9:00** to **18:00** from Time, lastly click the **Save** button to save the settings.

}



Rule Name* Rule3

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 192.168.1.9 To 192.168.1.20

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Dest IP ● IP Range 0.0.0.0 To 0.0.0.0

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Deny ▼

Filtering Type IP Filtering ▼

Protocol all(All) ▼

Dest Port Start* 0 Dest Port End * 0

Source Port Start 0 Source Port End 0

Schedule Settings

Days □ Every Day

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

Time ○ All Day

● From 09 ▼ : 00 ▼ To 18 ▼ : 00 ▼

**Figure 9-10 Access Control _Example 1_step 3**

### 9.2.1.5.2 Example Two

#### Requirements

A company uses the Device as a network access device. The requirements are as follows:

Block the users at IP address between 192.168.1.80 to 192.168.1.90 access to http://www.bbc.com (IP address is 29.58.246.93) and http://www.cnn.com (IP address is 157.166.255.18).

#### Analysis

We need to create two access control rules to meet requirements:

- Rule 1: Deny them access to http://www.bbc.com.
- Rule 2: Deny them access to http://www.cnn.com.

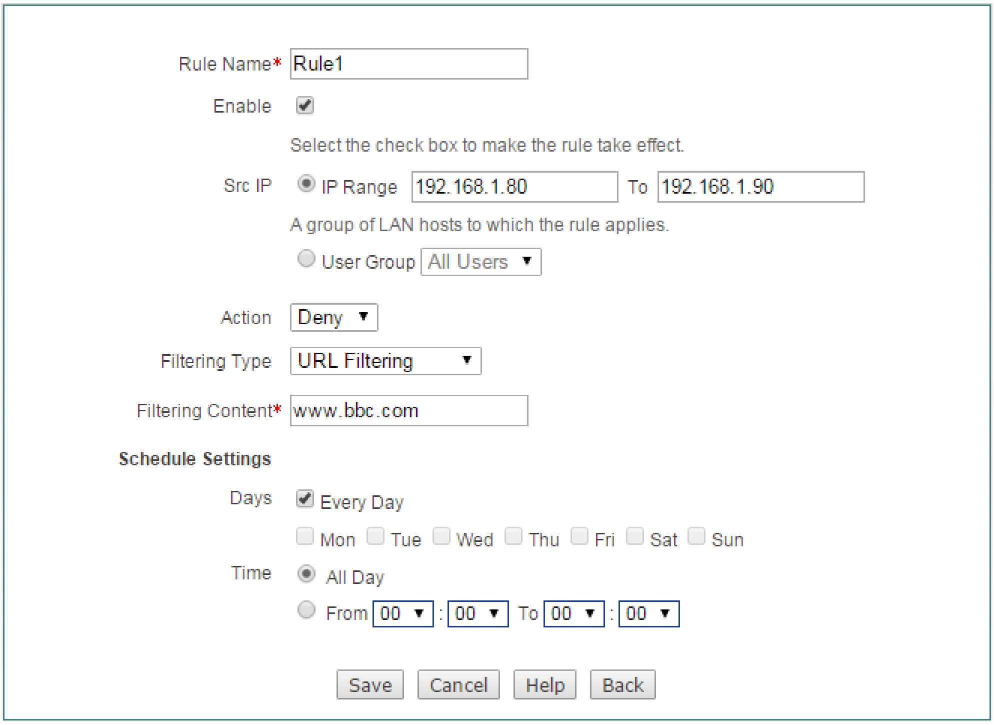
#### Configuration Procedure

**Step 1** Configuring Access Control Rule 1

Go to **Firewall** > **Access Control** page. Set the Src IP from 192.168.1.80 to

}

192.168.1.90, select **Deny** from the Action, select **URL Filtering** from Filtering Type, Enter www.bbc.com at Filtering Content textbox, lastly click the **Save** button to save the settings.



Rule Name* Rule1

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 192.168.1.80 To 192.168.1.90

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Deny ▼

Filtering Type URL Filtering ▼

Filtering Content* www.bbc.com

Schedule Settings

Days ☑ Every Day

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

Time ● All Day

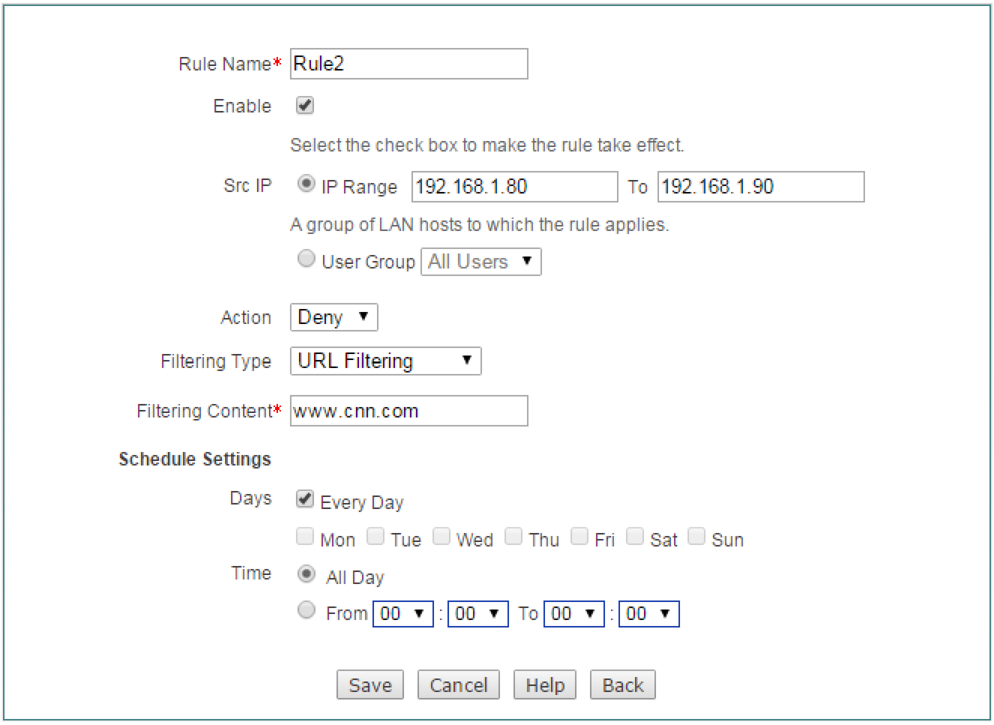
○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

**Figure 9-11 Access Control _Example 2_step 1**

**Step 2** Configuring Access Control Rule 2

Go to **Firewall** > **Access Control** page. Set the Src IP from 192.168.1.80 to 192.168.1.90, select **Deny** from the Action, select **URL Filtering** from Filtering Type, Enter **www.cnn.com** at Filtering Content textbox, lastly click the **Save** button to save the settings.

}



Rule Name* Rule2

Enable ☑

Select the check box to make the rule take effect.

Src IP ● IP Range 192.168.1.80 To 192.168.1.90

A group of LAN hosts to which the rule applies.

○ User Group All Users ▼

Action Deny ▼

Filtering Type URL Filtering ▼

Filtering Content* www.cnn.com

Schedule Settings

Days ☑ Every Day

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

Time ● All Day

○ From 00 ▼ : 00 ▼ To 00 ▼ : 00 ▼

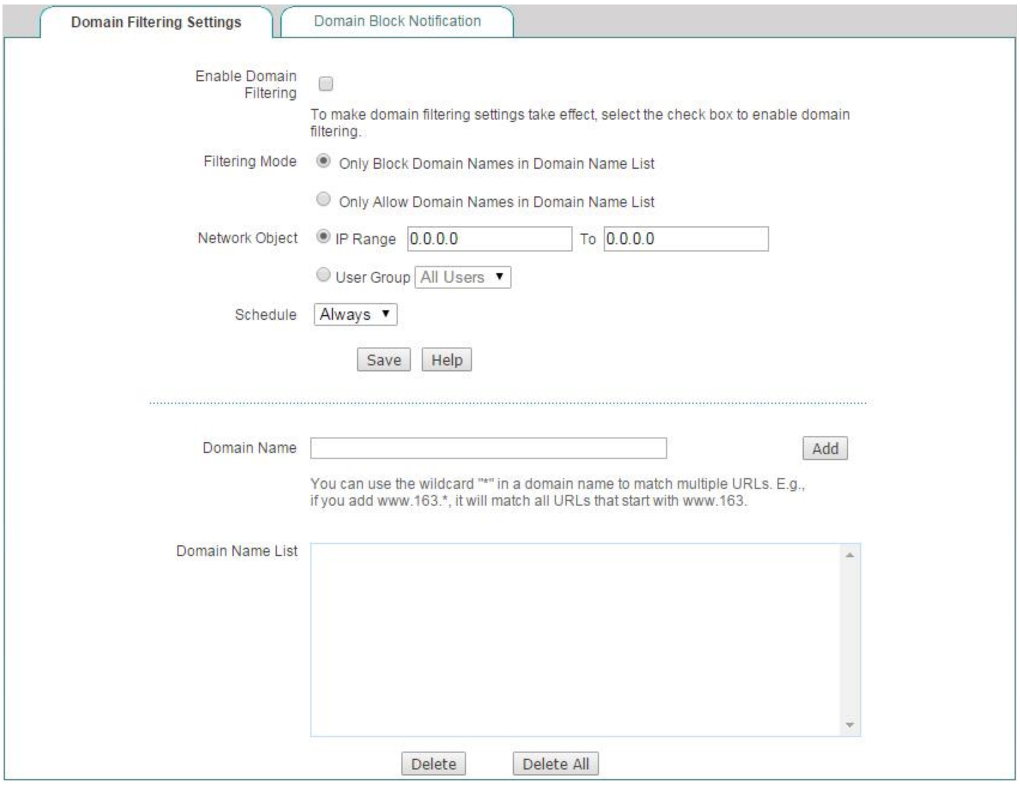
Figure 9-12 Access Control _Example 2_step 2

# 9.3 Domain Filtering

This section describes the steps and notes to setup Domain Filtering on the **Firewall > Domain Filtering** page.

}

### 9.3.1.1 Domain Filtering Settings



Enable Domain Filtering ☐

To make domain filtering settings take effect, select the check box to enable domain filtering.

Filtering Mode ● Only Block Domain Names in Domain Name List

○ Only Allow Domain Names in Domain Name List

Network Object ● IP Range 0.0.0.0 To 0.0.0.0

○ User Group All Users ▼

Schedule Always ▼

Domain Name

You can use the wildcard "*" in a domain name to match multiple URLs. E.g., if you add www.163.*, it will match all URLs that start with www.163.

Domain Name List

**Figure 9-13 Domain Filtering Settings**

- **Enable Domain Filtering:** Select to enable this domain filtering entries

- **Filtering Mode:** Specify the mode of domain filtering. There are two available options:

  - **Only Block Domain Names in Domain Name List:** If selected, the Device will block the LAN users from accessing the domain names in the **Domain Name list**, but allow the users to access any other domain names.

  - **Only Allow Domain Names in Domain Name List:** If selected, the Device will allow the LAN users to access the domain names in the **Domain Name list**, but block the users from accessing any other domain names.

- **Network Object:** Specify the IP addresses of the packets to which the domain filtering rule applies. There are two options:

  - **IP Range:** Specify the start and the end addresses.

  - **User Group:** Select it to choose an address group.

- **Schedule:** Specify the time to which the domain filtering rule applies. You can set the schedule list on the **APP Control > Schedule** page.

**}**

- **Domain Name:** Specify the domain names that will be blocked or allowed according to the **Filtering Mode**. You can create up to 90 domain names in the list.

- **Domain Name List:** Displays the domain names that will be blocked or allowed according to the **Filtering Mode**. You can delete them by clicking the **Delete** button or the **Delete All** button.

**Note:**

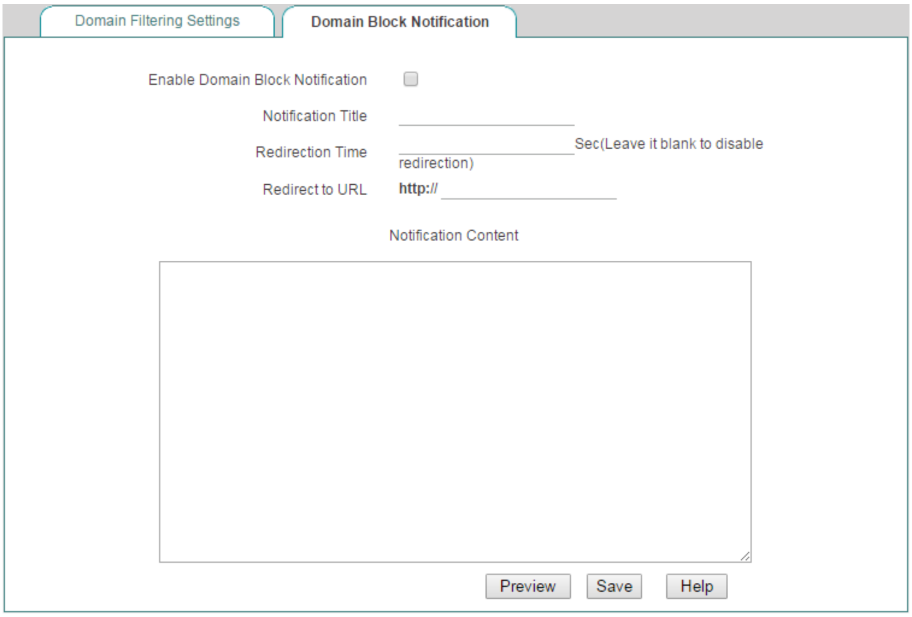
1) The matching rule of domain filtering is whole words matching, that is, only a domain name matches the whole words of the domain name in the **Domain Name List**, the Device will block or allow it according to the **Filtering Mode**.

2) You can use the wildcard "*" in a domain name to match multiple domain names. For example, if you have created www.163.* in the **Domain Name List**, then all the domain names that begin with www.163. will be blocked or allowed according to the **Filtering Mode.**

## 9.3.1.2 Domain Block Notification

This section describes the Security > Domain Filtering > Domain Block Notification page.

When domain block notification is enabled, if a LAN user accesses a domain name which is blocked by the Device, the Device will pop up a notice message to remind the user that the website is blocked rather than network problems.



Enable Domain Block Notification □

Notification Title

Redirection Time Sec(Leave it blank to disable redirection)

Redirect to URL http://

Notification Content

**Figure 9-14 Domain Blocking Notice**

}

- **Enable Domain Block Notification:** If selected, a LAN user accesses a domain name which is blocked by the Device, the Device will pop up a notice message to remind the user. And the requested web page will automatically jump to the specified web page (set on **Redirecting URL**) after the specified time interval (set on **Redirecting Time)**.

- **Notice Title:** Specify the title of the notice message.

- **Redirecting Time:** Specify the time interval after which the requested web page will jump to the specified web page. 0 means that the requested web page will immediately jump to the specified web page. Leave it blank if you don't want the requested web page to jump to any other web page.

- **Redirecting URL:** Specify the redirecting URL to which the requested web page will jump. Leave it blank if you don't want the requested web page to jump to any other web page.

- **Notice Content:** Specify the content of the notice message.

  - **Preview:** Click it to preview the notice message you just configured.

⌖ **Note:**

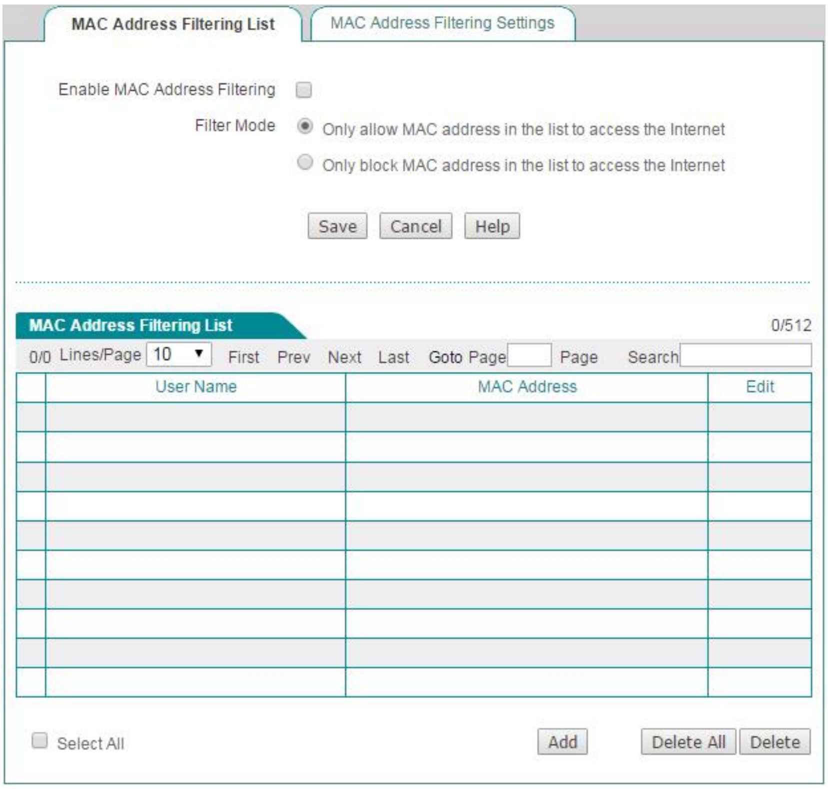
Only after you have enabled domain filtering and chosen the **Only Block Domain Names in Domain Name List** as the filtering mode, the Device will pop up the domain blocking notice messages to the LAN users.

## 9.4 MAC Address Filtering

This section describes the **Firewall > MAC Address Filtering** page. The MAC address filtering is used to filter the wireless clients based on their MAC addresses. With this feature, you can either allow or block specific wireless clients to connect to the Device.

**1) MAC Address Filtering List**

}



Enable MAC Address Filtering □

Filter Mode ● Only allow MAC address in the list to access the Internet

○ Only block MAC address in the list to access the Internet

MAC Address Filtering List 0/512

0/0 Lines/Page 10

| | User Name | MAC Address | Edit |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

□ Select All

Figure 9-15 MAC Address Filtering List

- **Enable MAC Filter:** Select to enable MAC address filtering.

- **Filtering Mode:** Select the mode of MAC address filtering.

  - **Only allow MAC address in the list to access the Internet:** Choose to allow the wireless clients with MAC address listed in **MAC Address Filtering List** to connect to the Device, but block all other wireless clients.

  - **Only block MAC address in the list to access the Internet:** Choose to block the wireless clients with MAC address listed in **MAC Address Filtering List** from connecting to the Device, but allow all other wireless clients.

- **MAC Address Filtering List:** Displays the MAC address filtering entries. You can add or delete them by clicking the **Add** button or the **Delete** button

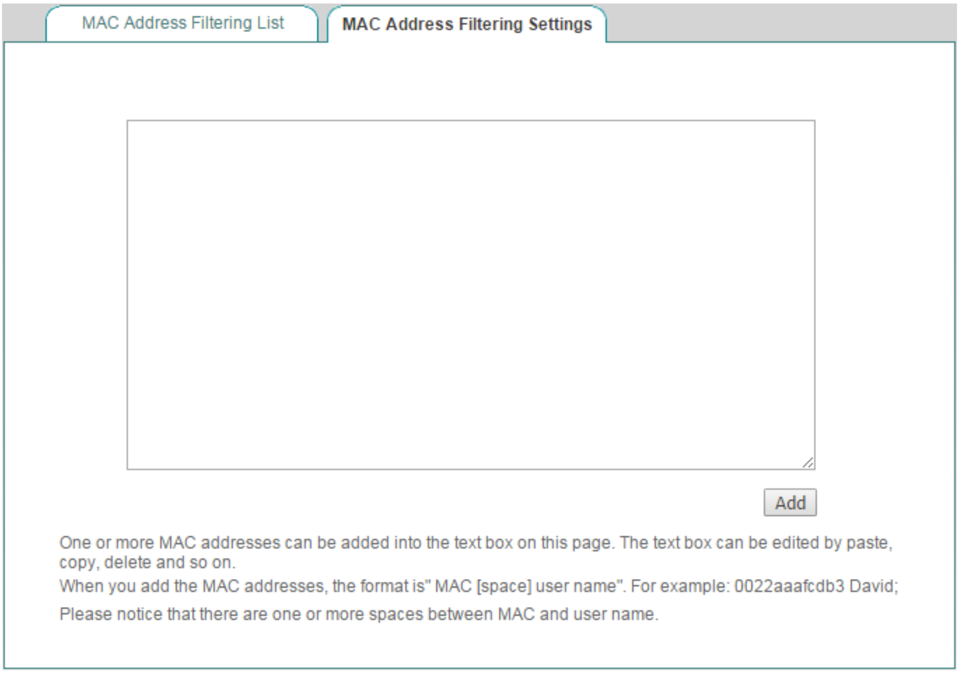
## 2) MAC Address Filtering Settings

You can add more than one MAC address once into the **MAC Address Filtering List** in **Firewall > MAC Address Filtering > MAC Address Filtering Settings** page.

Input or paste the MAC address entries into the textbox on the below figure and click the Add button to save the settings. The format is" MAC address [space] user name". For example: 0022aaafcdb3 David; Please notice that there is one or more spaces between MAC address and user name.

}

}



One or more MAC addresses can be added into the text box on this page. The text box can be edited by paste, copy, delete and so on.

When you add the MAC addresses, the format is" MAC [space] user name". For example: 0022aaafcdb3 David;

Please notice that there are one or more spaces between MAC and user name.

Figure 9-16 MAC Address Filtering Settings

}

# Chapter 10. VPN Menu

## 10.1 Introduction to VPN Technologies

PPTP and IPSec are the two most popular VPN tunneling protocols. Tunneling protocols are at the heart of all VPN implementations. VPN tunneling involves establishing and maintaining a logical network connection, on which the encapsulated packets are transmitted securely.

Tunneling protocols operate at the data link layer (Layer 2) or network layer (Layer 3) of the OSI model. Layer 2 tunneling protocols, such as PPTP, use frames as their unit of exchange, and encapsulate the original packets inside PPP frames before sending them through a VPN tunnel over the Internet. Layer 3 tunneling protocols, such as IPSec (in tunnel mode), use packets as their unit of exchange, and encapsulate IP packets in an additional IP header before sending them through a VPN tunnel over the Internet.

To implement secure data transmission, VPN tunneling protocols also need support one or more security measures to ensure data confidentiality and integrity. Although PPTP have their own advantages, they don't provide effective security measures to thoroughly solve the problem of tunnel and data encryption. Compared with PPTP, IPSec provides a higher level of security including data confidentiality (encryption), network-level peer authentication, data origin authentication, data integrity, as well as replay protection. IPSec provides two security mechanisms: encryption and authentication. Encryption mechanism is used to ensure data confidentiality (prevent eavesdropping); and authentication mechanism is used to ensure that data is from the initial sender and not destroyed or tampered during transmission. In short, IPSec provides transparent security services to protect communications over IP networks against eavesdropping and tampering and other network attacks.

Although PPTP are not as secure as IPSec, they still can meet the security requirements of most organizations; in addition, they have several advantages over IPSec, such as ease of use, low-cost and ease of deployment. On the other hand, although IPSec has a higher security and reliability, it is usually more complicated to deploy; and it is subjected to certain restrictions, for example, some NAT devices don't support IPSec pass-through. Therefore, before building your VPN infrastructure, you should choose an appropriate tunneling protocol for your VPN according to the actual needs.

Because most Windows operating systems (such as Windows 2000, XP, Vista, 7, etc.) have built-in PPTP client software, a Windows 2000/XP/Vista/7-based computer can act as a PPTP client to establish an end-to-site VPN tunnel (also known as remote access or dial up VPN) with a VPN appliance acting as a PPTP server. In addition, Windows 2000 and newer versions of Windows have built-in support for IPSec.

# 10.2 PPTP

PPTP is a VPN tunneling protocol which encapsulates PPP frames in IP packets for transmission over a public IP network such as the Internet. PPTP is based on client/server model. The PPTP client initiates a PPTP connection to the server, while the PPTP server accepts the incoming PPTP connection from the client. PPTP is often used to implement remote access VPNs over an IP network (such as a broadband network), to extend the reach of your Intranet.

## 10.2.1.1 Introduction to PPTP Implementation

As mentioned earlier, PPTP is used to encapsulate PPP frames in IP packets for transmission over a public IP network such as the Internet. The PPTP client or server encapsulates the original user packets inside PPP frames before sending them through a PPTP tunnel over the Internet; while the peer performs decapsulation firstly, and then forward the original packets to their intended destinations.

As shown in the following figure, the typical application of PPTP is that some laptop or desktop computers act as the PPTP client devices, that is, some employees in the remote branch offices or mobile users (traveling employees, telecommuters, etc.) use the Windows built-in PPTP client software to initiate PPTP connections to the server; the Device deployed at the head office acts as a PPTP server device, which accepts the PPTP incoming connections from the clients. After a PPTP tunnel has been established between the PPTP client and server, the PPTP server will receive the PPTP packets from the client firstly, and then perform decapsulation, lastly forward the original packets to their intended destinations.

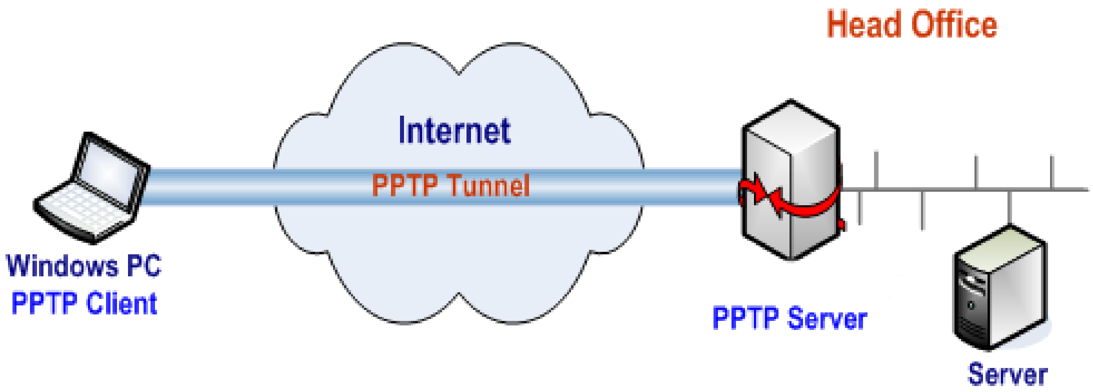


**Figure 10-1 Typical Application of PPTP**

The Device can function as a PPTP client or server; or both, that is, it is the PPTP client for some tunnels and PPTP server for other tunnels. When the Device functions as the PPTP client and server at the same time, on the one hand it can receive the packets from other PPTP client devices; on the other hand it can transmit the received packets to other PPTP server devices.

As shown in the following figure, to securely connect an enterprise's branch office with its head office, and connect some mobile users with both the branch office and head office, a Device at the branch office is configured to function as both the PPTP client and server: it functions as a PPTP client to establish a PPTP tunnel with

}

another Device that functions as a PPTP server at the head office; and at the same time, it also functions as a PPTP server to receive the packets from the mobile users, and transmit those packets destined for the head office internal network to the Device at the head office, thus the mobile users can access both the branch office and head office internal networks.

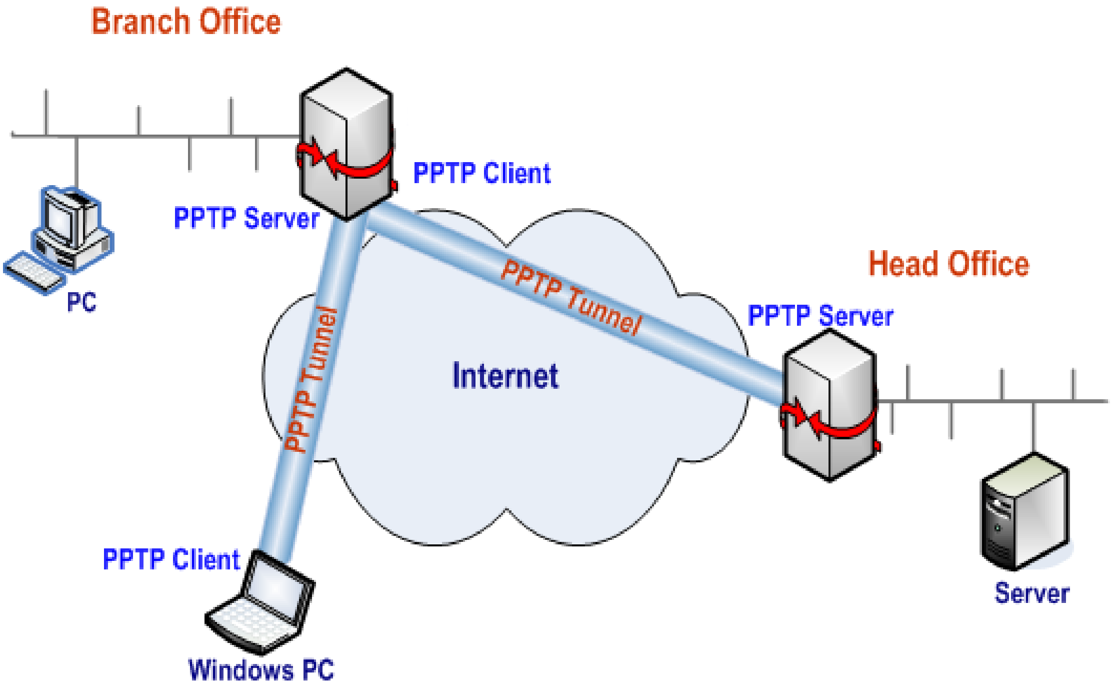


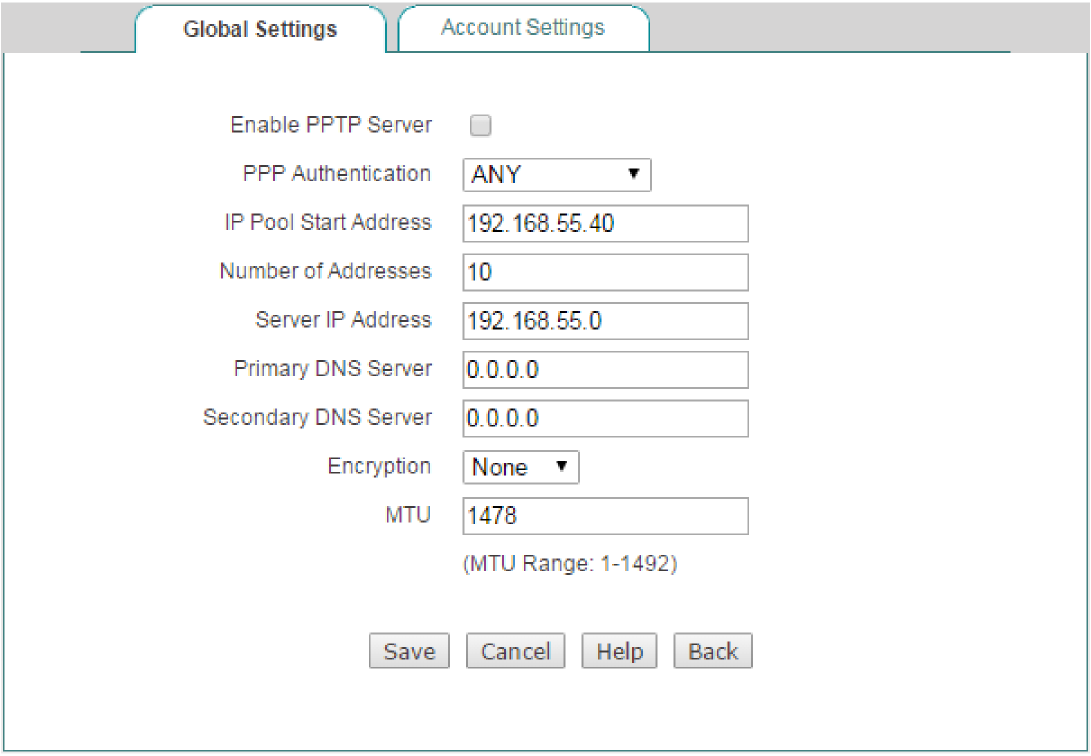
**Figure 10-2 A PPTP VPN scenario for Mobile Users**

### 10.2.1.2 PPTP Server settings

On the **VPN** > **PPTP** page, click the **Add Server** button to setup PPTP Server.

}

## 10.2.1.3 Global Settings



|  |  |
|---|---|
| Enable PPTP Server | □ |
| PPP Authentication | ANY ▼ |
| IP Pool Start Address | 192.168.55.40 |
| Number of Addresses | 10 |
| Server IP Address | 192.168.55.0 |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Encryption | None ▼ |
| MTU | 1478 |
|  | (MTU Range: 1-1492) |

**Figure 10-3 PPTP Server_Global Settings**

- **Enable PPTP Server:** Select to enable PPTP Server.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** The Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** The Device will automatically negotiate it with the remote VPN appliance.

- **IP Pool Start Address:** Specify the starting IP address assigned from the VPN address pool.

- **Number of Address:** Specify the maximum number of IP addresses that can be assigned from the VPN address pool.

}

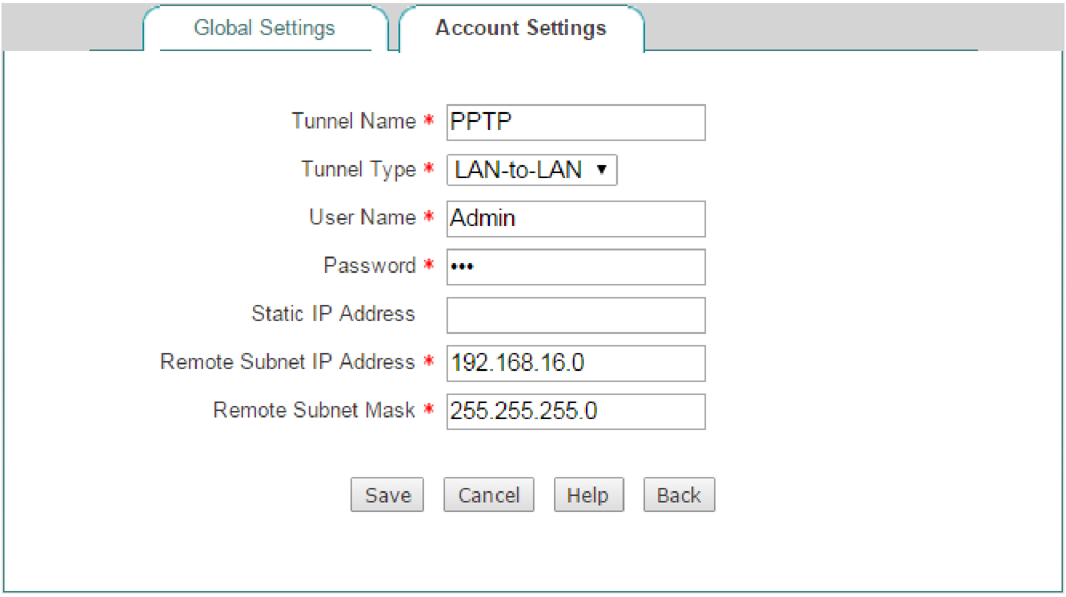
- **Server IP Server:** Specify the IP addresses of the VPN Server. This address should be on the same network segment with the VPN address pool but not including.

- **Primary / Secondary DNS Server:** When the device is setup to as the PPTP server, it can assign DNS address to the client to access internet.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.4 Account Settings



Tunnel Name * PPTP

Tunnel Type * LAN-to-LAN ▾

User Name * Admin

Password * •••

Static IP Address

Remote Subnet IP Address * 192.168.16.0

Remote Subnet Mask * 255.255.255.0

**Figure 10-4 PPTP Server_Account Settings**

- **Tunnel Name:** Specify the name of this tunnel.

- **Tunnel Type:** Specify the type of the PPTP tunnel.

  - **LAN-to-LAN:** If selected, two LAN sites can securely connect with each other over public networks like the Internet. All traffic from one LAN destined for the other one is tunneled, without individual hosts having to use VPN clients. In this case, either a Device or compatible VPN appliance can act as a PPTP client.

  - **Mobile User**: If selected, the remote individual users can securely connect the server over public networks like the Internet. In this case, a laptop or desktop computer will act as a PPTP client.

}

- **User Name:** Specify a unique user name of the PPTP client. It should be between 1 and 31 characters long. The PPTP server will use the **User Name** and **Password** to identify the remote PPTP client.

- **Password:** Specify the password of the PPTP client.

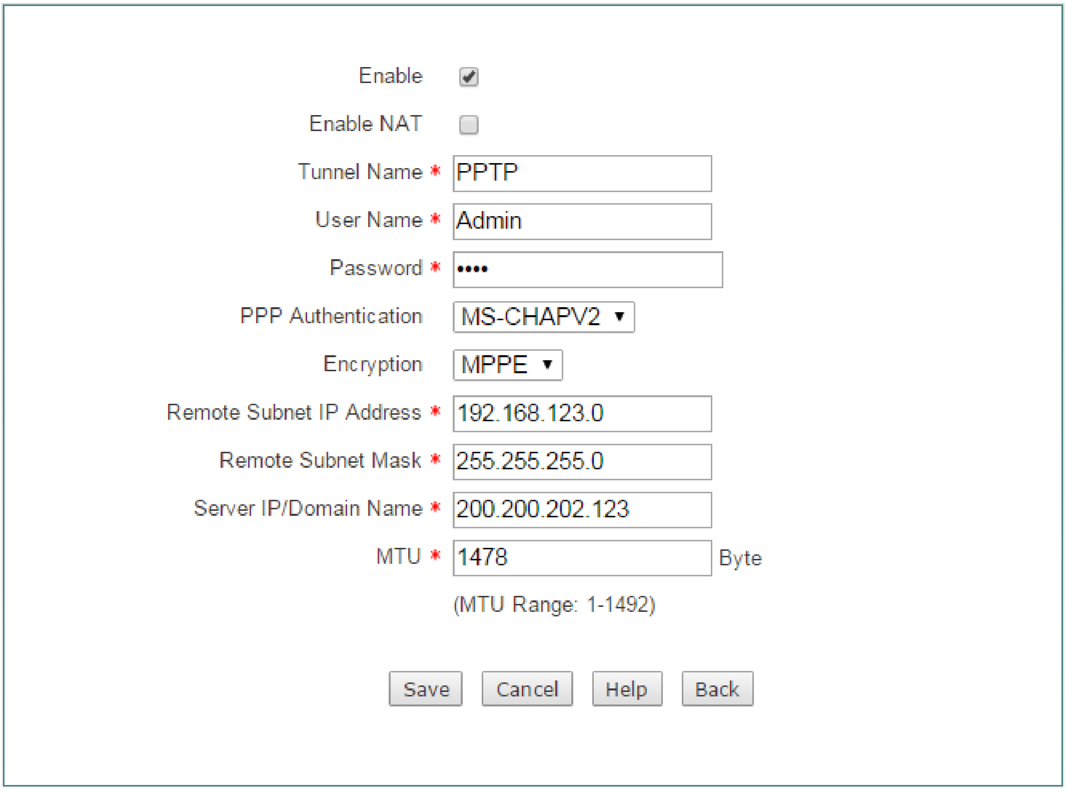
- **Static IP Address:** Specify the IP address the PPTP server assigns to PPTP client. Note this IP Address you set should be inside the VPN address pool.

- **Remote Subnet IP Address:** Specify the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface. If you choose **Mobile User** as the **Tunnel Type**, the system will automatically generate the **Remote Subnet IP Address** and **Remote Subnet Mask**.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

## 10.2.1.5 Client Settings

On the **VPN** > **PPTP** page, click the **Add Client** button to setup PPTP client.



Enable ☑

Enable NAT ☐

Tunnel Name * PPTP

User Name * Admin

Password * ••••

PPP Authentication MS-CHAPV2 ▾

Encryption MPPE ▾

Remote Subnet IP Address * 192.168.123.0

Remote Subnet Mask * 255.255.255.0

Server IP/Domain Name * 200.200.202.123

MTU * 1478 Byte

(MTU Range: 1-1492)

**Figure 10-5 PPTP Client Settings**

- **Enable:** Select to enable PPTP client.

- **Enable NAT:** If selected, it will only allow unidirectional access from the PPTP client side LAN to the server side LAN.

}

- **Tunnel Name:** Specify a unique name for the PPTP tunnel.

- **User Name:** Specify the user name of the PPTP client.

- **Password:** Specify the password of the PPTP client.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** the Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** If selected, the Device will automatically negotiate it with the remote VPN appliance.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **Remote Subnet IP Address:** Specify the IP address of the remote network.

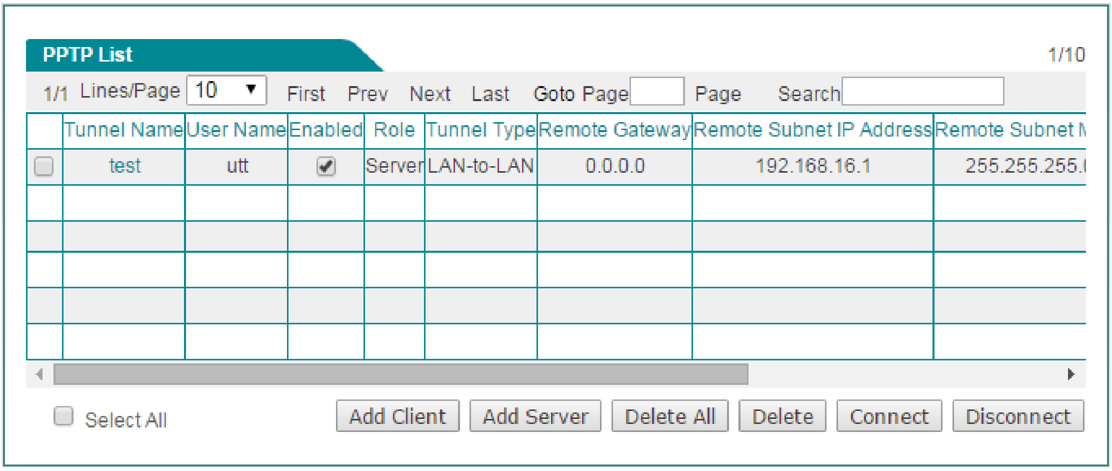
- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

- **Server IP/Domain Name:** The public IP address or domain name of the remote PPTP server.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.6 PPTP List

After you have configured a PPTP client or server entry, you can view its configuration and status information in the **PPTP List**.



PPTP List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | Tunnel Name | User Name | Enabled | Role | Tunnel Type | Remote Gateway | Remote Subnet IP Address | Remote Subnet |
|---|---|---|---|---|---|---|---|---|
| □ | test | utt | ☑ | Server | LAN-to-LAN | 0.0.0.0 | 192.168.16.1 | 255.255.255. |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**Figure 10-6 PPTP List**

## 10.2.1.7 Example of PPTP

In this scenario, a company’s head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet. In addition, some mobile users (traveling employees, telecommuters, etc.) want to securely access the head office’s internal network over the Internet.

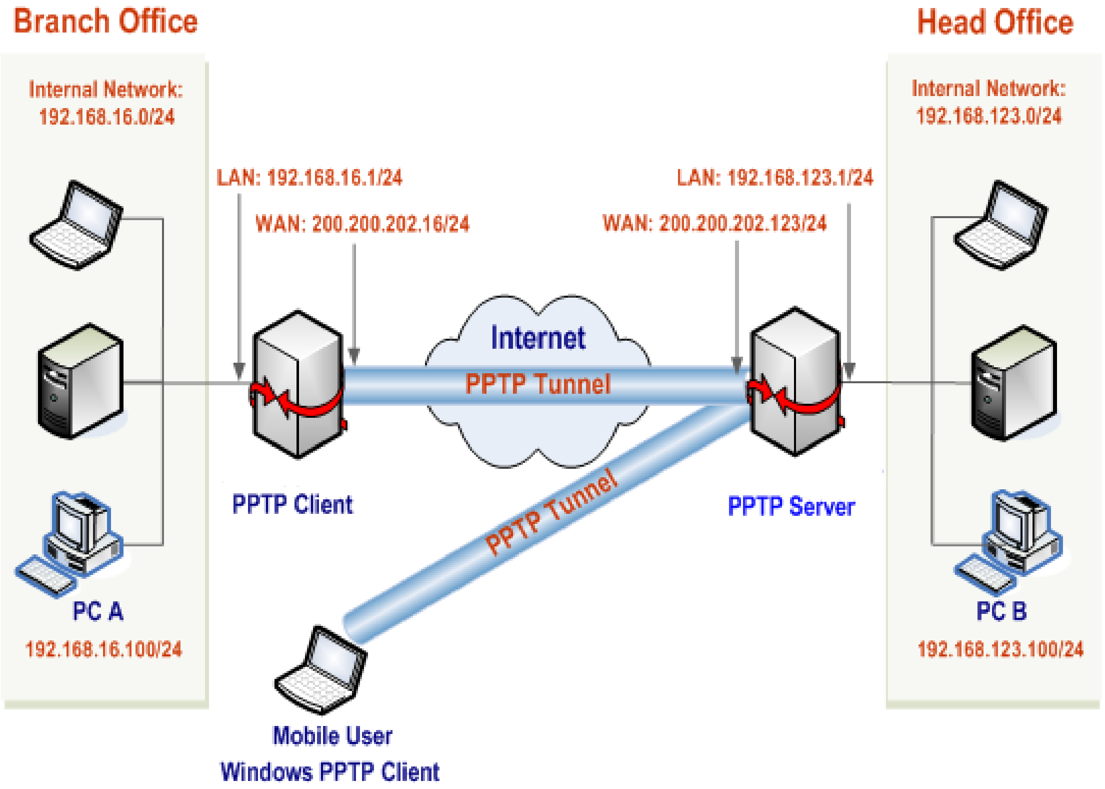


**Figure 10-7 Network Topology – the Device Acts as a PPTP Server**

We will use PPTP to establish VPN tunnels, deploy a enterprise wireless router

}

acting as a PPTP server at the head office, and another VPN appliance acting as a PPTP client at the branch office. And the mobile users will use the Windows XP built-in PPTP client. The IP addresses are as follows:

The Device (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.123/255.255.255.0

The VPN appliance (PPTP Client) at the branch office:

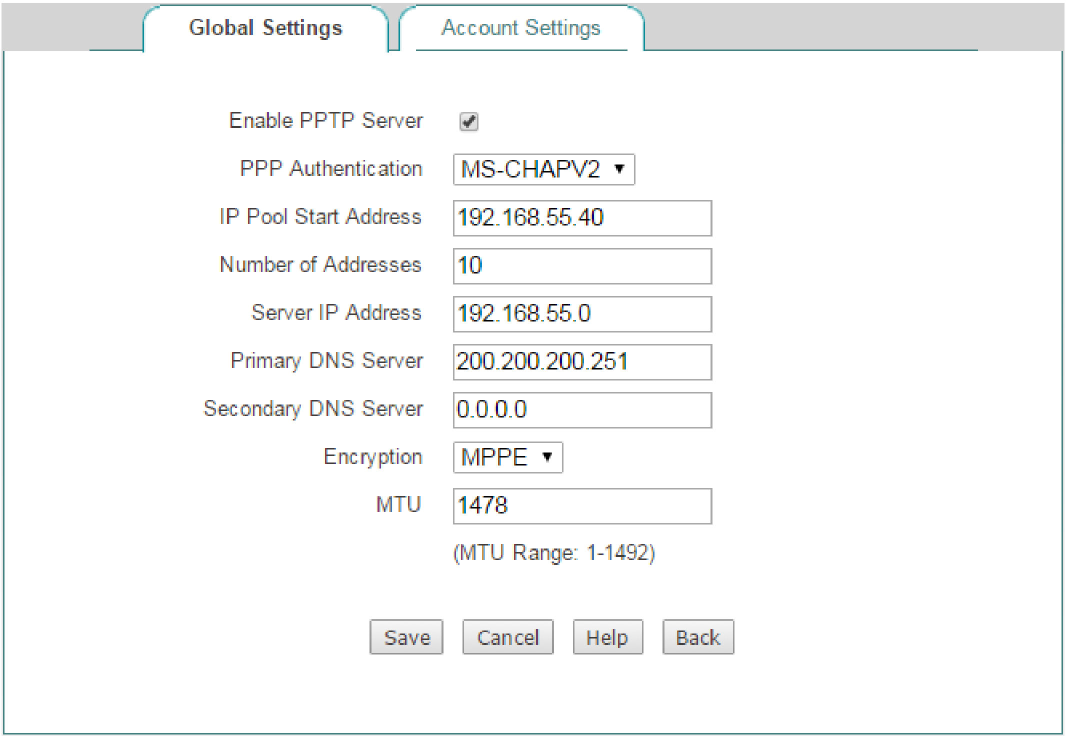
- LAN Subnet: 192.168.16.0/255.255.255.0
- LAN Interface IP Address: 192.168.16.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.16/255.255.255.0

**The mobile users:**

A mobile user with any public IP address can use the Windows XP built-in PPTP client to connect to the Device.

1) Configuring Head office’s Device as a PPTP Server (LAN-to-LAN and Mobile User)

Go to **VPN > PPTP** page, click the **Add Server** button and then make settings as the following figure, lastly click the **Save** button.



Enable PPTP Server ☑

PPP Authentication: MS-CHAPV2

IP Pool Start Address: 192.168.55.40

Number of Addresses: 10

Server IP Address: 192.168.55.0

Primary DNS Server: 200.200.200.251

Secondary DNS Server: 0.0.0.0

Encryption: MPPE

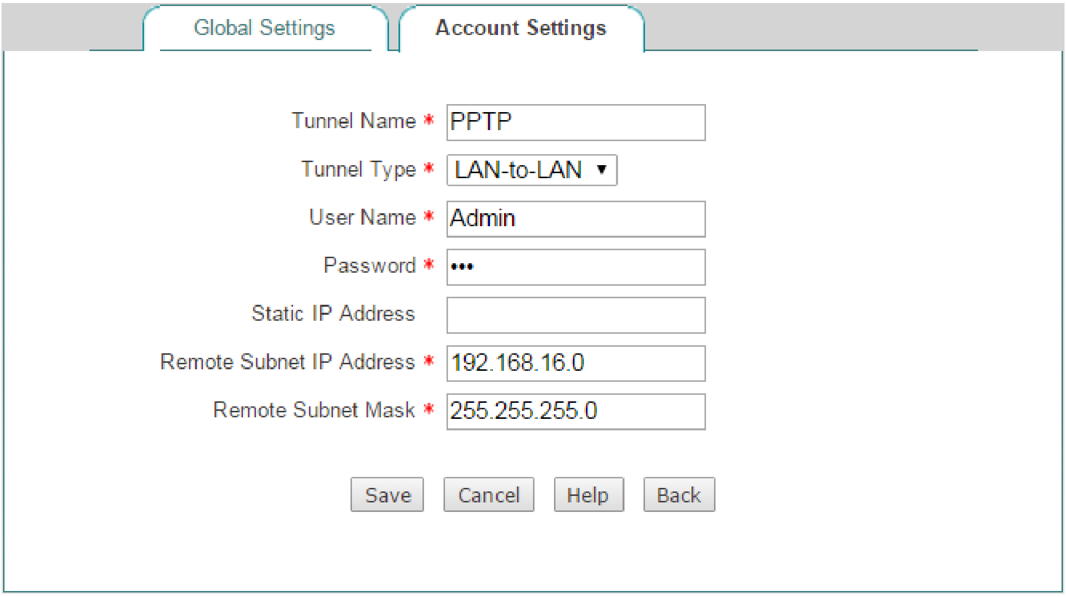
MTU: 1478

(MTU Range: 1-1492)

**Figure 10-8 PPTP Server Settings**

(1) Creating a LAN-to-LAN PPTP Server Account for the Branch Office

Click the **Account Settings** tab and make settings as the following figure, lastly click the **Save** button.



Tunnel Name *: PPTP

Tunnel Type *: LAN-to-LAN

User Name *: Admin

Password *: •••

Static IP Address:

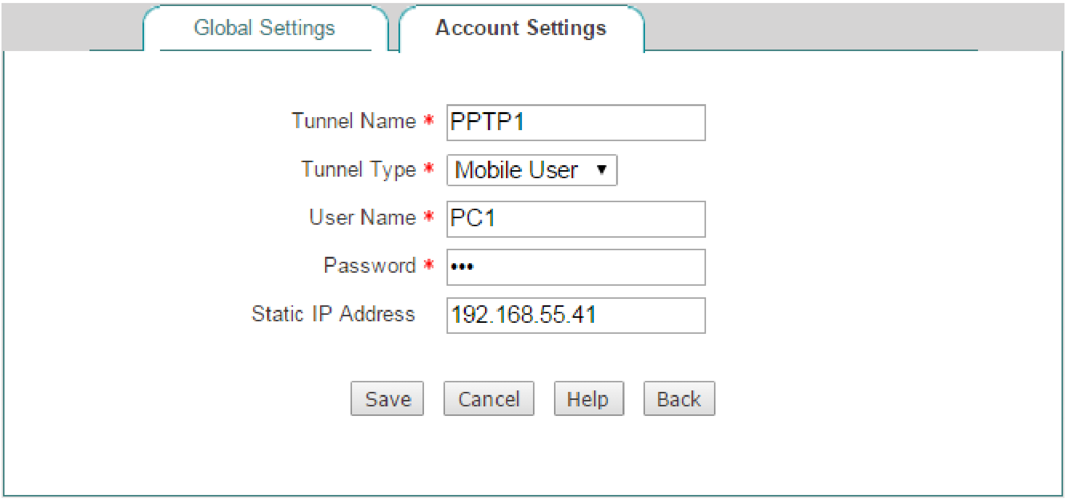
Remote Subnet IP Address *: 192.168.16.0

Remote Subnet Mask *: 255.255.255.0

**Figure 10-9 PPTP Server Settings_LAN-to-LAN**

(2) Creating a Mobile User Server Account for Mobile Users

}



Tunnel Name * PPTP1

Tunnel Type * Mobile User ▾

User Name * PC1

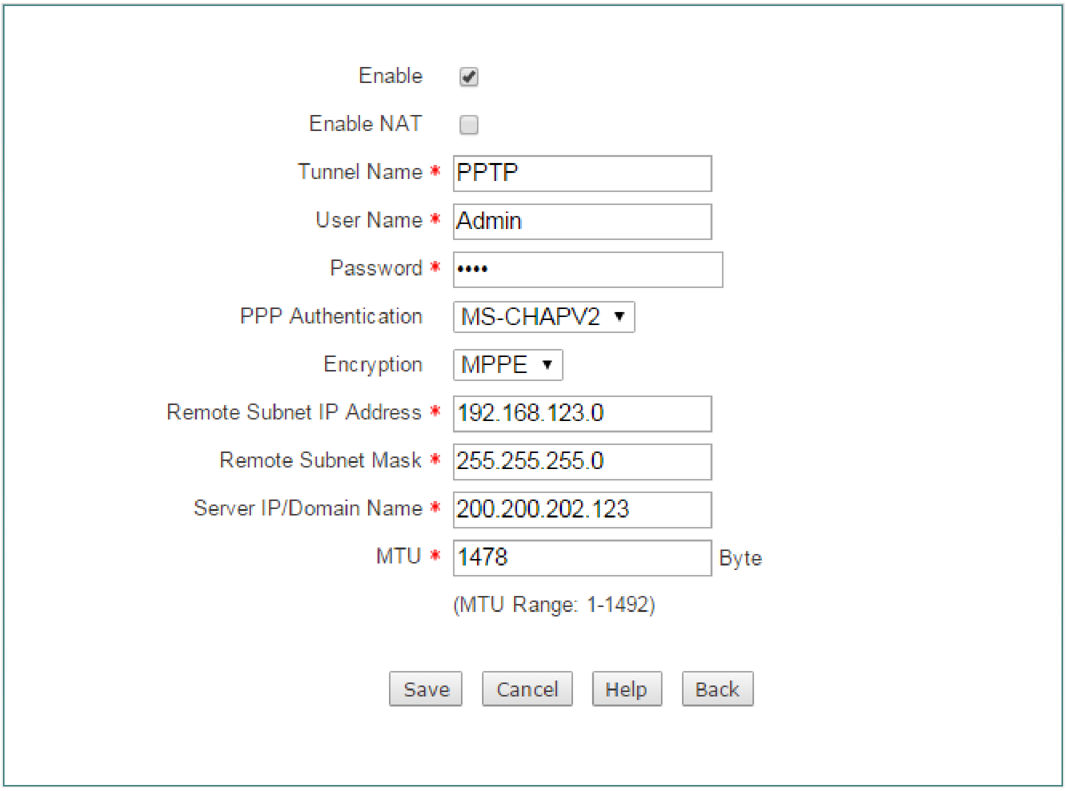
Password * •••

Static IP Address 192.168.55.41

**Figure 10-10 PPTP Server Settings_Mobile User**

2) Configuring Branch office's Device as a PPTP Client

Go to **VPN > PPTP** page, click the **Add Client** button and then make settings as the following figure, lastly click the **Save** button.



Enable ☑

Enable NAT □

Tunnel Name * PPTP

User Name * Admin

Password * ••••

PPP Authentication MS-CHAPV2 ▾

Encryption MPPE ▾

Remote Subnet IP Address * 192.168.123.0

Remote Subnet Mask * 255.255.255.0

Server IP/Domain Name * 200.200.202.123

MTU * 1478 Byte

(MTU Range: 1-1492)

**Figure 10-11 PPTP Client settings**

3) Configuring a Windows XP-based Computer as a PPTP Client (Mobile User)

Do the following steps on a Windows XP-based computer to configure it as a PPTP client.

}

(1) Creating the PPTP Dial-up Connection

a) Go to **Start > Settings > Control Panel**, and select the **Switch to Category View**.

b) Select the **Network and Internet Connections.**

c) Select the **Create** a **connection to the network at my workplace**.

d) Select the **Virtual Private Network connection** option, and then click the **Next** button.

e) Enter a name for the connection (**PPTP** in this example) in the **Company Name** text box, and then click the **Next** button.

f) Select the **Do not dial the initial connection** option, and then click the **Next** button.

g) Enter the remote PPTP server's IP address (**200.200.202.123** in this example) in the **Host name or IP address** text box, and then click the **Next** button.

h) Click the **Finish** button.

i) Double click the new connection **PPTP**, and click the **Properties** button.

j) Select the **Security** tab, select the **Advanced (custom settings)** option and click the **Settings** button.

k) Select **Optional Encryption (connect even if no encryption)** from the **Data encryption drop-down list.**

l) Select the **Unencrypted password (PAP)**, **Challenge Handshake Authentication Protocol (CHAP)**, and **Microsoft CHAP (MS-CHAP)** check boxes in the **Allow these protocols**, and then click the **OK** button.

m) Select the **Networking** tab, select **PPTP VPN** from the **Type of VPN** drop-down list.

n) Make sure that the **Internet Protocol (TCP/IP)** check box is checked.

o) Make sure that the **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, **File and Printer Sharing for Microsoft Networks**, and **Client for Microsoft Networks** check boxes are cleared.

p) Click the **OK** button to save the changes to make them take effect.

(2) Connect the Computer to the Device through the PPTP Tunnel

a) Please make sure that your computer has been connected to the Internet.

b) Double-click the new connection **PPTP** you have just created.

c) Enter **PC1** in the **User name** text box and **PC1** in the **Password** text box.

d) Click the **Connect** button.

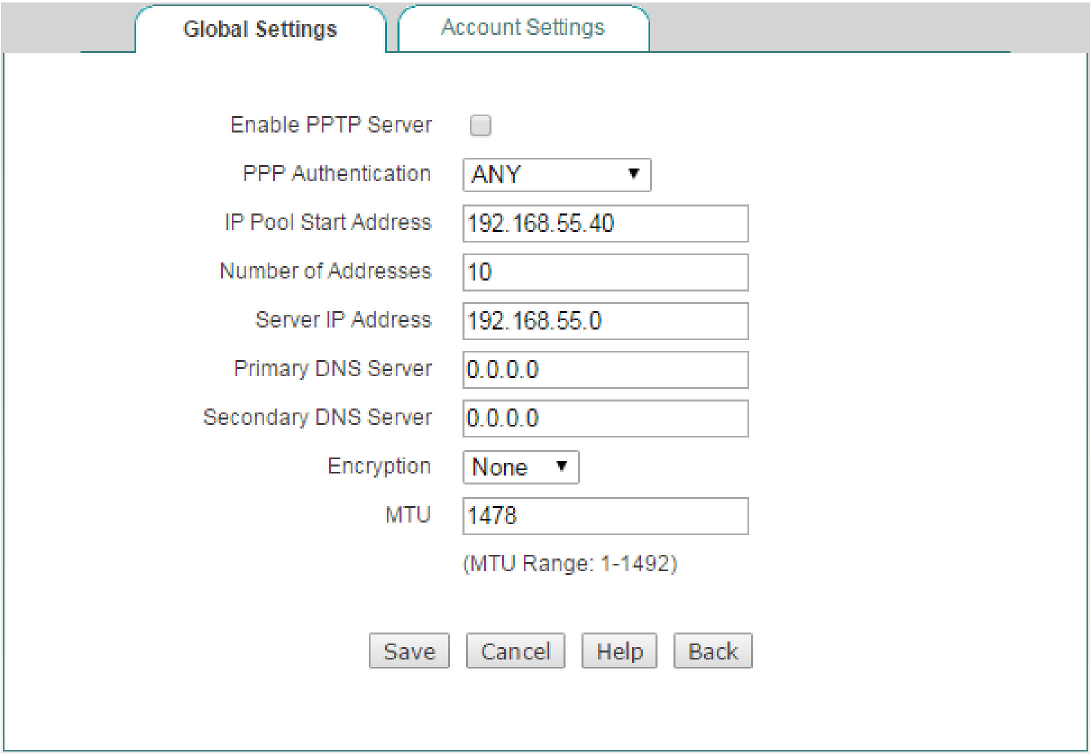
e) After the PPTP tunnel has been established successfully, if you run the **ipconfig** command at the MS-DOS command prompt on the computer, you can see the IP address assigned by the Device.

}

### 10.2.1.8 PPTP Server settings

On the **VPN** > **PPTP** page, click the **Add Server** button to setup PPTP Server.

### 10.2.1.9 Global Settings



Enable PPTP Server □

PPP Authentication ANY

IP Pool Start Address 192.168.55.40

Number of Addresses 10

Server IP Address 192.168.55.0

Primary DNS Server 0.0.0.0

Secondary DNS Server 0.0.0.0

Encryption None

MTU 1478

(MTU Range: 1-1492)

**Figure 10-12 PPTP Server_Global Settings**

- **Enable PPTP Server:** Select to enable PPTP Server.
- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.
  - **PAP:** Password Authentication Protocol.
  - **CHAP:** Challenge Handshake Authentication Protocol.
  - **MS-CHAPV2:** The Microsoft version of the Challenge-Handshake Authentication Protocol.
  - **ANY:** The Device will automatically negotiate it with the remote VPN appliance.
- **IP Pool Start Address:** Specify the starting IP address assigned from the VPN address pool.

}

- **Number of Address:** Specify the maximum number of IP addresses that can be assigned from the VPN address pool.

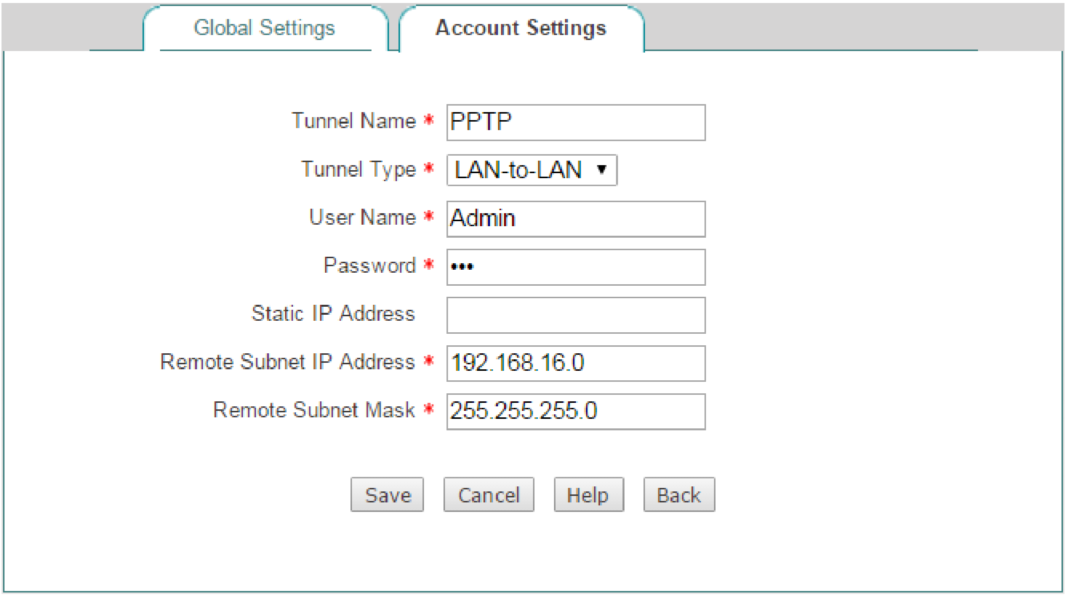
- **Server IP Server:** Specify the IP addresses of the VPN Server. This address should be on the same network segment with the VPN address pool but not including.

- **Primary / Secondary DNS Server:** When the device is setup to as the PPTP server, it can assign DNS address to the client to access internet.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.10 Account Settings



Tunnel Name * PPTP

Tunnel Type * LAN-to-LAN ▾

User Name * Admin

Password * •••

Static IP Address

Remote Subnet IP Address * 192.168.16.0

Remote Subnet Mask * 255.255.255.0

**Figure 10-13 PPTP Server_Account Settings**

- **Tunnel Name:** Specify the name of this tunnel.

- **Tunnel Type:** Specify the type of the PPTP tunnel.

  - **LAN-to-LAN:** If selected, two LAN sites can securely connect with each other over public networks like the Internet. All traffic from one LAN destined for the other one is tunneled, without individual hosts having to use VPN clients. In this case, either a Device or compatible VPN appliance can act as a PPTP client.

}

- **Mobile User**: If selected, the remote individual users can securely connect the server over public networks like the Internet. In this case, a laptop or desktop computer will act as a PPTP client.

- **User Name:** Specify a unique user name of the PPTP client. It should be between 1 and 31 characters long. The PPTP server will use the **User Name** and **Password** to identify the remote PPTP client.

- **Password:** Specify the password of the PPTP client.

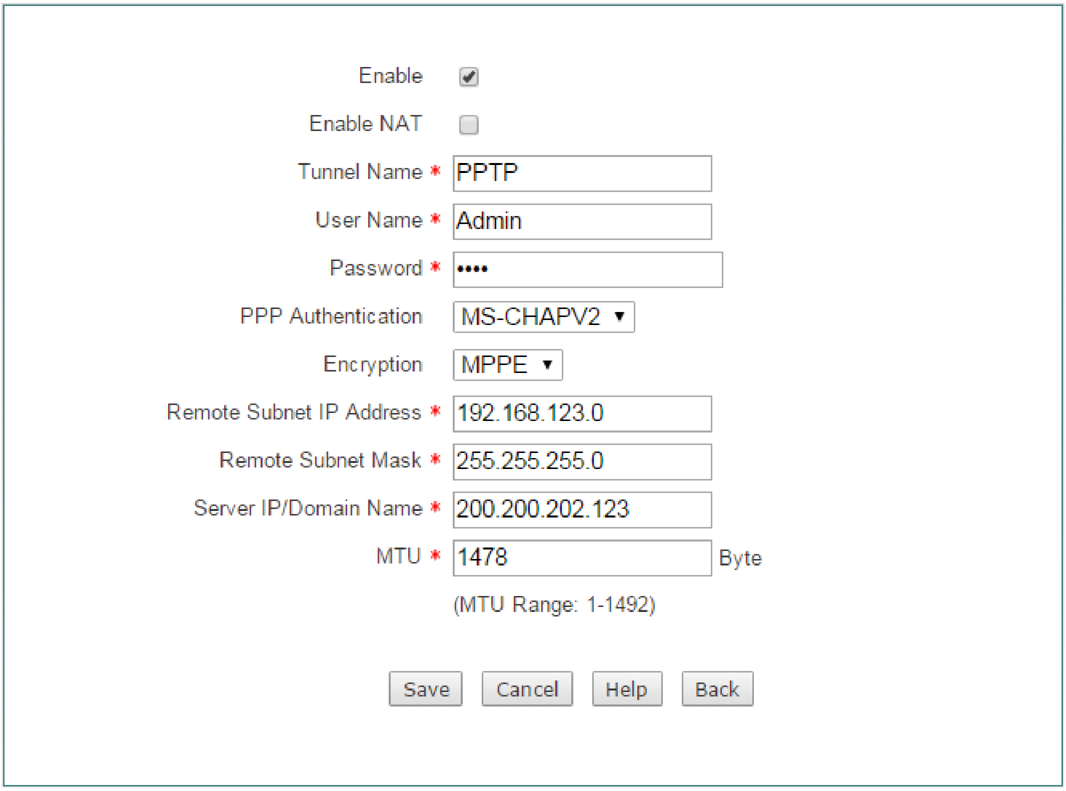
- **Static IP Address:** Specify the IP address the PPTP server assigns to PPTP client. Note this IP Address you set should be inside the VPN address pool.

- **Remote Subnet IP Address:** Specify the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface. If you choose **Mobile User** as the **Tunnel Type**, the system will automatically generate the **Remote Subnet IP Address** and **Remote Subnet Mask**.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

## 10.2.1.11 Client Settings

On the **VPN** > **PPTP** page, click the **Add Client** button to setup PPTP client.



| | |
|---|---|
| Enable | ☑ |
| Enable NAT | □ |
| Tunnel Name * | PPTP |
| User Name * | Admin |
| Password * | •••• |
| PPP Authentication | MS-CHAPV2 ▼ |
| Encryption | MPPE ▼ |
| Remote Subnet IP Address * | 192.168.123.0 |
| Remote Subnet Mask * | 255.255.255.0 |
| Server IP/Domain Name * | 200.200.202.123 |
| MTU * | 1478 Byte |
| | (MTU Range: 1-1492) |

**Figure 10-14 PPTP Client Settings**

- **Enable:** Select to enable PPTP client.

}

- **Enable NAT:** If selected, it will only allow unidirectional access from the PPTP client side LAN to the server side LAN.

- **Tunnel Name:** Specify a unique name for the PPTP tunnel.

- **User Name:** Specify the user name of the PPTP client.

- **Password:** Specify the password of the PPTP client.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** the Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** If selected, the Device will automatically negotiate it with the remote VPN appliance.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **Remote Subnet IP Address:** Specify the IP address of the remote network.

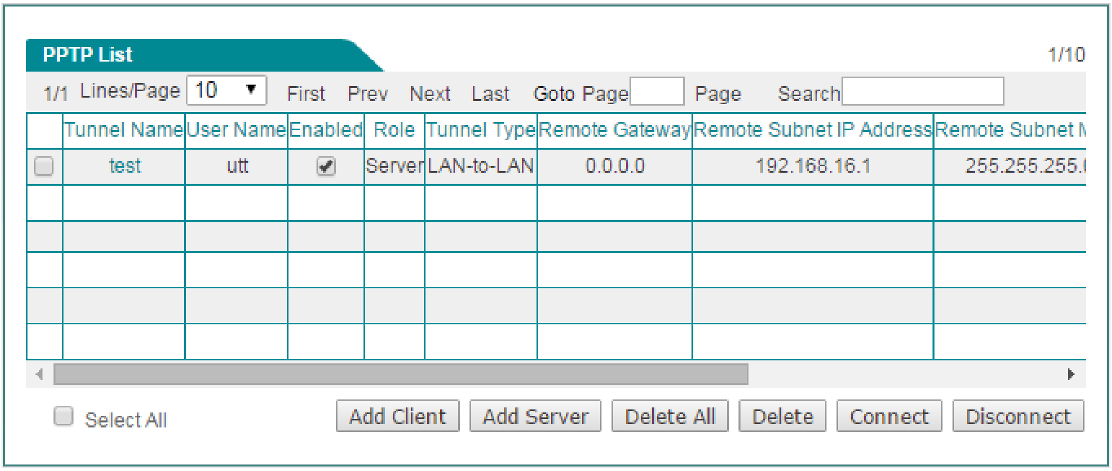
- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

- **Server IP/Domain Name:** The public IP address or domain name of the remote PPTP server.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.12 PPTP List

After you have configured a PPTP client or server entry, you can view its configuration and status information in the **PPTP List**.


PPTP List
1/10
1/1 Lines/Page 10 First Prev Next Last Goto Page Page Search

| | Tunnel Name | User Name | Enabled | Role | Tunnel Type | Remote Gateway | Remote Subnet IP Address | Remote Subnet M |
|---|---|---|---|---|---|---|---|---|
| ☐ | test | utt | ☑ | Server | LAN-to-LAN | 0.0.0.0 | 192.168.16.1 | 255.255.255. |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Figure 10-15 PPTP List

## 10.2.1.13 Example of PPTP

In this scenario, a company's head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet. In addition, some mobile users (traveling employees, telecommuters, etc.) want to securely access the head office's internal network over the Internet.

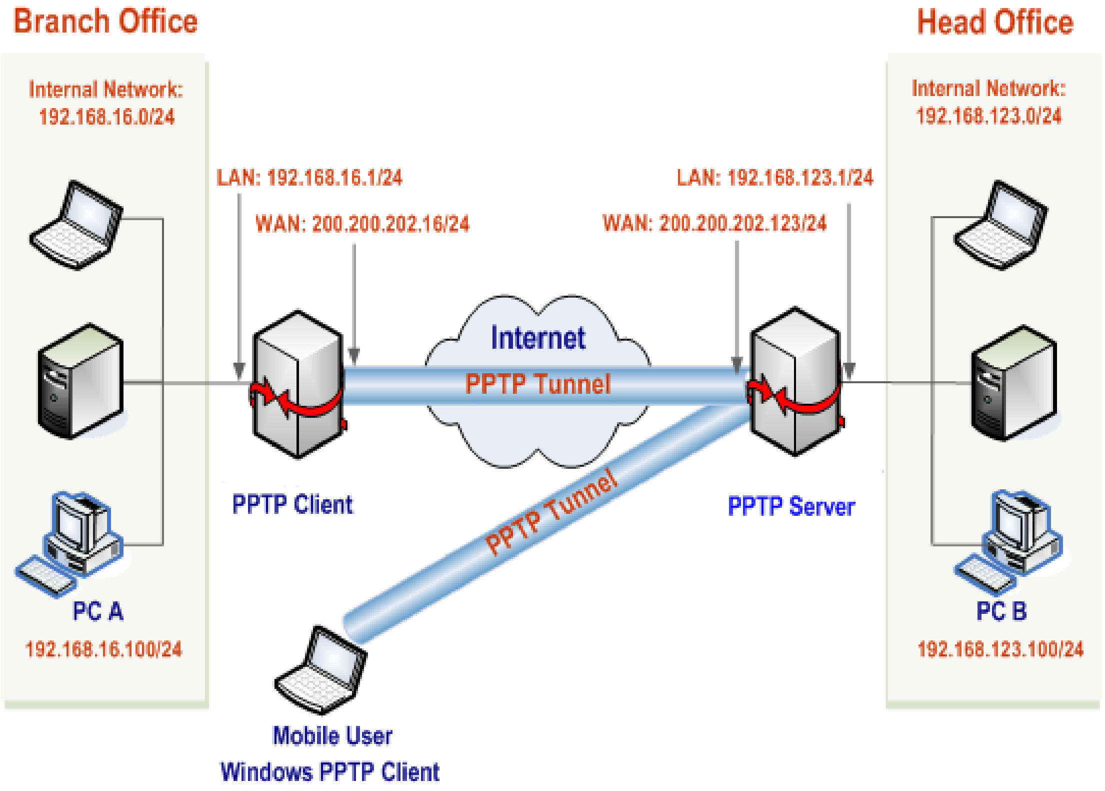


Figure 10-16 Network Topology – the Device Acts as a PPTP Server

We will use PPTP to establish VPN tunnels, deploy a enterprise wireless router

}

acting as a PPTP server at the head office, and another VPN appliance acting as a PPTP client at the branch office. And the mobile users will use the Windows XP built-in PPTP client. The IP addresses are as follows:

The Device (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.123/255.255.255.0

The VPN appliance (PPTP Client) at the branch office:

- LAN Subnet: 192.168.16.0/255.255.255.0
- LAN Interface IP Address: 192.168.16.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.16/255.255.255.0

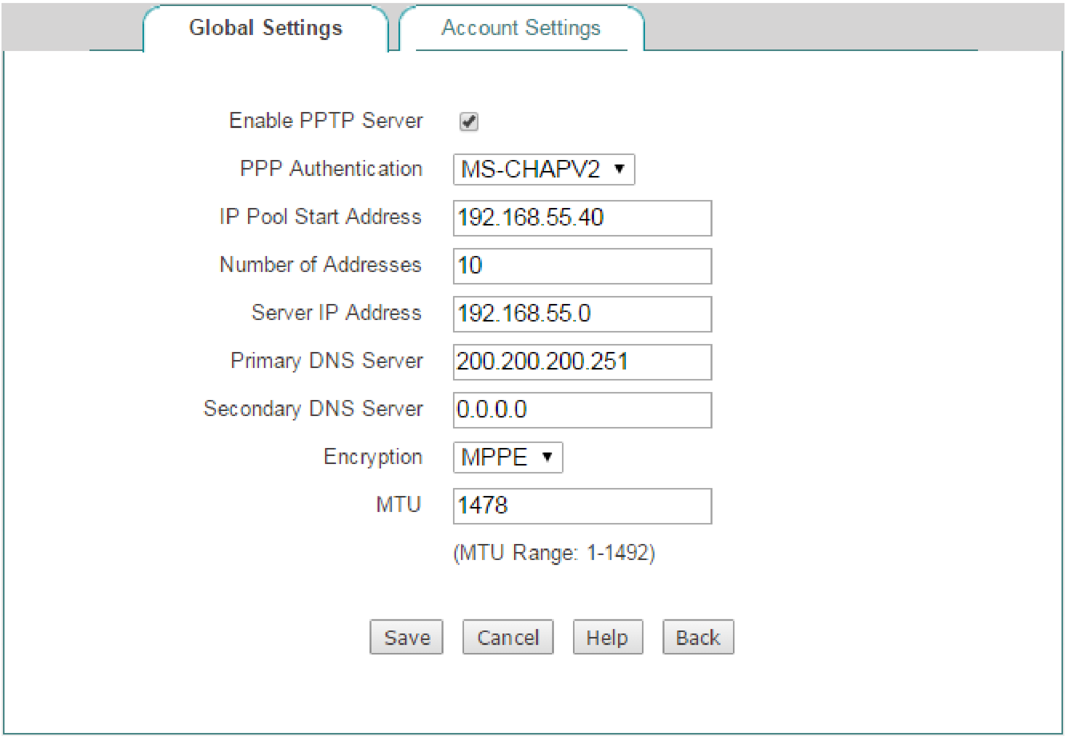
**The mobile users:**

A mobile user with any public IP address can use the Windows XP built-in PPTP client to connect to the Device.

4) Configuring Head office’s Device as a PPTP Server (LAN-to-LAN and Mobile User)

Go to **VPN > PPTP** page, click the **Add Server** button and then make settings as the following figure, lastly click the **Save** button.

}



Enable PPTP Server ☑

PPP Authentication MS-CHAPV2 ▾

IP Pool Start Address 192.168.55.40

Number of Addresses 10

Server IP Address 192.168.55.0

Primary DNS Server 200.200.200.251

Secondary DNS Server 0.0.0.0

Encryption MPPE ▾

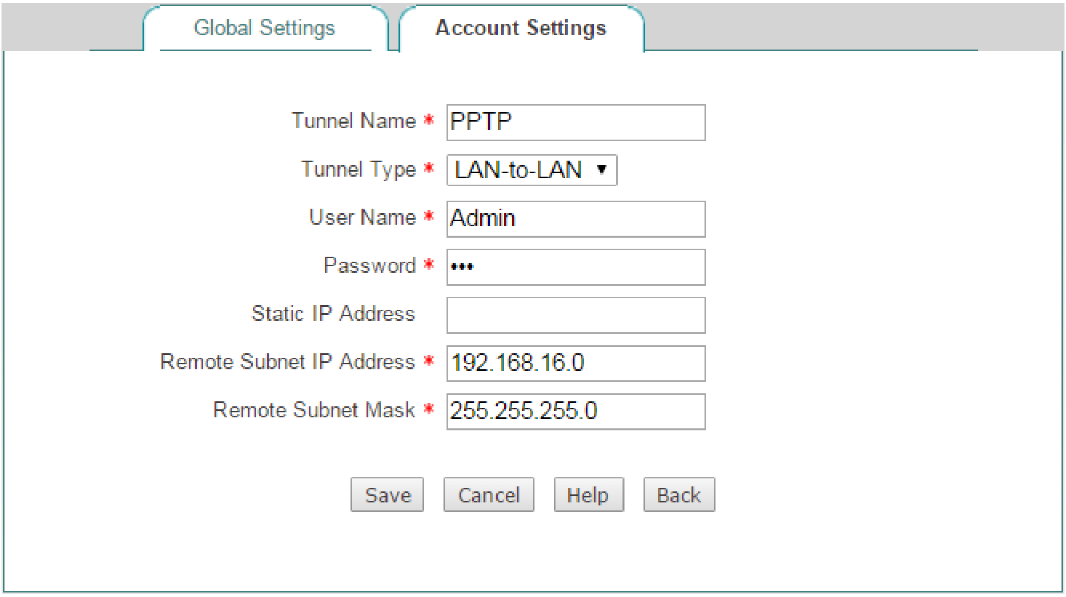
MTU 1478

(MTU Range: 1-1492)

**Figure 10-17 PPTP Server Settings**

(3) Creating a LAN-to-LAN PPTP Server Account for the Branch Office

Click the **Account Settings** tab and make settings as the following figure, lastly click the **Save** button.



Tunnel Name * PPTP

Tunnel Type * LAN-to-LAN ▾

User Name * Admin

Password * •••

Static IP Address

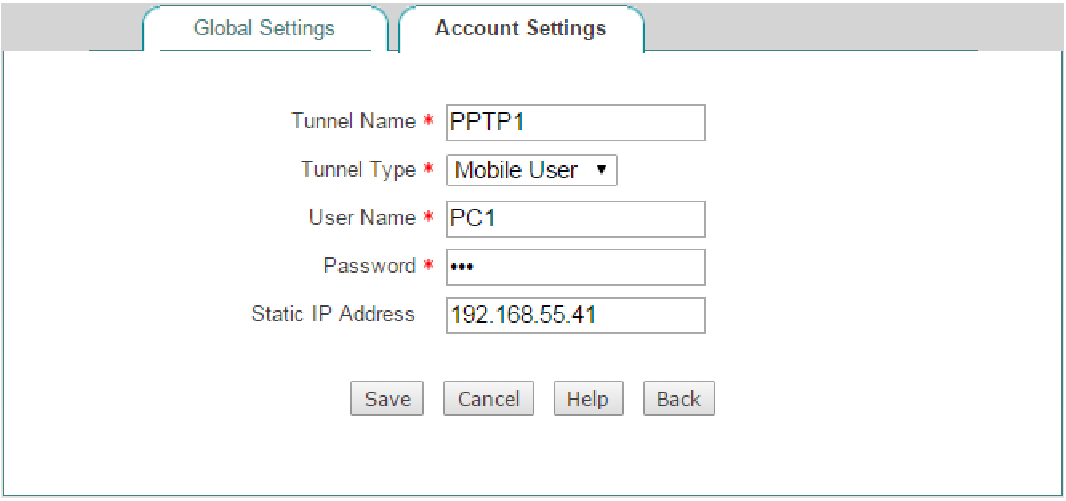
Remote Subnet IP Address * 192.168.16.0

Remote Subnet Mask * 255.255.255.0

**Figure 10-18 PPTP Server Settings_LAN-to-LAN**

(4) Creating a Mobile User Server Account for Mobile Users

}



Tunnel Name * PPTP1

Tunnel Type * Mobile User ▼

User Name * PC1

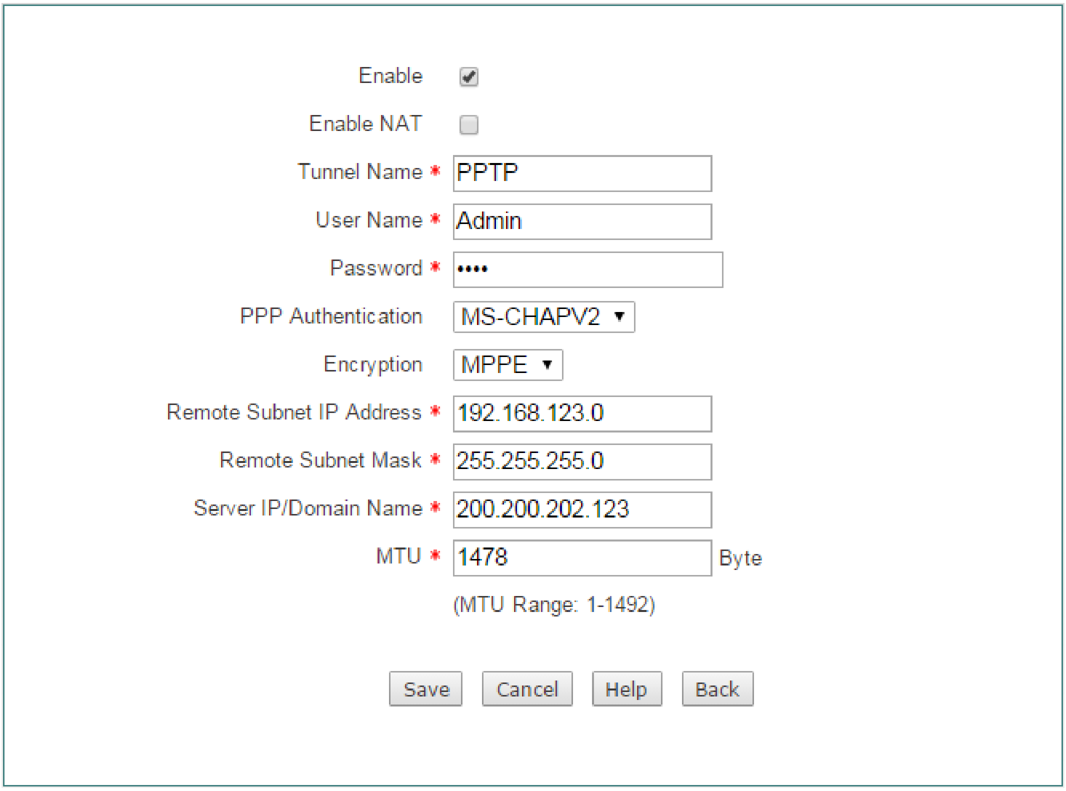
Password * •••

Static IP Address 192.168.55.41

**Figure 10-19 PPTP Server Settings_Mobile User**

5) Configuring Branch office's Device as a PPTP Client

Go to **VPN > PPTP** page, click the **Add Client** button and then make settings as the following figure, lastly click the **Save** button.



Enable ☑

Enable NAT ☐

Tunnel Name * PPTP

User Name * Admin

Password * ••••

PPP Authentication MS-CHAPV2 ▼

Encryption MPPE ▼

Remote Subnet IP Address * 192.168.123.0

Remote Subnet Mask * 255.255.255.0

Server IP/Domain Name * 200.200.202.123

MTU * 1478 Byte

(MTU Range: 1-1492)

**Figure 10-20 PPTP Client settings**

6) Configuring a Windows XP-based Computer as a PPTP Client (Mobile User)

Do the following steps on a Windows XP-based computer to configure it as a PPTP client.

}

(3) Creating the PPTP Dial-up Connection

q) Go to **Start > Settings > Control Panel**, and select the **Switch to Category View**.

r) Select the **Network and Internet Connections.**

s) Select the **Create** a **connection to the network at my workplace**.

t) Select the **Virtual Private Network connection** option, and then click the **Next** button.

u) Enter a name for the connection (**PPTP** in this example) in the **Company Name** text box, and then click the **Next** button.

v) Select the **Do not dial the initial connection** option, and then click the **Next** button.

w) Enter the remote PPTP server's IP address (**200.200.202.123** in this example) in the **Host name or IP address** text box, and then click the **Next** button.

x) Click the **Finish** button.

y) Double click the new connection **PPTP**, and click the **Properties** button.

z) Select the **Security** tab, select the **Advanced (custom settings)** option and click the **Settings** button.

aa) Select **Optional Encryption (connect even if no encryption)** from the **Data encryption drop-down list.**

bb) Select the **Unencrypted password (PAP)**, **Challenge Handshake Authentication Protocol (CHAP)**, and **Microsoft CHAP (MS-CHAP)** check boxes in the **Allow these protocols**, and then click the **OK** button.

cc) Select the **Networking** tab, select **PPTP VPN** from the **Type of VPN** drop-down list.

dd) Make sure that the **Internet Protocol (TCP/IP)** check box is checked.

ee) Make sure that the **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, **File and Printer Sharing for Microsoft Networks**, and **Client for Microsoft Networks** check boxes are cleared.

ff) Click the **OK** button to save the changes to make them take effect.

(4) Connect the Computer to the Device through the PPTP Tunnel

f) Please make sure that your computer has been connected to the Internet.

g) Double-click the new connection **PPTP** you have just created.

h) Enter **PC1** in the **User name** text box and **PC1** in the **Password** text box.

i) Click the **Connect** button.

j) After the PPTP tunnel has been established successfully, if you run the **ipconfig** command at the MS-DOS command prompt on the computer, you can see the IP address assigned by the Device.

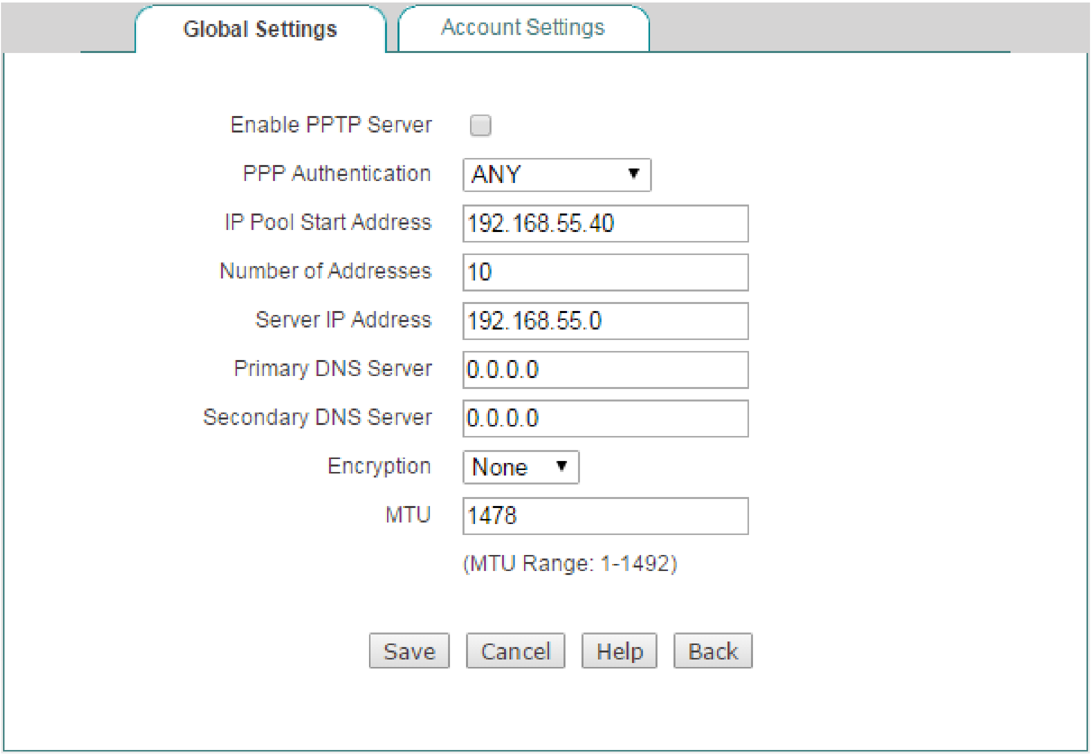
Xxxxxxxxxxxxxx

**}**

### 10.2.1.14 PPTP Server settings

On the **VPN** > **PPTP** page, click the **Add Server** button to setup PPTP Server.

### 10.2.1.15 Global Settings



| | |
|---|---|
| Enable PPTP Server | □ |
| PPP Authentication | ANY ▾ |
| IP Pool Start Address | 192.168.55.40 |
| Number of Addresses | 10 |
| Server IP Address | 192.168.55.0 |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Encryption | None ▾ |
| MTU | 1478 |
| | (MTU Range: 1-1492) |

**Figure 10-21 PPTP Server_Global Settings**

- **Enable PPTP Server:** Select to enable PPTP Server.
- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.
  - **PAP:** Password Authentication Protocol.
  - **CHAP:** Challenge Handshake Authentication Protocol.
  - **MS-CHAPV2:** The Microsoft version of the Challenge-Handshake Authentication Protocol.
  - **ANY:** The Device will automatically negotiate it with the remote VPN appliance.
- **IP Pool Start Address:** Specify the starting IP address assigned from the VPN address pool.

}

- **Number of Address:** Specify the maximum number of IP addresses that can be assigned from the VPN address pool.

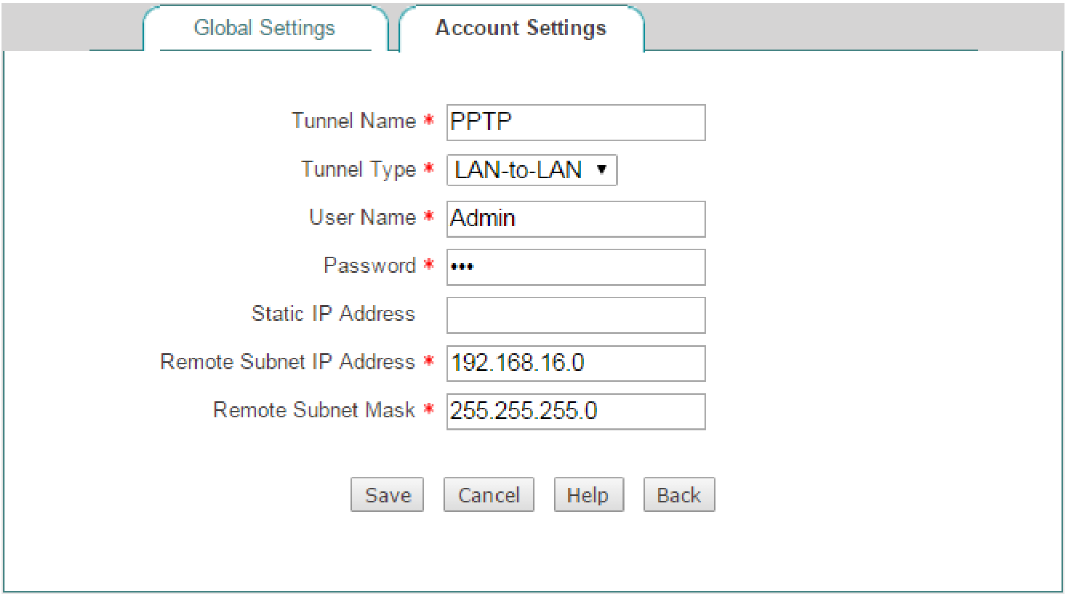
- **Server IP Server:** Specify the IP addresses of the VPN Server. This address should be on the same network segment with the VPN address pool but not including.

- **Primary / Secondary DNS Server:** When the device is setup to as the PPTP server, it can assign DNS address to the client to access internet.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

## 10.2.1.16 Account Settings



Tunnel Name * PPTP

Tunnel Type * LAN-to-LAN ▾

User Name * Admin

Password * •••

Static IP Address

Remote Subnet IP Address * 192.168.16.0

Remote Subnet Mask * 255.255.255.0

**Figure 10-22 PPTP Server_Account Settings**

- **Tunnel Name:** Specify the name of this tunnel.

- **Tunnel Type:** Specify the type of the PPTP tunnel.

  - **LAN-to-LAN:** If selected, two LAN sites can securely connect with each other over public networks like the Internet. All traffic from one LAN destined for the other one is tunneled, without individual hosts having to use VPN clients. In this case, either a Device or compatible VPN appliance can act as a PPTP client.

}

  - **Mobile User**: If selected, the remote individual users can securely connect the server over public networks like the Internet. In this case, a laptop or desktop computer will act as a PPTP client.

- **User Name:** Specify a unique user name of the PPTP client. It should be between 1 and 31 characters long. The PPTP server will use the **User Name** and **Password** to identify the remote PPTP client.

- **Password:** Specify the password of the PPTP client.

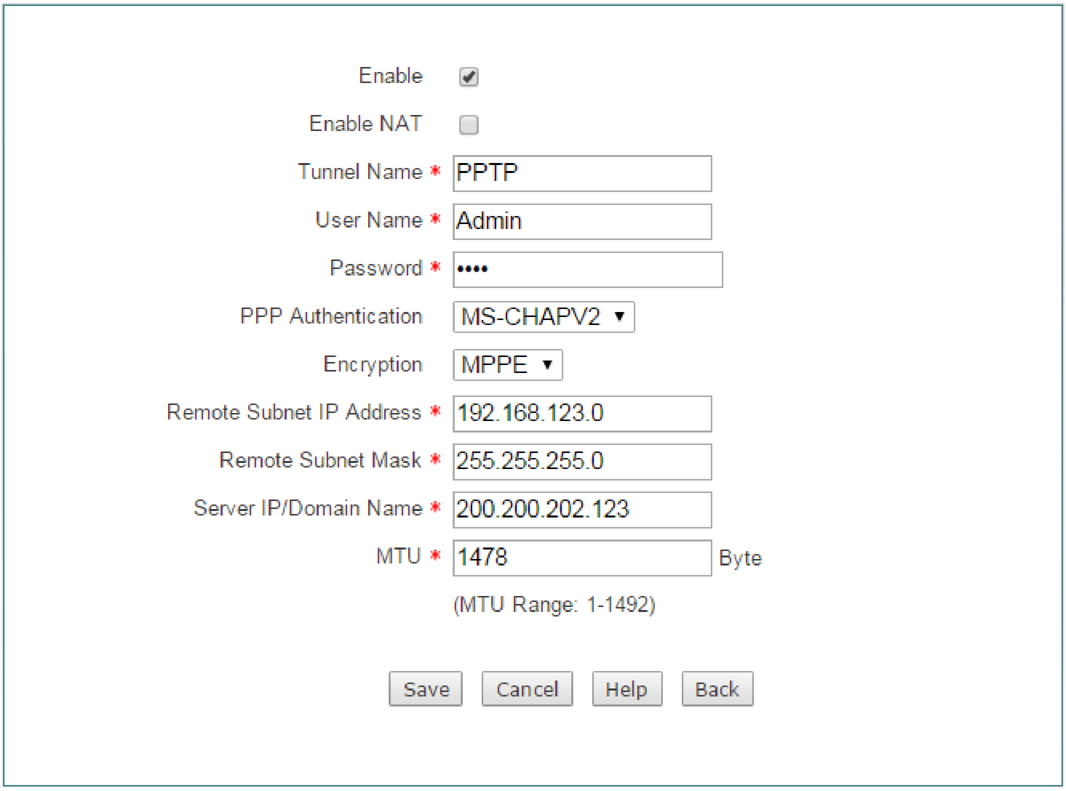
- **Static IP Address:** Specify the IP address the PPTP server assigns to PPTP client. Note this IP Address you set should be inside the VPN address pool.

- **Remote Subnet IP Address:** Specify the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface. If you choose **Mobile User** as the **Tunnel Type**, the system will automatically generate the **Remote Subnet IP Address** and **Remote Subnet Mask**.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

### 10.2.1.17 Client Settings

On the **VPN** > **PPTP** page, click the **Add Client** button to setup PPTP client.



| | |
|---|---|
| Enable | ☑ |
| Enable NAT | □ |
| Tunnel Name * | PPTP |
| User Name * | Admin |
| Password * | •••• |
| PPP Authentication | MS-CHAPV2 ▾ |
| Encryption | MPPE ▾ |
| Remote Subnet IP Address * | 192.168.123.0 |
| Remote Subnet Mask * | 255.255.255.0 |
| Server IP/Domain Name * | 200.200.202.123 |
| MTU * | 1478 Byte<br>(MTU Range: 1-1492) |

**Figure 10-23 PPTP Client Settings**

- **Enable:** Select to enable PPTP client.

}

- **Enable NAT:** If selected, it will only allow unidirectional access from the PPTP client side LAN to the server side LAN.

- **Tunnel Name:** Specify a unique name for the PPTP tunnel.

- **User Name:** Specify the user name of the PPTP client.

- **Password:** Specify the password of the PPTP client.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** the Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** If selected, the Device will automatically negotiate it with the remote VPN appliance.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **Remote Subnet IP Address:** Specify the IP address of the remote network.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

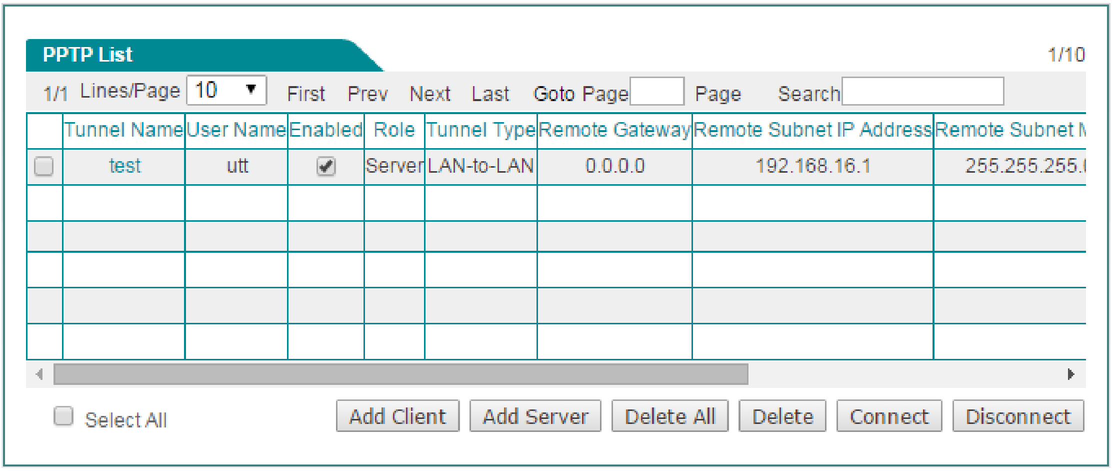
- **Server IP/Domain Name:** The public IP address or domain name of the remote PPTP server.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.18 PPTP List

After you have configured a PPTP client or server entry, you can view its configuration and status information in the **PPTP List**.

}



PPTP List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | Tunnel Name | User Name | Enabled | Role | Tunnel Type | Remote Gateway | Remote Subnet IP Address | Remote Subnet M |
|---|---|---|---|---|---|---|---|---|
| ☐ | test | utt | ☑ | Server | LAN-to-LAN | 0.0.0.0 | 192.168.16.1 | 255.255.255.( |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

☐ Select All

Figure 10-24 PPTP List

## 10.2.1.19 Example of PPTP

In this scenario, a company's head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet. In addition, some mobile users (traveling employees, telecommuters, etc.) want to securely access the head office's internal network over the Internet.

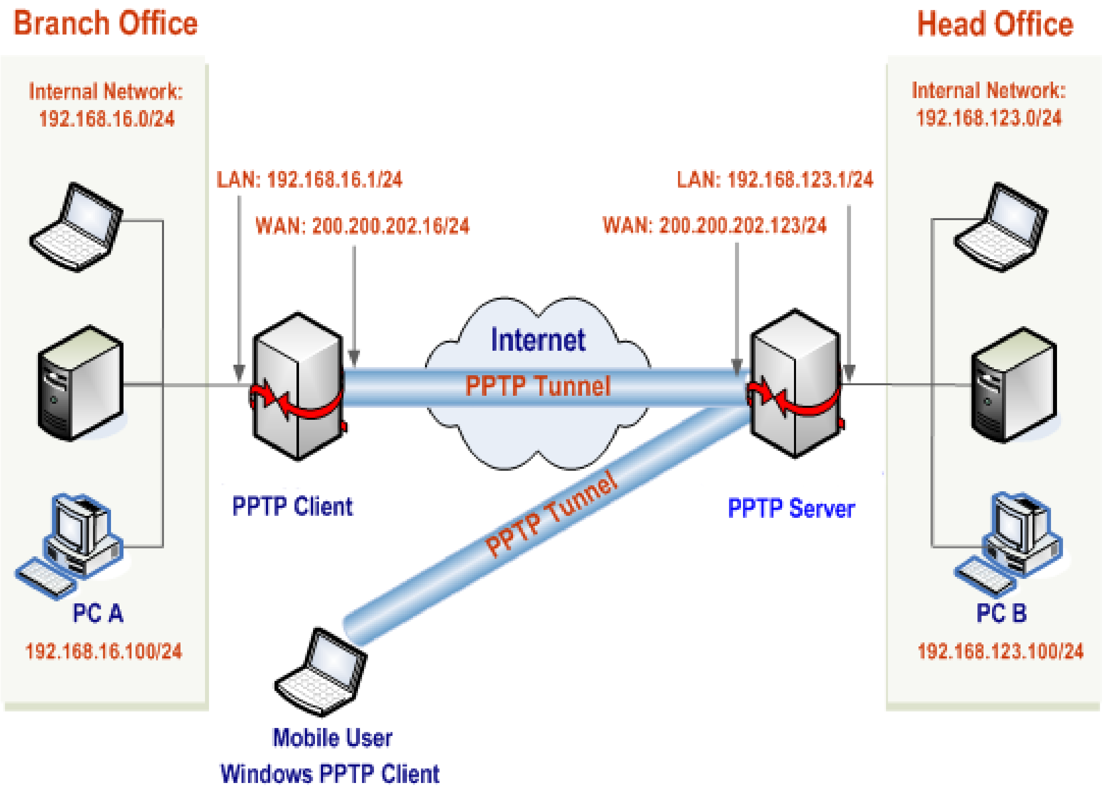


Figure 10-25 Network Topology – the Device Acts as a PPTP Server

We will use PPTP to establish VPN tunnels, deploy a enterprise wireless router

}

acting as a PPTP server at the head office, and another VPN appliance acting as a PPTP client at the branch office. And the mobile users will use the Windows XP built-in PPTP client. The IP addresses are as follows:

The Device (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.123/255.255.255.0

The VPN appliance (PPTP Client) at the branch office:

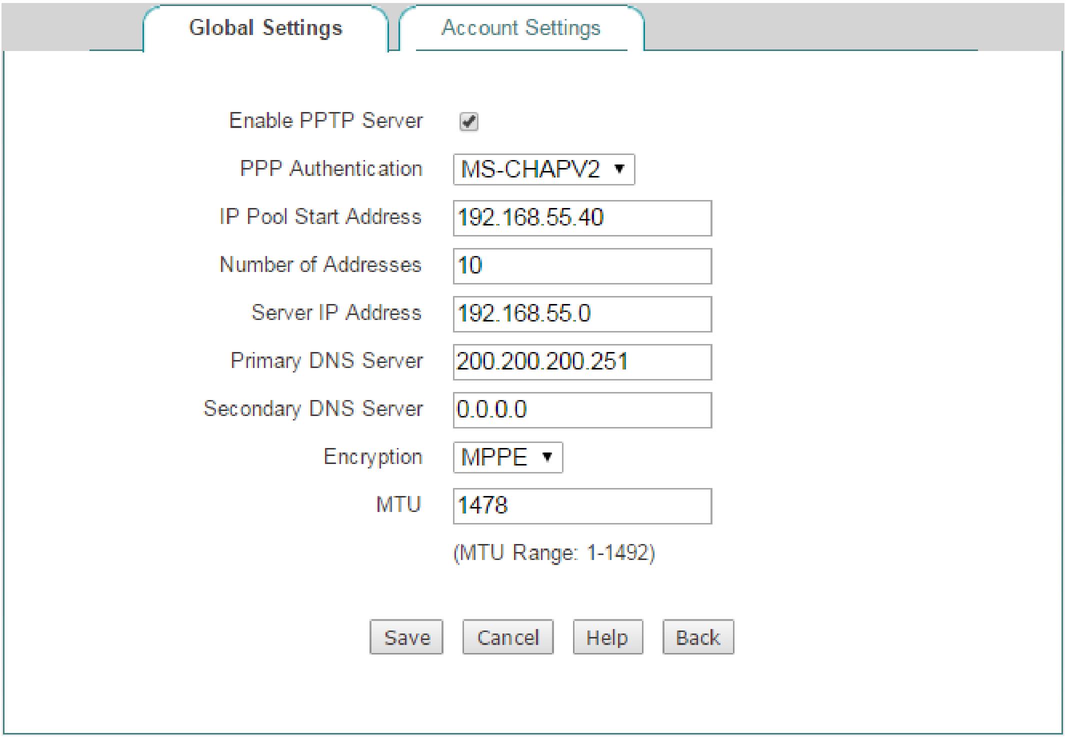
- LAN Subnet: 192.168.16.0/255.255.255.0
- LAN Interface IP Address: 192.168.16.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.16/255.255.255.0

**The mobile users:**

A mobile user with any public IP address can use the Windows XP built-in PPTP client to connect to the Device.

7) Configuring Head office's Device as a PPTP Server (LAN-to-LAN and Mobile User)

Go to **VPN > PPTP** page, click the **Add Server** button and then make settings as the following figure, lastly click the **Save** button.

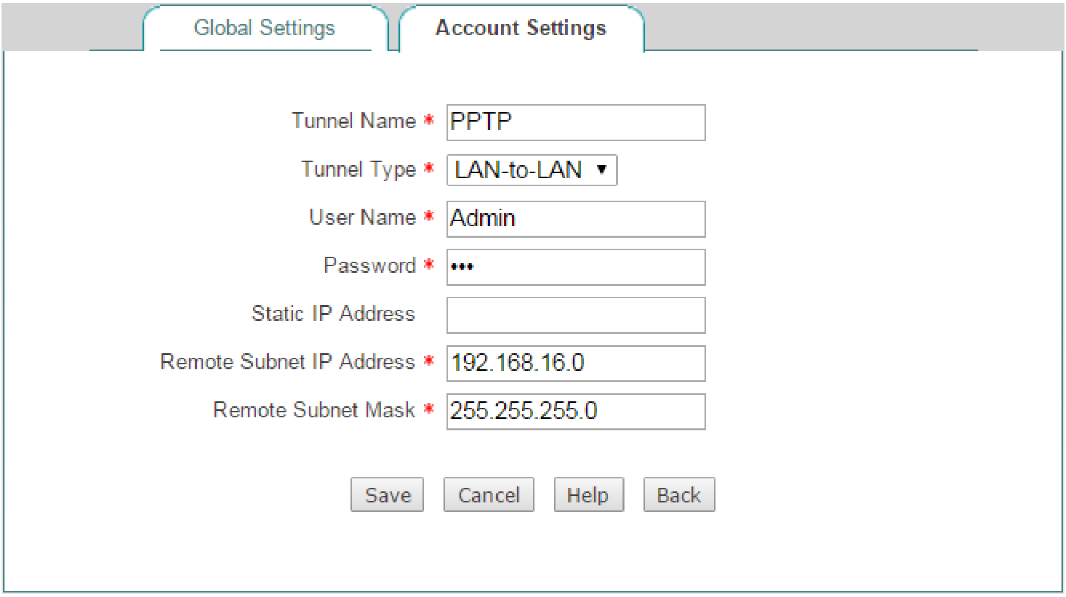


| | |
|---|---|
| Enable PPTP Server | ☑ |
| PPP Authentication | MS-CHAPV2 ▾ |
| IP Pool Start Address | 192.168.55.40 |
| Number of Addresses | 10 |
| Server IP Address | 192.168.55.0 |
| Primary DNS Server | 200.200.200.251 |
| Secondary DNS Server | 0.0.0.0 |
| Encryption | MPPE ▾ |
| MTU | 1478 |
| | (MTU Range: 1-1492) |

**Figure 10-26 PPTP Server Settings**

(5) Creating a LAN-to-LAN PPTP Server Account for the Branch Office

Click the **Account Settings** tab and make settings as the following figure, lastly click the **Save** button.

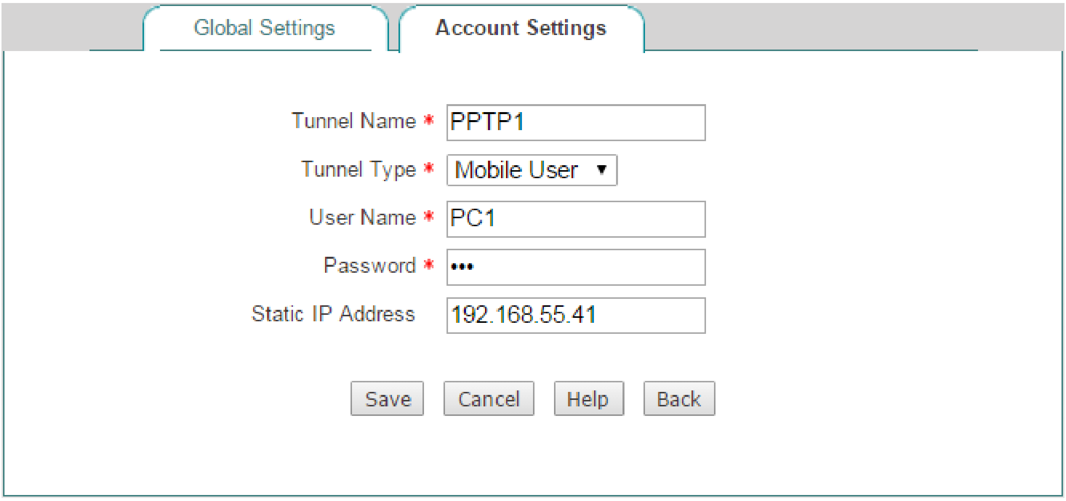


| | |
|---|---|
| Tunnel Name * | PPTP |
| Tunnel Type * | LAN-to-LAN ▾ |
| User Name * | Admin |
| Password * | ••• |
| Static IP Address | |
| Remote Subnet IP Address * | 192.168.16.0 |
| Remote Subnet Mask * | 255.255.255.0 |

**Figure 10-27 PPTP Server Settings_LAN-to-LAN**

(6) Creating a Mobile User Server Account for Mobile Users

}



Tunnel Name * PPTP1

Tunnel Type * Mobile User ▾

User Name * PC1

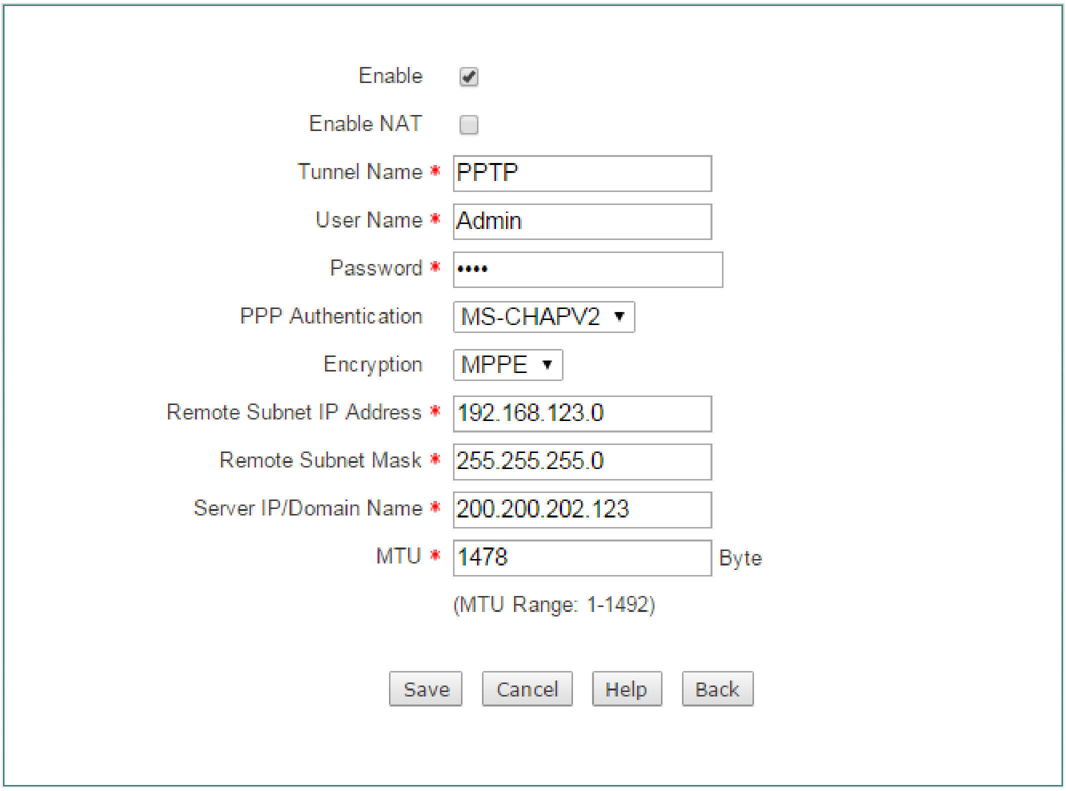
Password * •••

Static IP Address 192.168.55.41

**Figure 10-28 PPTP Server Settings_Mobile User**

8) Configuring Branch office’s Device as a PPTP Client

Go to **VPN > PPTP** page, click the **Add Client** button and then make settings as the following figure, lastly click the **Save** button.



Enable ☑

Enable NAT ☐

Tunnel Name * PPTP

User Name * Admin

Password * ••••

PPP Authentication MS-CHAPV2 ▾

Encryption MPPE ▾

Remote Subnet IP Address * 192.168.123.0

Remote Subnet Mask * 255.255.255.0

Server IP/Domain Name * 200.200.202.123

MTU * 1478 Byte

(MTU Range: 1-1492)

**Figure 10-29 PPTP Client settings**

9) Configuring a Windows XP-based Computer as a PPTP Client (Mobile User)

Do the following steps on a Windows XP-based computer to configure it as a PPTP client.

}

(5) Creating the PPTP Dial-up Connection

gg) Go to **Start > Settings > Control Panel**, and select the **Switch to Category View**.

hh) Select the **Network and Internet Connections.**

ii) Select the **Create** a **connection to the network at my workplace**.

jj) Select the **Virtual Private Network connection** option, and then click the **Next** button.

kk) Enter a name for the connection (**PPTP** in this example) in the **Company Name** text box, and then click the **Next** button.

ll) Select the **Do not dial the initial connection** option, and then click the **Next** button.

mm) Enter the remote PPTP server's IP address (**200.200.202.123** in this example) in the **Host name or IP address** text box, and then click the **Next** button.

nn) Click the **Finish** button.

oo) Double click the new connection **PPTP**, and click the **Properties** button.

pp) Select the **Security** tab, select the **Advanced (custom settings)** option and click the **Settings** button.

qq) Select **Optional Encryption (connect even if no encryption)** from the **Data encryption drop-down list.**

rr) Select the **Unencrypted password (PAP)**, **Challenge Handshake Authentication Protocol (CHAP)**, and **Microsoft CHAP (MS-CHAP)** check boxes in the **Allow these protocols**, and then click the **OK** button.

ss) Select the **Networking** tab, select **PPTP VPN** from the **Type of VPN** drop-down list.

tt) Make sure that the **Internet Protocol (TCP/IP)** check box is checked.

uu) Make sure that the **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, **File and Printer Sharing for Microsoft Networks**, and **Client for Microsoft Networks** check boxes are cleared.

vv) Click the **OK** button to save the changes to make them take effect.

(6) Connect the Computer to the Device through the PPTP Tunnel

k) Please make sure that your computer has been connected to the Internet.

l) Double-click the new connection **PPTP** you have just created.

m) Enter **PC1** in the **User name** text box and **PC1** in the **Password** text box.

n) Click the **Connect** button.

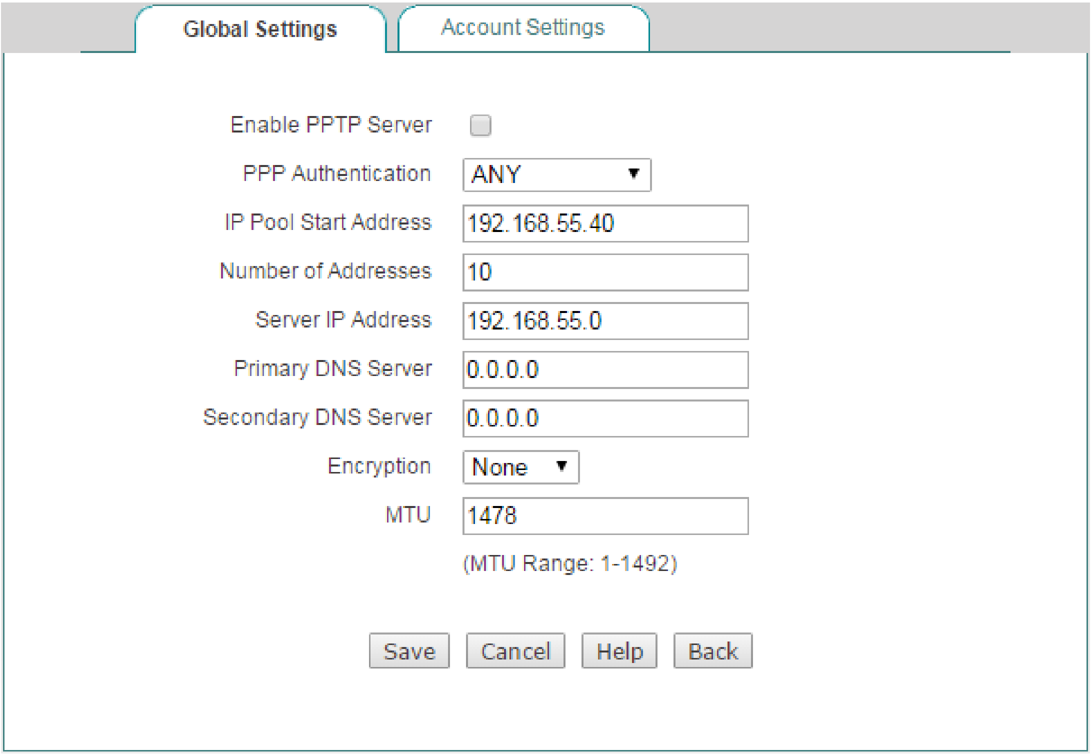
o) After the PPTP tunnel has been established successfully, if you run the **ipconfig** command at the MS-DOS command prompt on the computer, you can see the IP address assigned by the Device.

**}**

### 10.2.1.20 PPTP Server settings

On the **VPN** > **PPTP** page, click the **Add Server** button to setup PPTP Server.

### 10.2.1.21 Global Settings



| | |
|---|---|
| Enable PPTP Server | □ |
| PPP Authentication | ANY |
| IP Pool Start Address | 192.168.55.40 |
| Number of Addresses | 10 |
| Server IP Address | 192.168.55.0 |
| Primary DNS Server | 0.0.0.0 |
| Secondary DNS Server | 0.0.0.0 |
| Encryption | None |
| MTU | 1478 |
| | (MTU Range: 1-1492) |

**Figure 10-30 PPTP Server_Global Settings**

- **Enable PPTP Server:** Select to enable PPTP Server.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** The Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** The Device will automatically negotiate it with the remote VPN appliance.

- **IP Pool Start Address:** Specify the starting IP address assigned from the VPN address pool.

}

- **Number of Address:** Specify the maximum number of IP addresses that can be assigned from the VPN address pool.

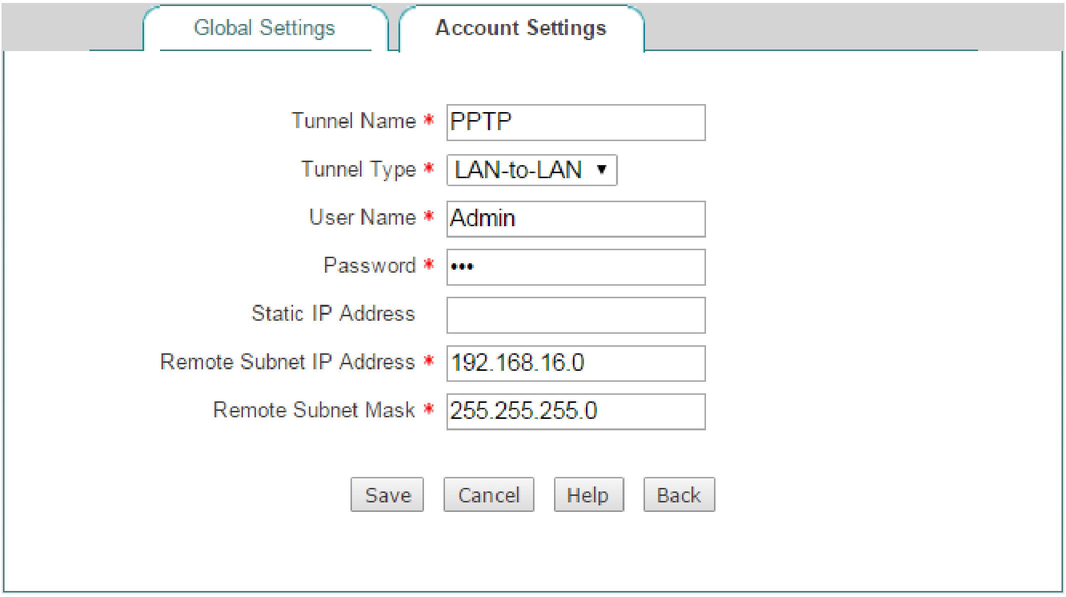
- **Server IP Server:** Specify the IP addresses of the VPN Server. This address should be on the same network segment with the VPN address pool but not including.

- **Primary / Secondary DNS Server:** When the device is setup to as the PPTP server, it can assign DNS address to the client to access internet.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.22 Account Settings



| | |
|---|---|
| Tunnel Name * | PPTP |
| Tunnel Type * | LAN-to-LAN ▾ |
| User Name * | Admin |
| Password * | ••• |
| Static IP Address | |
| Remote Subnet IP Address * | 192.168.16.0 |
| Remote Subnet Mask * | 255.255.255.0 |

**Figure 10-31 PPTP Server_Account Settings**

- **Tunnel Name:** Specify the name of this tunnel.

- **Tunnel Type:** Specify the type of the PPTP tunnel.

  - **LAN-to-LAN:** If selected, two LAN sites can securely connect with each other over public networks like the Internet. All traffic from one LAN destined for the other one is tunneled, without individual hosts having to use VPN clients. In this case, either a Device or compatible VPN appliance can act as a PPTP client.

}

  - **Mobile User**: If selected, the remote individual users can securely connect the server over public networks like the Internet. In this case, a laptop or desktop computer will act as a PPTP client.

- **User Name:** Specify a unique user name of the PPTP client. It should be between 1 and 31 characters long. The PPTP server will use the **User Name** and **Password** to identify the remote PPTP client.

- **Password:** Specify the password of the PPTP client.

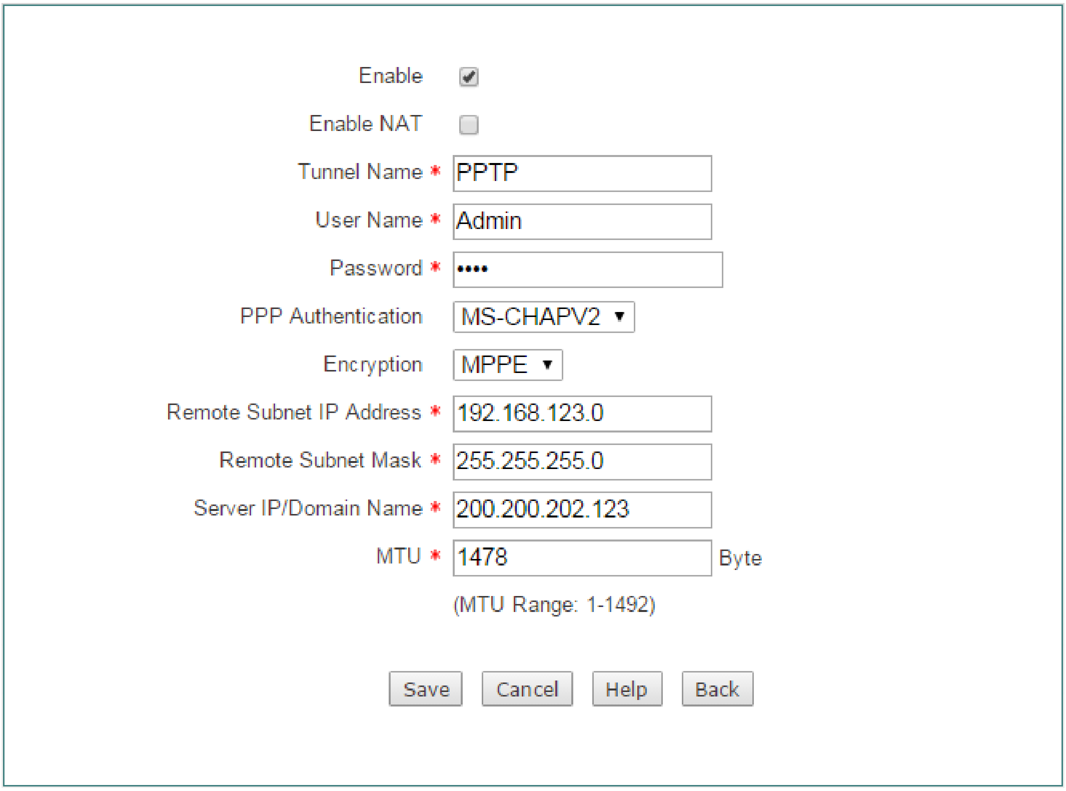
- **Static IP Address:** Specify the IP address the PPTP server assigns to PPTP client. Note this IP Address you set should be inside the VPN address pool.

- **Remote Subnet IP Address:** Specify the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface. If you choose **Mobile User** as the **Tunnel Type**, the system will automatically generate the **Remote Subnet IP Address** and **Remote Subnet Mask**.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

## 10.2.1.23 Client Settings

On the **VPN** > **PPTP** page, click the **Add Client** button to setup PPTP client.



| | |
|---|---|
| Enable | ☑ |
| Enable NAT | □ |
| Tunnel Name * | PPTP |
| User Name * | Admin |
| Password * | •••• |
| PPP Authentication | MS-CHAPV2 ▾ |
| Encryption | MPPE ▾ |
| Remote Subnet IP Address * | 192.168.123.0 |
| Remote Subnet Mask * | 255.255.255.0 |
| Server IP/Domain Name * | 200.200.202.123 |
| MTU * | 1478 Byte |
| | (MTU Range: 1-1492) |

**Figure 10-32 PPTP Client Settings**

- **Enable:** Select to enable PPTP client.

}

- **Enable NAT:** If selected, it will only allow unidirectional access from the PPTP client side LAN to the server side LAN.

- **Tunnel Name:** Specify a unique name for the PPTP tunnel.

- **User Name:** Specify the user name of the PPTP client.

- **Password:** Specify the password of the PPTP client.

- **PPP Authentication:** Specify the PPP authentication mode of the PPTP tunnel. The available options are **PAP**, **CHAP** , **MS-CHAPV2 and ANY**.

  - **PAP:** Password Authentication Protocol.

  - **CHAP:** Challenge Handshake Authentication Protocol.

  - **MS-CHAPV2:** the Microsoft version of the Challenge-Handshake Authentication Protocol.

  - **ANY:** If selected, the Device will automatically negotiate it with the remote VPN appliance.

- **Encryption:** Select the way of data encryption mode. Note when you choose MS-CHAPV2 as PPP aunthentication mode, you must select MPPE as data encryption mode.

- **Remote Subnet IP Address:** Specify the IP address of the remote network.

- **Remote Subnet Mask:** Specify the subnet mask of the remote network.

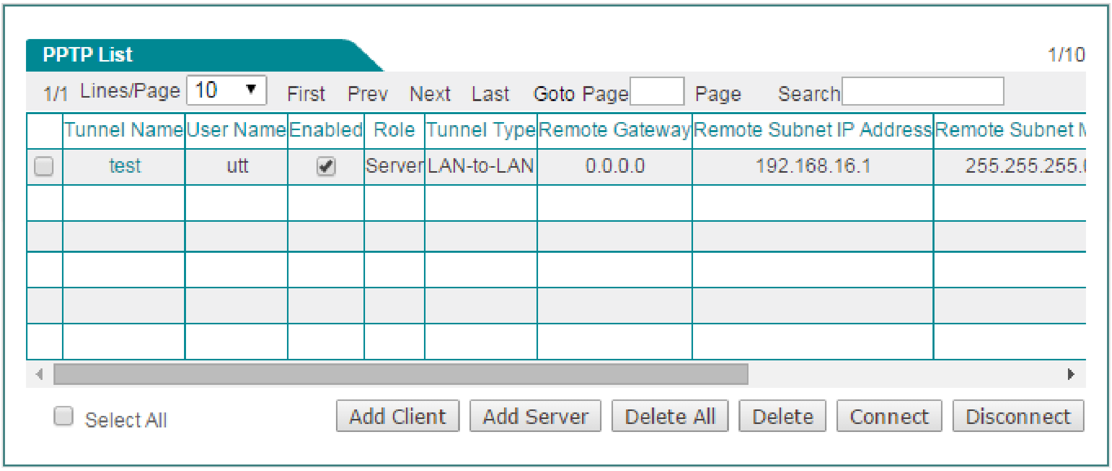
- **Server IP/Domain Name:** The public IP address or domain name of the remote PPTP server.

- **MTU:** Specify the largest packet size permitted for network receive. During dialing, The Device will automatically negotiate it with the remote VPN appliance when dialing. Unless special application, please leave the default value of 1478 bytes.

### 10.2.1.24 PPTP List

After you have configured a PPTP client or server entry, you can view its configuration and status information in the **PPTP List**.

}



PPTP List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | Tunnel Name | User Name | Enabled | Role | Tunnel Type | Remote Gateway | Remote Subnet IP Address | Remote Subnet M |
|---|---|---|---|---|---|---|---|---|
| ☐ | test | utt | ☑ | Server | LAN-to-LAN | 0.0.0.0 | 192.168.16.1 | 255.255.255.( |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

☐ Select All

Figure 10-33 PPTP List

## 10.2.1.25 Example of PPTP

In this scenario, a company’s head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet. In addition, some mobile users (traveling employees, telecommuters, etc.) want to securely access the head office’s internal network over the Internet.

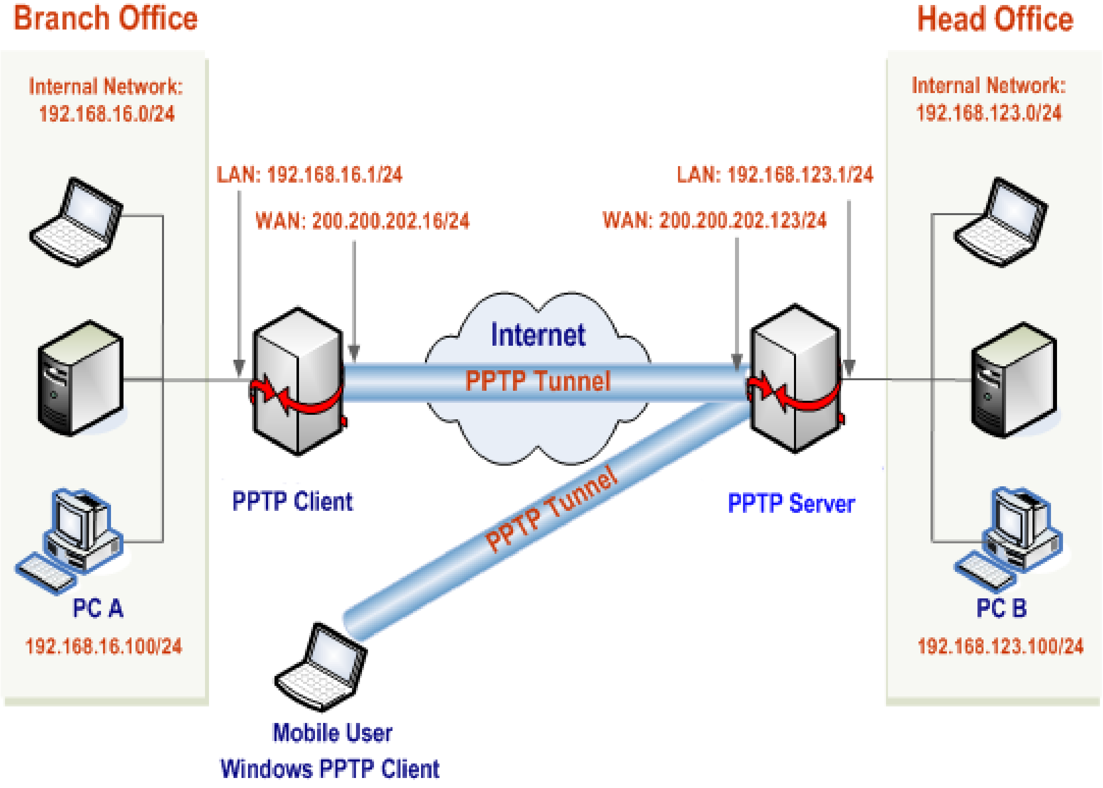


Figure 10-34 Network Topology – the Device Acts as a PPTP Server

We will use PPTP to establish VPN tunnels, deploy a enterprise wireless router

}

acting as a PPTP server at the head office, and another VPN appliance acting as a PPTP client at the branch office. And the mobile users will use the Windows XP built-in PPTP client. The IP addresses are as follows:

The Device (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.123/255.255.255.0

The VPN appliance (PPTP Client) at the branch office:

- LAN Subnet: 192.168.16.0/255.255.255.0
- LAN Interface IP Address: 192.168.16.1/255.255.255.0
- WAN Interface IP Address: 200.200.202.16/255.255.255.0

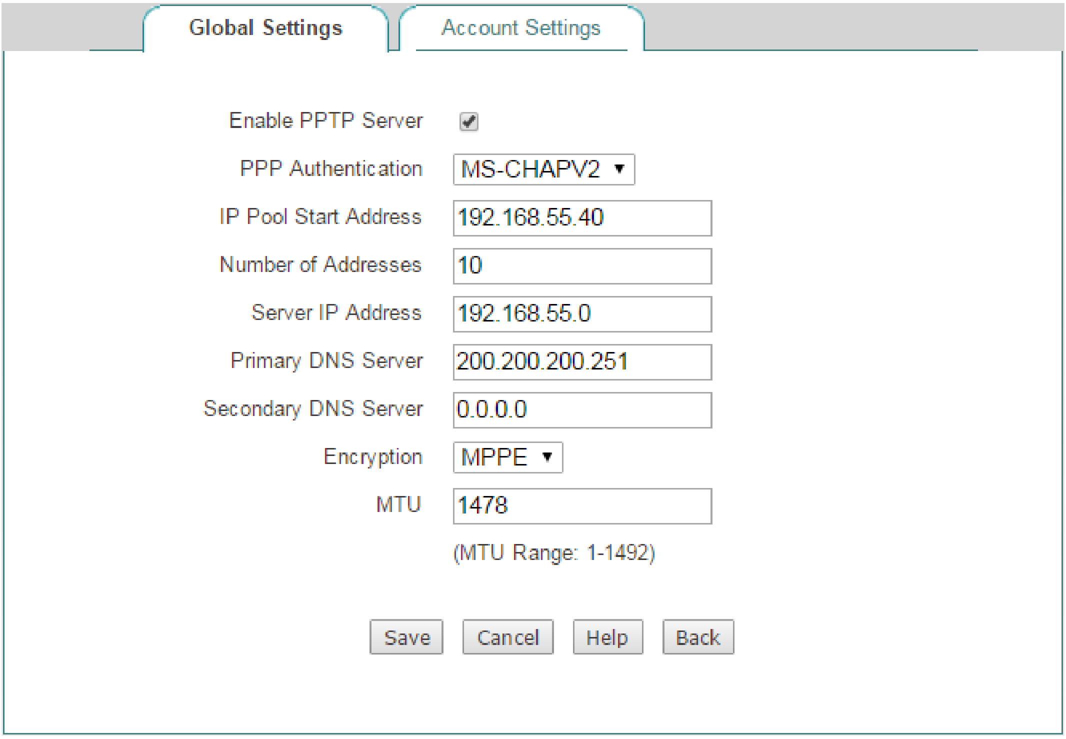
**The mobile users:**

A mobile user with any public IP address can use the Windows XP built-in PPTP client to connect to the Device.

10) Configuring Head office’s Device as a PPTP Server (LAN-to-LAN and Mobile User)

Go to **VPN > PPTP** page, click the **Add Server** button and then make settings as the following figure, lastly click the **Save** button.

}



Enable PPTP Server ☑

PPP Authentication: MS-CHAPV2 ▼

IP Pool Start Address: 192.168.55.40

Number of Addresses: 10

Server IP Address: 192.168.55.0

Primary DNS Server: 200.200.200.251

Secondary DNS Server: 0.0.0.0

Encryption: MPPE ▼

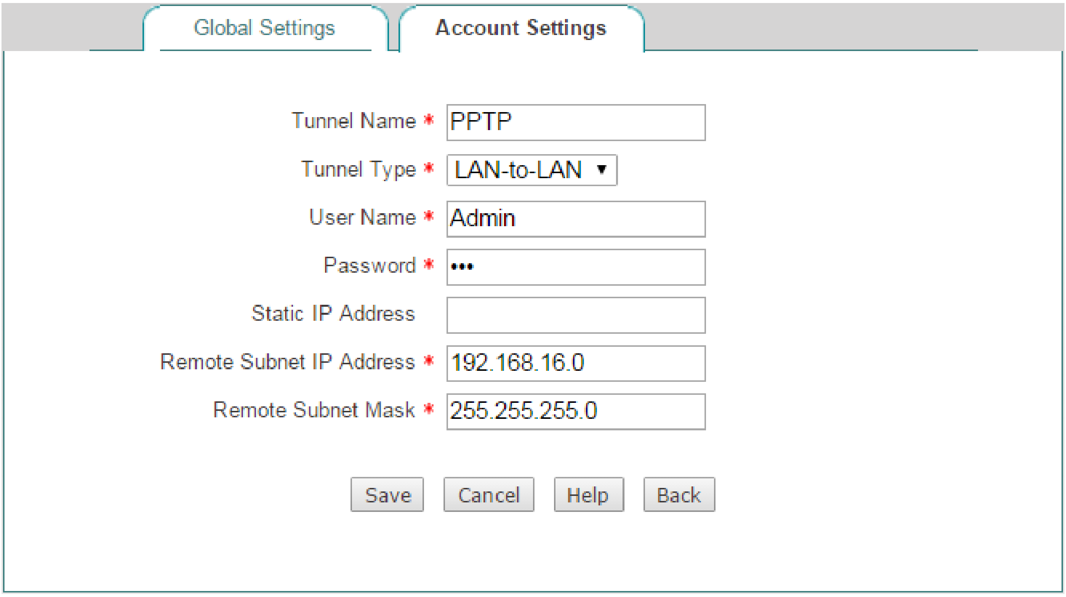
MTU: 1478

(MTU Range: 1-1492)

**Figure 10-35 PPTP Server Settings**

(7) Creating a LAN-to-LAN PPTP Server Account for the Branch Office

Click the **Account Settings** tab and make settings as the following figure, lastly click the **Save** button.



Tunnel Name *: PPTP

Tunnel Type *: LAN-to-LAN ▼

User Name *: Admin

Password *: •••

Static IP Address:

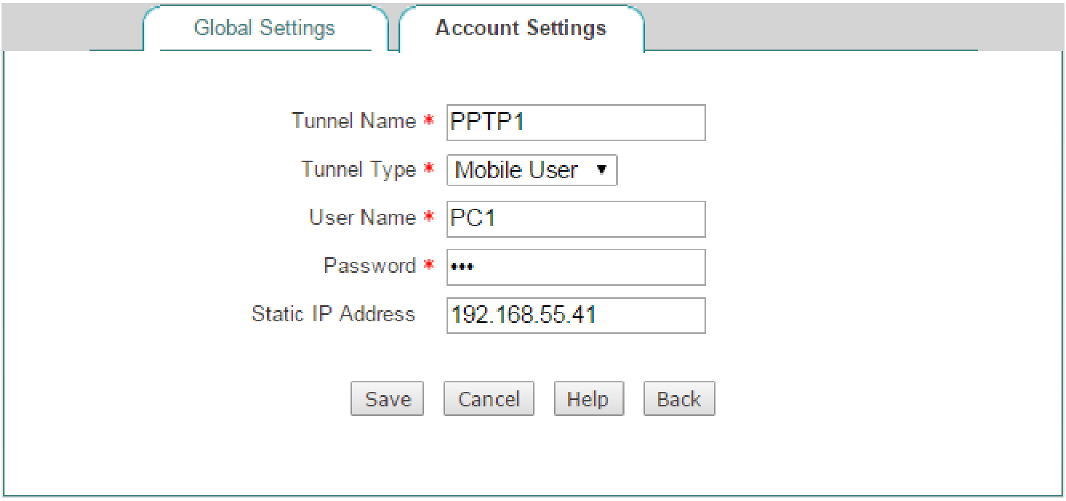
Remote Subnet IP Address *: 192.168.16.0

Remote Subnet Mask *: 255.255.255.0

**Figure 10-36 PPTP Server Settings_LAN-to-LAN**

(8) Creating a Mobile User Server Account for Mobile Users

}



Tunnel Name * PPTP1

Tunnel Type * Mobile User ▼

User Name * PC1

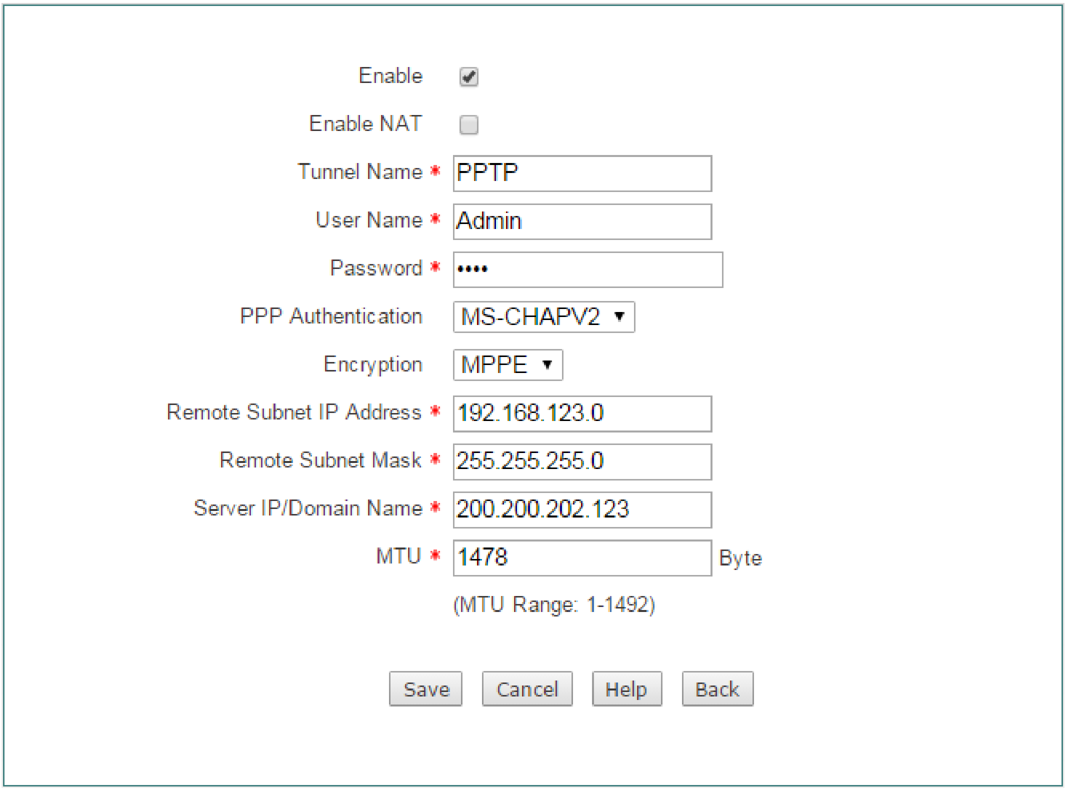
Password * •••

Static IP Address 192.168.55.41

**Figure 10-37 PPTP Server Settings_Mobile User**

11) Configuring Branch office’s Device as a PPTP Client

Go to **VPN > PPTP** page, click the **Add Client** button and then make settings as the following figure, lastly click the **Save** button.



Enable ☑

Enable NAT □

Tunnel Name * PPTP

User Name * Admin

Password * ••••

PPP Authentication MS-CHAPV2 ▼

Encryption MPPE ▼

Remote Subnet IP Address * 192.168.123.0

Remote Subnet Mask * 255.255.255.0

Server IP/Domain Name * 200.200.202.123

MTU * 1478 Byte

(MTU Range: 1-1492)

**Figure 10-38 PPTP Client settings**

12) Configuring a Windows XP-based Computer as a PPTP Client (Mobile User)

Do the following steps on a Windows XP-based computer to configure it as a PPTP client.

}

(7) Creating the PPTP Dial-up Connection

ww) Go to **Start > Settings > Control Panel**, and select the **Switch to Category View**.

xx) Select the **Network and Internet Connections.**

yy) Select the **Create** a **connection to the network at my workplace**.

zz) Select the **Virtual Private Network connection** option, and then click the **Next** button.

aaa) Enter a name for the connection (**PPTP** in this example) in the **Company Name** text box, and then click the **Next** button.

bbb) Select the **Do not dial the initial connection** option, and then click the **Next** button.

ccc) Enter the remote PPTP server's IP address (**200.200.202.123** in this example) in the **Host name or IP address** text box, and then click the **Next** button.

ddd) Click the **Finish** button.

eee) Double click the new connection **PPTP**, and click the **Properties** button.

fff) Select the **Security** tab, select the **Advanced (custom settings)** option and click the **Settings** button.

ggg) Select **Optional Encryption (connect even if no encryption)** from the **Data encryption drop-down list.**

hhh) Select the **Unencrypted password (PAP)**, **Challenge Handshake Authentication Protocol (CHAP)**, and **Microsoft CHAP (MS-CHAP)** check boxes in the **Allow these protocols**, and then click the **OK** button.

iii) Select the **Networking** tab, select **PPTP VPN** from the **Type of VPN** drop-down list.

jjj) Make sure that the **Internet Protocol (TCP/IP)** check box is checked.

kkk) Make sure that the **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, **File and Printer Sharing for Microsoft Networks**, and **Client for Microsoft Networks** check boxes are cleared.

lll) Click the **OK** button to save the changes to make them take effect.

(8) Connect the Computer to the Device through the PPTP Tunnel

p) Please make sure that your computer has been connected to the Internet.

q) Double-click the new connection **PPTP** you have just created.

r) Enter **PC1** in the **User name** text box and **PC1** in the **Password** text box.

s) Click the **Connect** button.

t) After the PPTP tunnel has been established successfully, if you run the **ipconfig** command at the MS-DOS command prompt on the computer, you can see the IP address assigned by the Device.

**}**

## 10.3 IPSec

With the development of network safety standards and protocols, various VPN technologies have emerged. IPSec VPN is one of the most widely used VPN security technologies today.

IPSec is a set of open standards and protocols to implement network secure communication, which provides two security mechanisms: encryption and authentication. Encryption mechanism is used to ensure data confidentiality; and authentication mechanism is used to ensure that data is from the claimed sender and not destroyed or tampered during transmission.

### 10.3.1.1 Abbreviations and Terminology

IPSec (IP Security): IPSec consists of a set of services and protocols developed by the IETF. It provides various types of protection, including authentication, integrity, and confidentiality, to support secure exchange of packets at the IP layer over the Internet.

IKE (Internet Key Exchange): IKE is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec endpoints, negotiation and creation of IKE and IPSec security associations, and establishment of keys for encryption algorithms used by IPSec.

DES (Data Encryption Standard): DES is a data encryption algorithm supported by IPSec. DES uses a 56-bit key to encrypt and decrypt the packets, ensuring high-performance encryption.

3DES (Triple Data Encryption Standard): 3DES is a data encryption algorithm supported by IPSec. As a variant of the 56-bit DES, 3DES effectively doubles encryption strength over 56-bit DES.

AES (Advanced Encryption Standard): AES is a data encryption algorithm supported by IPSec. In comparison with DES and 3DES, AES is safer and more efficient.

DH (Diffie-Hellman): DH is a public key cryptography protocol. It allows two endpoints to establish a shared secret key dynamically over an insecure network channel. DH is used in IKE to establish session keys which are used by encryption algorithms, such as DES, 3DES, AES or MD5.

MD5 (Message Digest 5): MD5 is a hash algorithm that produces a 128-bit hash (also called message digest or digital signature) from a message of arbitrary length. The hash is used to verify data origin authentication and data integrity.

SHA-1 (Secure Hash Algorithm 1): SHA-1 is a hash algorithm produces a 160-bit hash (also called message digest or digital signature) from a message of arbitrary length. As SHA-1 can produce a larger hash, it is considered cryptographically stronger than MD5.

}

SA (Security Association): The concept of a **Security Association** (**SA**) is fundamental to **IPSec**. An SA is a relationship between two IPSec endpoints that describes how the endpoints will use security services to communicate. Each SA consists of a set of security parameters like security protocol (ESP or AH), encryption and/or authentication algorithms and keys, SA lifetime, and so on.

SPI (Security Parameter Index): SPI is a 32-bit number that is used to identify an SA. The receiver uses the SPI, along with the destination IP address and security protocol type (AH or ESP) to uniquely identify an SA.

AH (Authentication Header): IPSec has two core security protocols: AH and ESP. AH provides data origin authentication, data integrity, and optional anti-replay services. In comparison with ESP, it does not provide data confidentiality; but it provides one benefit that ESP does not: integrity protection for the outermost IP header.

ESP (Encapsulating Security Payload): IPSec has two core security protocols: AH and ESP. ESP provides data confidentiality, data integrity, and optional data origin authentication and anti-replay services.

PSK (Pre-Shared Key): It is one of the IKE authentication methods. In this method, IKE endpoints use the same pre-shared key to authenticate each other.

Phase 1 and Phase 2: When using IKE to establish an IPSec tunnel, the basic operation of IKE can be broken down into two phases: Phase 1 is used to authenticate the two endpoints, and negotiate the parameters and key material required to establish a secure channel (i.e., IKE SA). The IKE SA is then used to protect further IKE exchanges; and Phase 2 is used to negotiate the parameters and key material required to establish IPSec SAs. The IPSec SAs are then used to authenticate and encrypt the user data.

Main Mode and Aggressive Mode: IKE supports two modes of its phase 1 negotiations: main mode and aggressive mode. Aggressive mode offers a faster alternative to main mode. In main mode, the initiator and recipient negotiate the IKE SA through three pairs of messages. In aggressive mode, the initiator and recipient negotiate the IKE SA through three messages.

DPD (Dead Peer Detect): DPD is a method to enable a device to periodically detect whether its peer is still available. The Device performs this detection by sending DPD heartbeat messages at the specified time interval.

IPSec NAT-T (NAT-Traversal): It allows two IPSec devices establish an IPSec tunnel traverse one or more NAT devices.

MTU (Maximum Transmission Unit): It represents the maximum packet size that can be transmitted over a network.

IPSec Tunnel: An IPSec tunnel is a virtual secure pipe between two endpoints. The IPSec tunnel can across multiple routers and networks, and it allows the IPSec protected packets are transparently forwarded through these routers and networks.

}

## 10.3.1.2 Creating Security Associations (SAs)

The concept of a Security Association (SA) is fundamental to IPSec. An SA is a relationship between two IPSec endpoints that describes how the endpoints will use security services to communicate**.** Each SA consists of a set of security parameters like security protocol (ESP or AH), encryption and/or authentication algorithms, session keys, SA lifetime, and so on. Because an IPSec SA is simplex (unidirectional) in nature, a bidirectional communication requires at least two SAs, one in each direction.

The basic operation of IKE can be broken down into two phases:

- IKE Phase 1 is used to authenticate the two endpoints and negotiate the parameters and key material required to establish a secure channel (i.e., IKE SA). The IKE SA is then used to protect further IKE exchanges.

- IKE Phase 2 is used to negotiate the parameters and key material required to establish IPSec SAs. The IPSec SAs are then used to authenticate and encrypt the user data.

### 1) IKE Phase 1

During IKE phase 1, one or more security proposals are exchanged and agreed upon between the two endpoints. The two endpoints exchange proposals for acceptable security services such as:

- Encryption algorithm (DES, 3DES, or AES 98/99/256)

- Authentication algorithm (MD5 or SHA-1)

- Diffie-Hellman group (Refer to Diffie-Hellman Exchange described later in this section for more information.)

- Preshared key

When both IPSec endpoints agree to accept at least one set of the proposed phase 1 security parameters and then process them, a successful phase 1 negotiation concludes. When acting as an initiator, the Device supports up to 8 phase 1 proposals, which allow you to specify a series of security parameters; when acting as a responder, it can accept any phase 1 proposal.

### Main Mode and Aggressive Mode

IKE supports two modes of its phase 1 negotiations: main mode and aggressive mode, the following describes them respectively.

**Main Mode**

Main mode has three two-way exchanges with a total of six messages between the initiator and the responder.

- First exchange (message 1 and 2): The encryption and authentication algorithms used to secure the IKE communications are negotiated and agreed upon between the two endpoints.
- Second exchange (message 3 and 4): A Diffie-Hellman exchange is performed. Each endpoint exchanges a nonce (i.e., random number).
- Third exchange (message 5 and 6): Identities of both endpoints are exchanged and verified.

In the third exchange, identities are not transmitted in clear text. The identities are protected by the encryption algorithm agreed upon in the first two exchanges.

### Aggressive Mode

Aggressive mode has two exchanges with a total of three messages between the initiator and the responder.

- First message: The initiator proposes the SA, initiates a Diffie-Hellman exchange, and sends a nonce (i.e., random number) and its IKE identity.
- Second message: The responder accepts the proposed SA, authenticates the initiator, and sends a nonce (i.e., random number), its IKE identity, and its certificates if it is being used.
- Third message: The initiator authenticates the responder, confirms the exchange, and sends its certificates if it is being used.

The weakness of using aggressive mode is that it does not provide identity protection because the identities of both sides are exchanged in clear text. However, aggressive mode is faster than main mode.

**Note:** If one of the two IPSec endpoints has a dynamic IP address, you must use aggressive mode to establish an IPSec tunnel.

## Diffie-Hellman Exchange

The Diffie-Hellman exchange is a public key cryptography protocol used for key exchange. With Diffie-Hellman exchange, the two IPSec endpoints publicly exchange key material over an insecure network channel to derive a shared secret key, which is never exchanged over the insecure channel.

There are five basic DH groups (The Device supports DH groups 2 and 5). Each DH group has a different size modulus. A larger modulus provides higher security, but requires more processing time to generate the key. The modulus of DH groups 2 and 5 are as follows:

- DH Group 2: 924-bit modulus

- DH Group 5: 1536-bit modulus

⌖ **Note:** Both endpoints of an IPSec tunnel should use the same DH group because each group has a different size modulus.

### 2) IKE Phase 2

Once an IKE SA is established successfully in phase 1, the two IPSec endpoints will use it to negotiate IPsec SAs in phase 2. The IPSec SAs are used to secure the user data to be transmitted through the IPSec tunnel.

During IKE Phase 2, the two IPSec endpoints also exchange security proposals to determine which security parameters to be used in the IPSec SAs. A phase 2 proposal consists of one or two IPSec security protocols (either ESP or AH, or both), the encryption and/or authentication algorithms used with the selected security protocol.

IKE phase 2 has one mode, which is called **Quick Mode**. Quick mode uses three messages to establish IPSec SAs.

## 10.3.1.3 Maintain Security Associations (SAs)

After the SAs have been established, the two IPSec endpoints should maintain the SAs to ensure that the SAs are secure and available. IPSec provides the following methods to maintain and detect SAs.

### 1) SA Lifetime

During IKE and IPSec SAs negotiation and creation, the two IPSec endpoints also negotiate a lifetime for each SA. If an SA is nearing the end of the lifetime, the endpoints must negotiate and create a new SA and use it instead. The SA lifetime specifies how often each SA should be renegotiated, either based on elapsed time or the amount of network traffic.

Reducing the lifetime forces the IPSec endpoints to renegotiate the SAs more frequently. This frequent renegotiation improves security, but at the expense of higher CPU utilization and possible delays during the renegotiation process. Therefore, the SA lifetime is often set to a relatively long time (the suggested value is between 1 and 24 hours). Because there is no way for the IPSec endpoints to identify the loss of peer connectivity, the SAs can remain until their lifetimes naturally expire, and each endpoint assumes that its peer is available before their SAs expire. Then, if the connectivity between the two endpoints goes down unexpectedly due to routing problems, system rebooting, etc., one endpoint still continues to send the packets to its peer until the SAs expire; this results in a false connection (SAs are normal, but the tunnel is disconnected) where packets are tunneled to oblivion. Therefore, it is necessary that either endpoint can detect a dead peer as soon as possible; a method called Dead Peer Detection (DPD) is used to achieve this purpose. DPD has smaller cost than SA renegotiation, so it is always performed at a higher frequency.

### 2) DPD (Dead Peer Detect)

}

Dead Peer Detection (DPD) is a traffic-based method of detecting a dead IKE peer. DPD allows an endpoint to prove its peer’s liveliness periodically. This can help the endpoint to avoid a situation where it sends IPSec packets to a peer that is no longer available (“Martian” host). After DPD is enabled, the endpoint periodically sends DPD heartbeat messages at the specified time interval (usually 20 seconds or about 1 minute) to the peer to verify its availability. After missing several consecutive heartbeat messages, the endpoint will renegotiate the SAs with the peer.

## 10.3.1.4 IPSec NAT Traversal

Network Address Translation (NAT) is a technology that allows multiple hosts on a private network to share a single or a small group of public IP addresses. Undoubtedly, NAT can help conserve the remaining IP address space and provide the benefit of network security assurance; however, it has introduced problems for end-to-end protocols like IPSec. NAT is incompatible with IPSec, which is one of the most popular VPN technologies.

Why doesn’t NAT work with IPSec? One main reason is that NAT devices modify the IP header of a packet, this causes an AH-protected packet to fail checksum validation; and they cannot modify the ports in the encrypted TCP header of an ESP-protected packet. The solution is IPSec NAT Traversal, or NAT-T.

The IPSec working group of the IEEE has created standards for NAT-T that are defined in RFC 3947 (Negotiation of NAT-Traversal in the IKE) and RFC 3948 (UDP Encapsulation of IPsec ESP Packets). IPSec NAT-T is designed to solve the problems inherent in using IPSec with NAT.

During IKE phase 1 negotiation, the two IPSec NAT-T-capable endpoints can automatically determine:

- Whether both of the IPSec endpoints can perform IPSec NAT-T.
- If there are any NAT devices along the path between them.

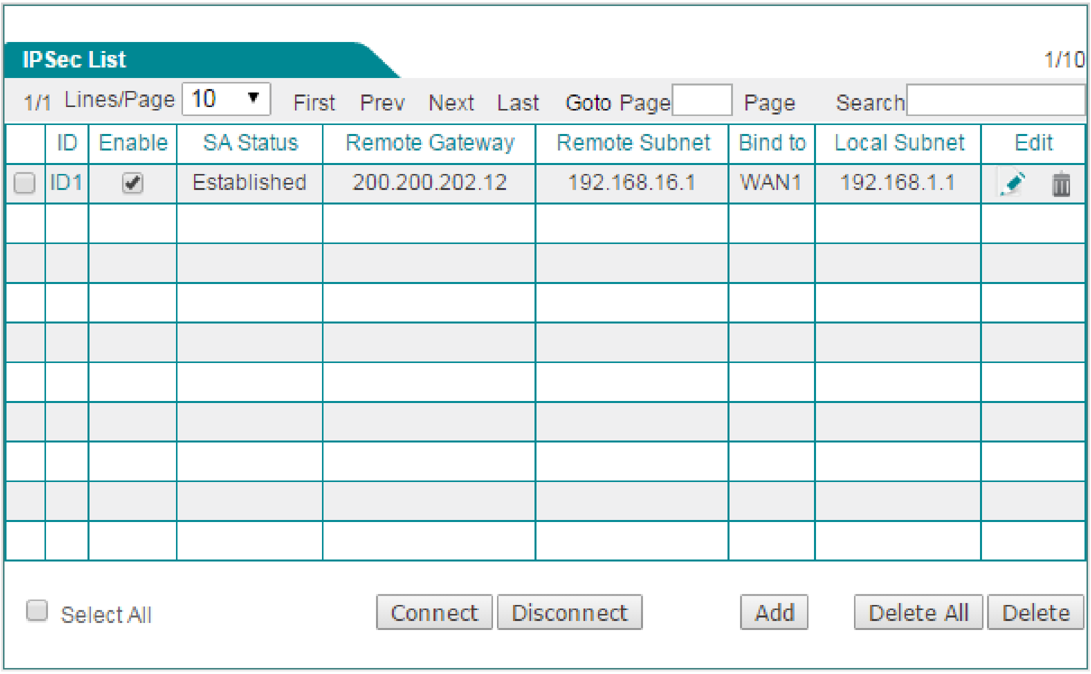
If both of these two conditions are true, the two endpoints will automatically use IPSec NAT-T to send IPSec protected packets. If either endpoint doesn’t support IPSec NAT-T, they will perform normal IPSec negotiations (beyond the first two messages) and IPSec protection. If both endpoints support IPSec NAT-T, but there is no NAT device between them, they will perform normal IPSec protection.

**Note:** IPSec NAT-T is only defined for ESP traffic. AH traffic cannot traverse NAT devices, therefore, do not use AH if any **NAT device** is present on your network.

The Device supports IPSec NAT-T feature. With NAT-T, the Device will add a UDP header to the ESP-protected packets after detecting one of more NAT devices along the data path during IKE phase 1 negotiation. This new UDP header sits between the ESP header and the outer IP header, and usually uses UDP port 4500.

## 10.3.1.5 IPSec List

You can view the IPSec entry configuration and status information in the **IPSec List.** Note when the connection type is **Answer-Only**, the **Connect** button is invalid.



IPSec List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | ID | Enable | SA Status | Remote Gateway | Remote Subnet | Bind to | Local Subnet | Edit |
|---|---|---|---|---|---|---|---|---|
| □ | ID1 | ☑ | Established | 200.200.202.12 | 192.168.16.1 | WAN1 | 192.168.1.1 | ✎ 🗑 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

**Figure 10-39 IPSec List**

## 10.3.1.6 IPSec settings

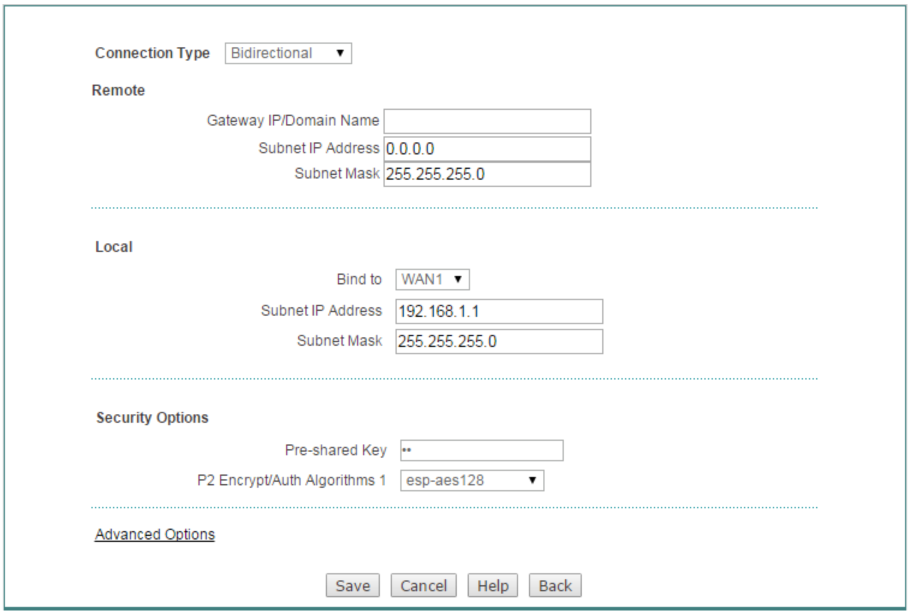
There are three connection types to choose: **Bidirectional**, **Originate-Only**, and **Answer-Only**. For each connection type, the configuration parameters are divided into two categories: basic and advanced parameters. Therein, the basic parameters for each type are different, but the advanced parameters are the same. The following will describe the basic parameters for each connection type respectively, and then describe the advanced parameters for them.

1) Basic Parameters Settings

(1) Bidirectional

If both IPSec endpoints have static IP addresses, you can choose **Bidirectional** as the connection type. In this case, the local Device can act as an initiator or responder.

}



Connection Type: Bidirectional

Remote

Gateway IP/Domain Name:

Subnet IP Address: 0.0.0.0

Subnet Mask: 255.255.255.0

Local

Bind to: WAN1

Subnet IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Security Options

Pre-shared Key: ••

P2 Encrypt/Auth Algorithms 1: esp-aes128

**Figure 10-40 IPSec Settings_Bidirectional**

- **Connection Type:** Specify the role of the Device in the IPSec tunnel establishment. The available options are **Bidirectional**, **Originate-Only** and **Answer-Only**. Here please select **Bidirectional**.

- **Gateway IP/Domain Name (Remote):** Specify the IP address or domain name of the Device at the other end of the IPSec tunnel. Note: If you enter a domain name, you should configure at least one DNS server on the Device. Then the Device will periodically resolve the domain name, and renegotiate the IPSec tunnel if the remote IPSec device's IP address changes.

- **Subnet IP Address** and **Subnet Mask (Remote):** Specify the remote subnet or host that can be accessed from the local side of the IPSec tunnel. If you want to define a subnet, please enter any IP address belonging to that subnet in the **Subnet IP** text box and its mask in the **Subnet Mask** text box; if you want to define a host, please enter the IP address of that host in the **Subnet IP** text box and 255.255.255.255 in the **Subnet Mask** text box.

- **Bind to (Local):** Specify an interface to which the IPSec tunnel is bound. The IPSec module will check any inbound and outbound packets through this interface to decide if the packets require IPSec processing.

- **Subnet IP Address** and **Subnet Mask (Remote):** Specify the local subnet or host that can be accessed from the remote side of the IPSec tunnel. If you want to define a subnet, please enter any IP address belonging to that subnet in the **Subnet IP** text box and its mask in the **Subnet Mask** text box; if you want to define a host, please enter the IP address of that host in the **Subnet IP** text box and 255.255.255.255 in the **Subnet Mask** text box.

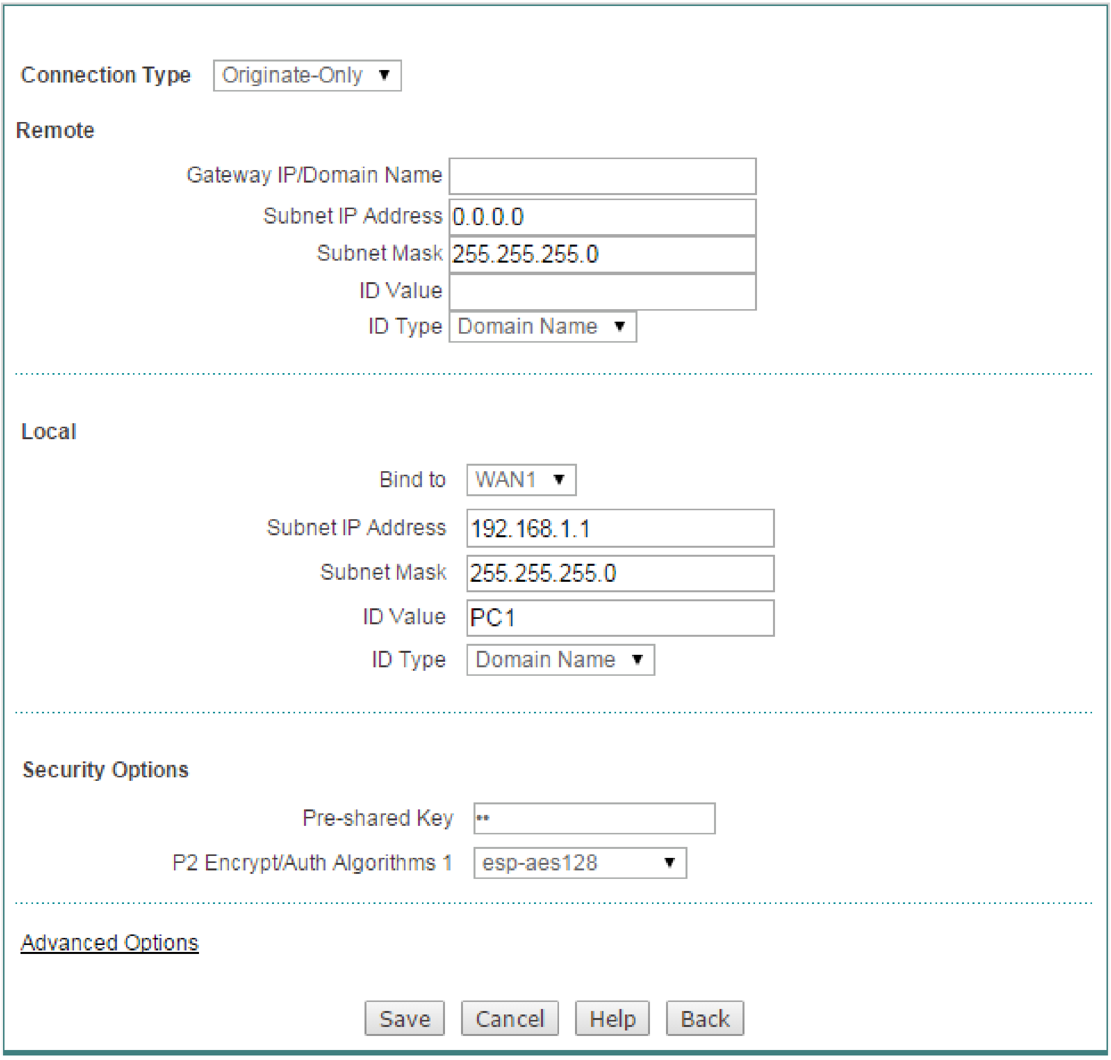
- **Pre-shared Key:** Specify a preshared key for IKE negotiation. It should be no more than 128 characters long. Note that you must enter the same preshared key at the remote IPSec device.

}

- **P2 Encrypt/Auth Algorithms 1:** It refers to the preferred phase 2 proposal that specifies a set of security protocols and algorithms for phase 2 negotiation.

(2) Originate-Only

If the local Device has a dynamically assigned IP address, and the remote endpoint (another enterprise wireless router or compatible VPN appliance) has a static IP address, you can choose **Originate-Only** as the connection type. In this case, the local Device can only act as an initiator, and both IPSec endpoints should use aggressive mode for phase 1 IKE negotiation.



Connection Type: Originate-Only ▼

Remote

Gateway IP/Domain Name:
Subnet IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0
ID Value:
ID Type: Domain Name ▼

Local

Bind to: WAN1 ▼
Subnet IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
ID Value: PC1
ID Type: Domain Name ▼

Security Options

Pre-shared Key: ••
P2 Encrypt/Auth Algorithms 1: esp-aes128 ▼

**Figure 10-41 IPSec Settings_Originate-Only**

The parameters **Gateway IP/Domain Name (Remote)**, **Subnet IP (Remote)**, **Subnet Mask (Remote)**, **Bind to (Local)**, **Subnet IP (Local)**, **Subnet Mask (Local)**, **Preshared Key**, and **P2 Encrypt/Auth Algorithms 1** are the same as those in the **Bidirectional** connection type, please refer to the detailed descriptions of them.

The difference is that this connection type requires identity authentication. Specifically, the identity authentication for the local Device is required, that is, the local Device should provide its identity information to the remote IPSec endpoint for

}

authentication; but the identity authentication for the remote IPSec endpoint is optional.

- **ID Type (Remote):** Specify the type of remote ID. The available options are **Domain Name**, **Email Address**, **IP Address** and **Other**. In this connection type, it is an optional parameter. If you want remote IPSec device to be authenticated, please select one type and then specify **ID Value (Remote)**.

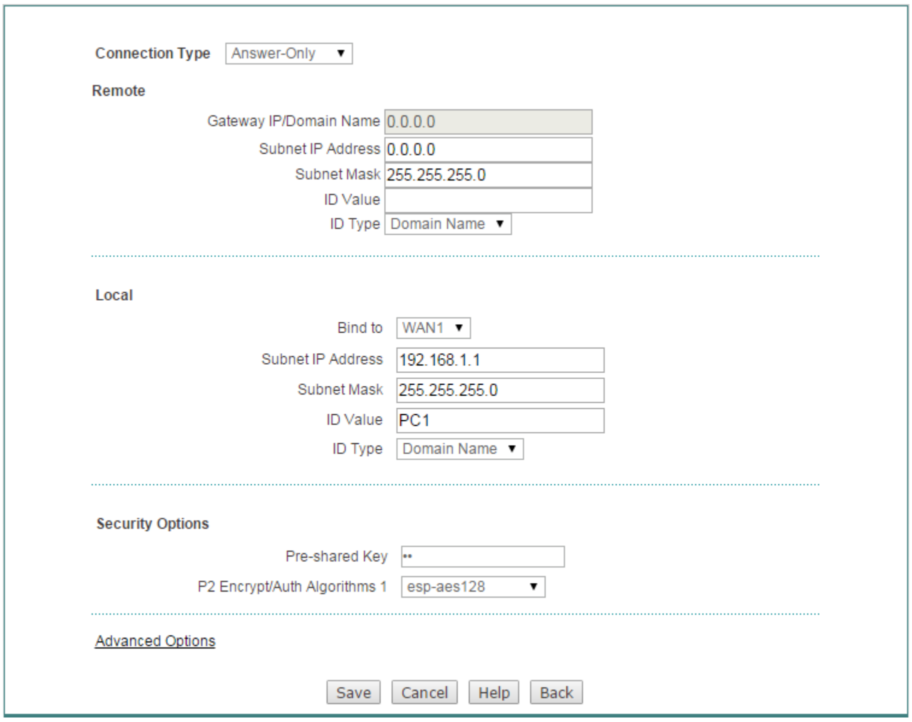
- **ID Value (Remote):** Specify the identity of the remote IPSec device. In this connection type, it is an optional parameter. Please enter an ID value according to the selected **ID Type (Remote)**.

- **ID Type (Local):** Specify the type of local ID. The available options are **Domain Name**, **Email Address**, **IP Address** and **Other**. In this connection type, it is a required parameter. You must select one type and then specify **ID Value (Local)** to allow the remote IPSec device to authenticate the local Device.

- **ID Value (Local):** Specify the identity of the local Device. In this connection type, it is a required parameter. Please enter an ID value according to the selected **ID Type (Local)**.

(3) Answer-Only

If the local Device has a static IP address, and the remote endpoint (another enterprise wireless router or compatible VPN appliance) has a dynamically assigned IP address, you can choose **Answer-Only** as the connection type. In this case, the local Device can only act as a responder, and both IPSec endpoints should use aggressive mode for phase 1 IKE negotiation.



Connection Type: Answer-Only

Remote

Gateway IP/Domain Name: 0.0.0.0
Subnet IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0
ID Value:
ID Type: Domain Name

Local

Bind to: WAN1
Subnet IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
ID Value: PC1
ID Type: Domain Name

Security Options

Pre-shared Key: ••
P2 Encrypt/Auth Algorithms 1: esp-aes128

**Figure 10-42 IPSec Settings_Answer-Only**

}

The parameters **Gateway IP/Domain Name (Remote)**, **Subnet IP (Remote)**, **Subnet Mask (Remote)**, **Bind to (Local)**, **Subnet IP (Local)**, **Subnet Mask (Local)**, **Preshared Key**, and **P2 Encrypt/Auth Algorithms 1** are the same as those in the **Bidirectional** connection type, please refer to the detailed descriptions of them.

The difference is that this connection type requires identity authentication. Specifically, the identity authentication for the remote IPSec endpoint is required, that is, the remote IPSec endpoint should provide its identity information to the local Device for authentication; but the identity authentication for the local Device is optional.

- **ID Type (Remote):** Specify the type of remote ID. The available options are **Domain Name**, **Email Address**, and **IP Address**. In this connection type, it is a required parameter. You must select one type and then specify **ID Value (Remote)** to allow the local Device to authenticate the remote IPSec device.

- **ID Value (Remote):** Specify the identity of the remote IPSec device. In this connection type, it is an optional parameter. Please enter an ID value according to the selected **ID Type (Remote)**.

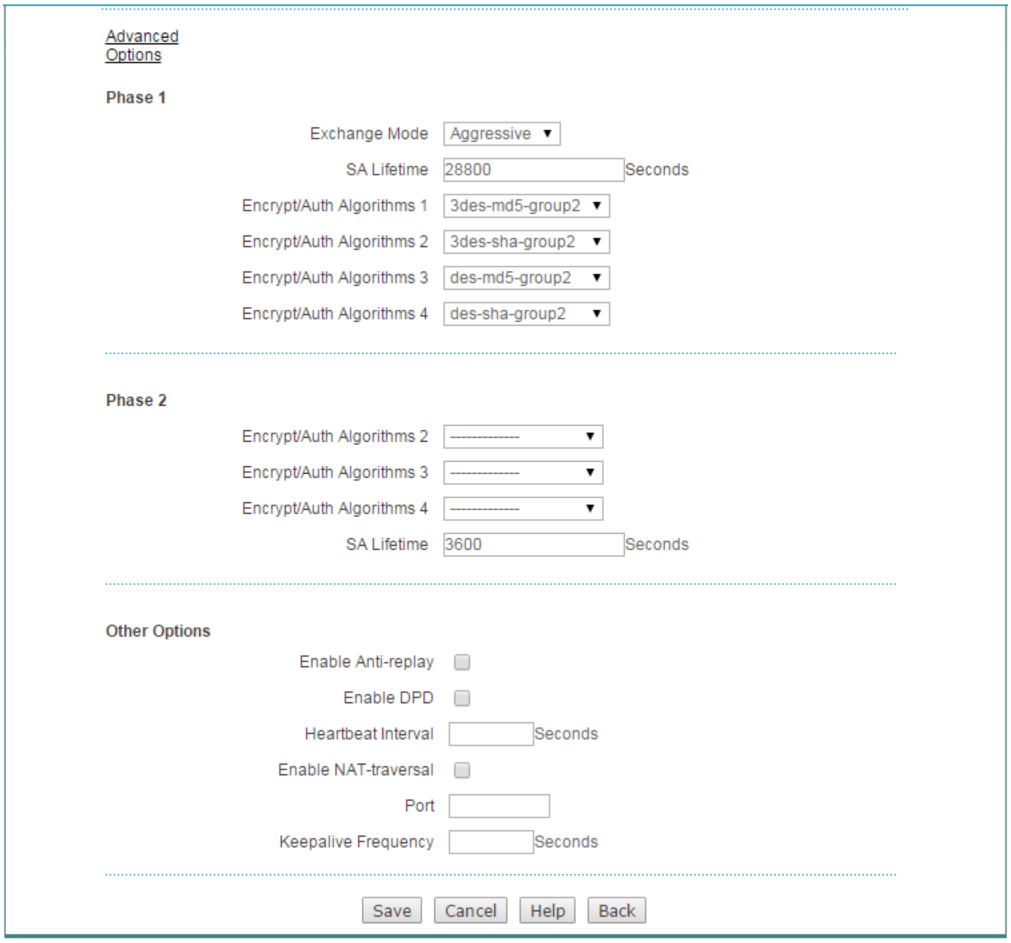
- **ID Type (Local):** Specify the type of local ID. The available options are **Domain Name**, **Email Address**, and **IP Address**. In this connection type, it is an optional parameter. If you want the local Device to be authenticated, please select one type and then specify **ID Value (Local).**

- **ID Value (Local):** Specify the identity of the local Device. In this connection type, it is a required parameter. Please enter an ID value according to the selected **ID Type (Local)**.

2) Advanced Parameters Settings

Click the **Advanced Options** hyperlink to view and configure advanced parameters. In most cases, you need not configure them. In the **Bidirectional** connection type, you should choose **Main** mode as the exchange mode for phase 1 IKE negotiation; in the **Originate-Only** or **Answer-Only** connection type, you should choose **Aggressive** mode.

**}**



Advanced Options

**Phase 1**

| | |
|---|---|
| Exchange Mode | Aggressive ▼ |
| SA Lifetime | 28800 Seconds |
| Encrypt/Auth Algorithms 1 | 3des-md5-group2 ▼ |
| Encrypt/Auth Algorithms 2 | 3des-sha-group2 ▼ |
| Encrypt/Auth Algorithms 3 | des-md5-group2 ▼ |
| Encrypt/Auth Algorithms 4 | des-sha-group2 ▼ |

**Phase 2**

| | |
|---|---|
| Encrypt/Auth Algorithms 2 | ------------- ▼ |
| Encrypt/Auth Algorithms 3 | ------------- ▼ |
| Encrypt/Auth Algorithms 4 | ------------- ▼ |
| SA Lifetime | 3600 Seconds |

**Other Options**

| | |
|---|---|
| Enable Anti-replay | □ |
| Enable DPD | □ |
| Heartbeat Interval | Seconds |
| Enable NAT-traversal | □ |
| Port | |
| Keepalive Frequency | Seconds |

**Figure 10-43 IPSec Advanced settings**

- **Exchange Mode:** Specify the exchange mode used for IKE phase 1 negotiation. The available options are **Main** and **Aggressive**. If the **Connection Type** is **Bidirectional**, you should choose **Main** mode; else, you should choose **Aggressive** mode.

- **SA Lifetime:** It refers to IKE SA lifetime, which specifies the number of seconds (at least 600 seconds) an IKE SA will exist before expiring. A new IKE SA is negotiated 540 seconds before the existing IKE SA expires.

- **Encrypt/Auth Algorithms 1 ~ Encrypt/Auth Algorithms 4 (Phase 1):** They refer to phase 1 proposal that specifies a set of security algorithms for phase 1 negotiation. A phase 1 proposal includes an encryption algorithm, an authentication algorithm, and a DH group. You can choose up to four phase 1 proposals.

- **Encrypt/Auth Algorithms 2 ~ Encrypt/Auth Algorithms 4 (Phase 2):** They refer to phase 2 proposal that specifies a set of security protocols and algorithms for phase 2 negotiation. You can choose up to three phase 2 proposals together with **P2 Encrypt/Auth Algorithms 1**.

- **SA Lifetime:** It refers to IPSec SA time lifetime, which specifies the number of seconds (at least 600 seconds) an IPSec SA will exist before expiring. A new IPSec SA is negotiated 540 seconds before the existing IPSec SA expires.

}

- **Enable Anti-replay:** If selected, the Device can detect and reject replayed packets (i.e., old or duplicate packets) to protect itself against replay attacks.

- **Enable DPD:** If selected, the Device will periodically send DPD heartbeat messages at the specified time interval (set by the **Heartbeat Interval)** to the remote IPSec device to verify its availability.

- **Heartbeat Interval:** Specify a time interval (in seconds) at which the Device will periodically send DPD heartbeat messages to the remote IPSec device to verify its availability.

- **Enable NAT-traversal:** If selected, two IPSec devices could establish an IPSec tunnel traverse one or more NAT devices.

- **Port:** Specify the number of UPD port for NAT traversal. The default value is 4500.

- **Keepalive Frequency:** Specify a time interval (in seconds) at which the Device will periodically send keepalive packets to the NAT device to keep the NAT mapping active, so that the NAT mapping doesn't change until the IKE SA and IPSec SAs expire. This parameter will only take effect when NAT-traversal is enabled.

## 10.3.1.7 Example of IPSec

## 10.3.1.8 Bidirectional

If both IPSec endpoints have static IP addresses, you can choose **Bidirectional** as the connection type.

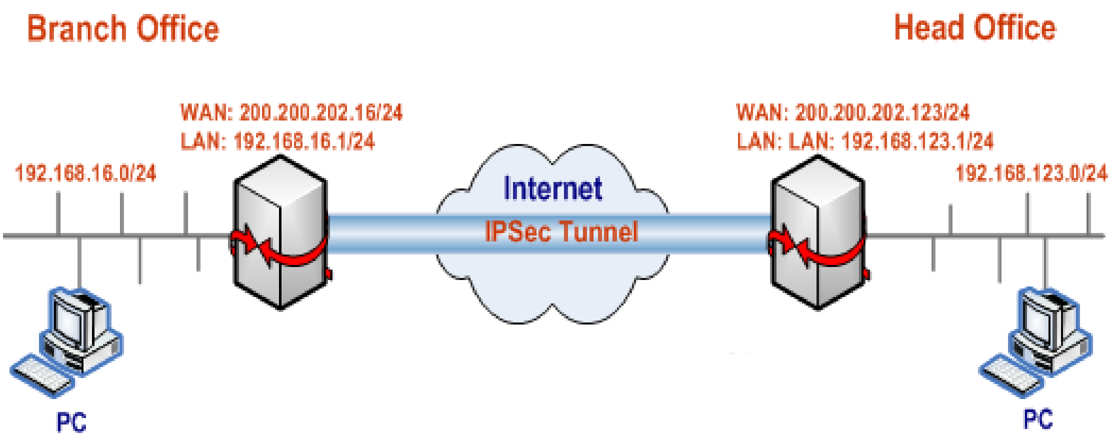


**Figure 10-44 Network Topology – Bidirectional**

In this scenario, we deploy two UTT enterprise wireless routers at a company: one is located at the head office, and the other is located at the branch office. Now we want to establish an IPSec tunnel between them, and use the following proposals (i.e., encryption and authentication algorithms): the phase 1 proposals are left at their default values, and the preferred phase 2 proposal is esp-aes256-md5; in addition,

}

the preshared key is testing, and the IP addresses are as follows:

**The Device at the head office:**

- WAN Interface IP Address: 200.200.202.123/24
- Default Gateway IP Address: 200.200.202.254/24
- LAN Interface IP Address: 192.168.123.1/24

**The Device at the branch office:**

- WAN Interface IP Address: 200.200.202.16/24
- Default Gateway IP Address: 200.200.202.254/24
- LAN Interface IP Address: 192.168.16.1/24

1) Configuring the Device at the head office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

| | |
|---|---|
| Connection Type | Bidirectional |
| Gateway IP/Domain Name (Remote) | 200.200.202.16 |
| Subnet IP (Remote) | 192.168.16.1 |
| Subnet Mask (Remote) | 255.255.255.0 |
| Bind to (Local) | WAN1 |
| Subnet IP (Local) | 192.168.123.1 |
| Subnet Mask (Local) | 255.255.255.0 |
| Preshared Key | testing |
| P2 Encrypt/Auth Algorithms 1 | esp-aes256-md5 |

2) Configuring the Device at the branch office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

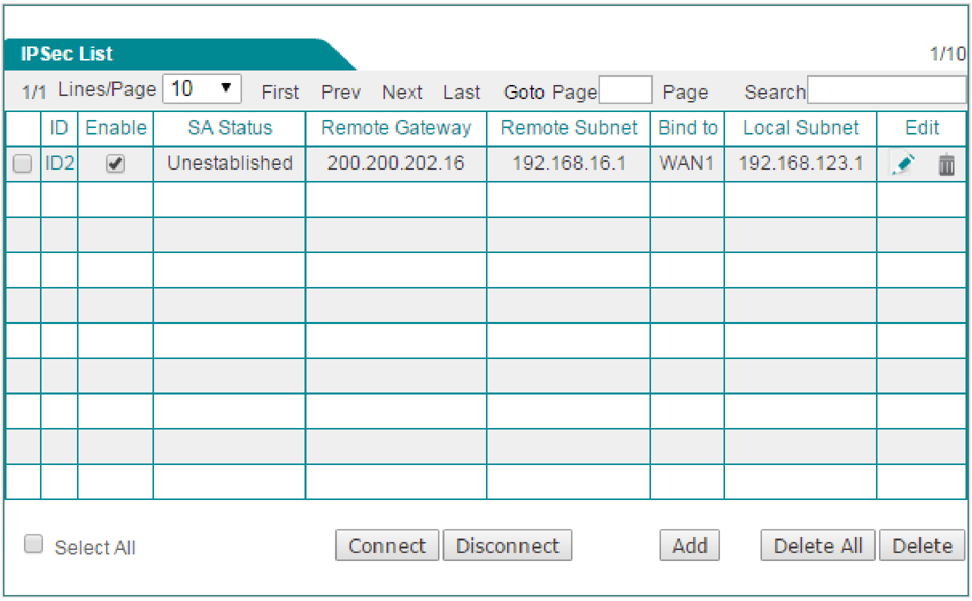
**}**

| | |
|---|---|
| Connection Type | Bidirectional |
| Gateway IP/Domain Name (Remote) | 200.200.202.123 |
| Subnet IP (Remote) | 192.168.123.1 |
| Subnet Mask (Remote) | 255.255.255.0 |
| Bind to (Local) | WAN1 |
| Subnet IP (Local) | 192.168.16.1 |
| Subnet Mask (Local) | 255.255.255.0 |
| Preshared Key | testing |
| P2 Encrypt/Auth Algorithms 1 | esp-aes256-md5 |

3) Viewing the IPSec tunnel status

After you have configured IPSec parameters on both Devices, the IPSec tunnel establishment can be triggered manually.

On the Device, you can go to the **VPN > IPSec > IPSec List** page to view the configuration of the IPSec tunnel, including the **SA Status**, **Remote Gateway**, **Remote Subnet**, **Bind to** and **Local Subnet**. After the IPSec tunnel has been established, you can see that the **SA Status** displays **Established**.


IPSec List
1/10
1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search
Select All
Connect
Disconnect
Add
Delete All
Delete

| | ID | Enable | SA Status | Remote Gateway | Remote Subnet | Bind to | Local Subnet | Edit |
|---|---|---|---|---|---|---|---|---|
| □ | ID2 | ☑ | Unestablished | 200.200.202.16 | 192.168.16.1 | WAN1 | 192.168.123.1 | ✎ 🗑 |

Figure 10-45 IPSec List – Bidirectional

}

## 10.3.1.9 Answer-Only and Originate-Only

If the local gateway has a dynamically assigned IP address (PPPoE or DHCP), and the remote endpoint has a static IP address, you can choose **Originate-Only** as the connection type and **Answer-Only** as the connection type on the other side. In this case, both IPSec endpoints should use aggressive mode for phase 1 IKE negotiation.

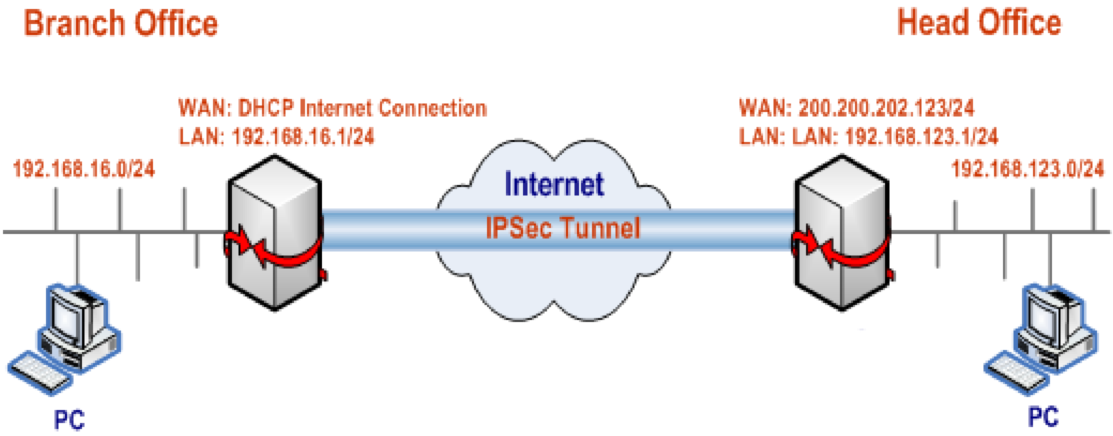


**Figure 10-46 Network Topology_Answer-Only and Originate-Only**

In this scenario, we deploy two enterprise wireless router at a company: one is located at the head office and connected to the Internet with a static IP address; the other is located at the branch office and connected to the Internet with a dynamic IP address (DHCP Internet connection).

Now we want to establish an IPSec tunnel between them, and use the following proposals (i.e., encryption and authentication algorithms): the phase 1 proposals are left at their default values, and the preferred phase 2 proposal is esp-aes192; in addition, the preshared key is testing, the originator's ID type is Email address and value is hiper@utt.com.cn, and the IP addresses are as follows:

The Device at the head office:

- WAN Interface IP Address: 200.200.202.123/24
- LAN Interface IP Address: 192.168.123.1/24

The Device at the branch office:

- WAN Interface IP Address: Dynamic (DHCP)
- LAN Interface IP Address: 192.168.16.1/24

1) Configuring the Device at the head office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

}

| | |
|---|---|
| Connection Type | Answer-Only |
| Gateway IP/Domain Name (Remote) | 0.0.0.0 |
| Subnet IP (Remote) | 192.168.16.1 |
| Subnet Mask (Remote) | 255.255.255.0 |
| ID Type (Remote) | Email Address |
| ID Value (Remote) | hiper@utt.com.cn |
| Bind to (Local) | WAN1 |
| Subnet IP (Local) | 192.168.123.1 |
| Subnet Mask (Local) | 255.255.255.0 |
| Preshared Key | testing |
| P2 Encrypt/Auth Algorithms 1 | esp-aes192 |
| Advanced Options | |
| Exchange Mode | Aggressive |

2) Configuring the Device at the branch office

Go to the **VPN > IPSec > IPSec Settings** page, make the following settings (leave the default values for the other parameters), and then click the **Save** button.

| | |
|---|---|
| Connection Type | Originate-Only |
| Gateway IP/Domain Name (Remote) | 200.200.202.123 |
| Subnet IP (Remote) | 192.168.123.1 |
| Subnet Mask (Remote) | 255.255.255.0 |
| Bind to (Local) | WAN1 |
| Subnet IP (Local) | 192.168.16.1 |
| Subnet Mask (Local) | 255.255.255.0 |
| ID Type (Local) | Email Address |
| ID Value (Local) | hiper@utt.com.cn |
| Preshared Key | testing |
| P2 Encrypt/Auth Algorithms 1 | esp-aes192 |
| Advanced Options | |
| Exchange Mode | Aggressive |

**}**

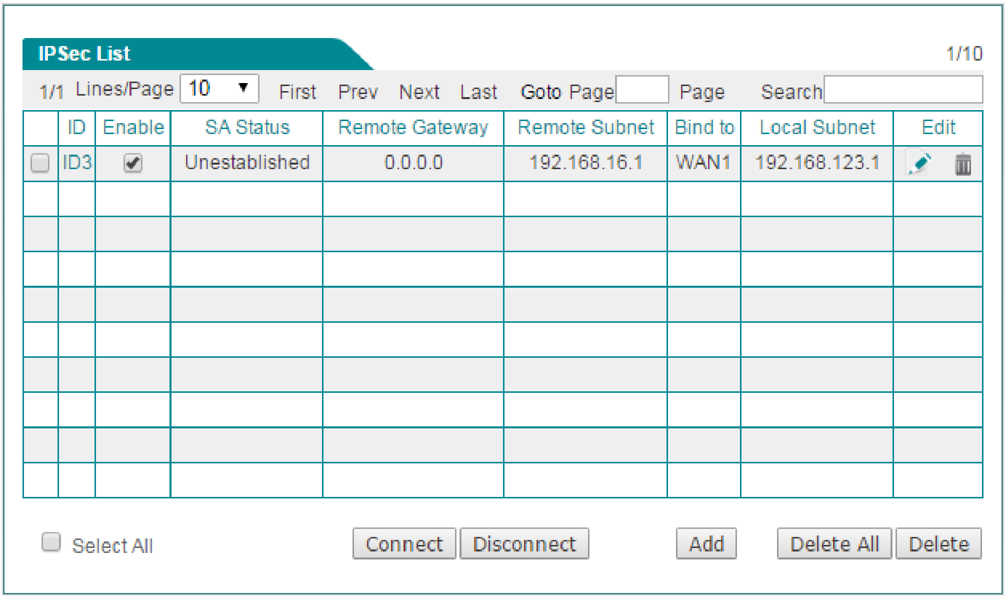
3) Viewing the IPSec tunnel status

After you have configured IPSec parameters on both Devices, the IPSec tunnel establishment can be triggered manually.

On the Device, you can go to the **VPN > IPSec > IPSec List** page to view the configuration of the IPSec tunnel, including the **Key Mode**, **Remote Gateway**, **Remote Subnet IP**, **Bind to** and **Local Subnet IP**,. After the IPSec tunnel has been established, you can see that the **SA Status** displays **Established**, and the **Out Pkts** and **In Pkts** will go on increasing as long as there is some network traffic being passed through the IPSec tunnel.

(1) Viewing the Device at the head office

The following figure shows the configuration and status of the IPSec tunnel on the Device with a static IP address at the head office.



IPSec List 1/10

1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page [ ] Page Search [ ]

| | ID | Enable | SA Status | Remote Gateway | Remote Subnet | Bind to | Local Subnet | Edit |
|---|---|---|---|---|---|---|---|---|
| □ | ID3 | ☑ | Unestablished | 0.0.0.0 | 192.168.16.1 | WAN1 | 192.168.123.1 | ✎ 🗑 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

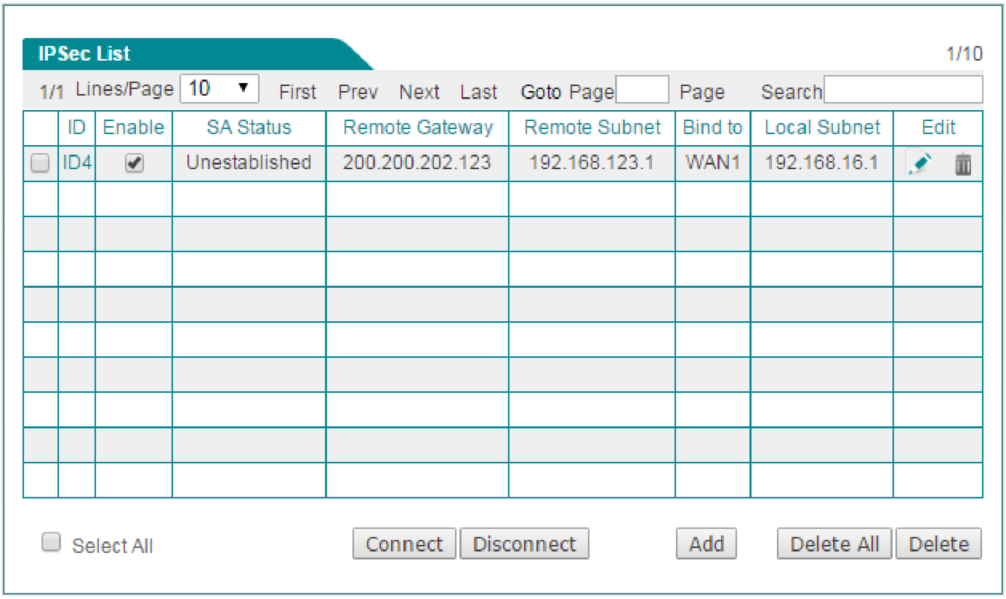
□ Select All   Connect   Disconnect   Add   Delete All   Delete

**Figure 10-47 Responder's IPSec List**

(2) Viewing the Device at the branch office

The following figure shows the configuration and status of the IPSec tunnel on the Device with a dynamic IP address at the branch office.

}



IPSec List
1/10
1/1 Lines/Page 10 ▼ First Prev Next Last Goto Page Page Search

| | ID | Enable | SA Status | Remote Gateway | Remote Subnet | Bind to | Local Subnet | Edit |
|---|---|---|---|---|---|---|---|---|
| □ | ID4 | ☑ | Unestablished | 200.200.202.123 | 192.168.123.1 | WAN1 | 192.168.16.1 | ✎ 🗑 |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

□ Select All
Connect
Disconnect
Add
Delete All
Delete

**Figure 10-48 Initiator's IPSec List**

}

# Chapter 11. System Menu

## 11.1 Administrator

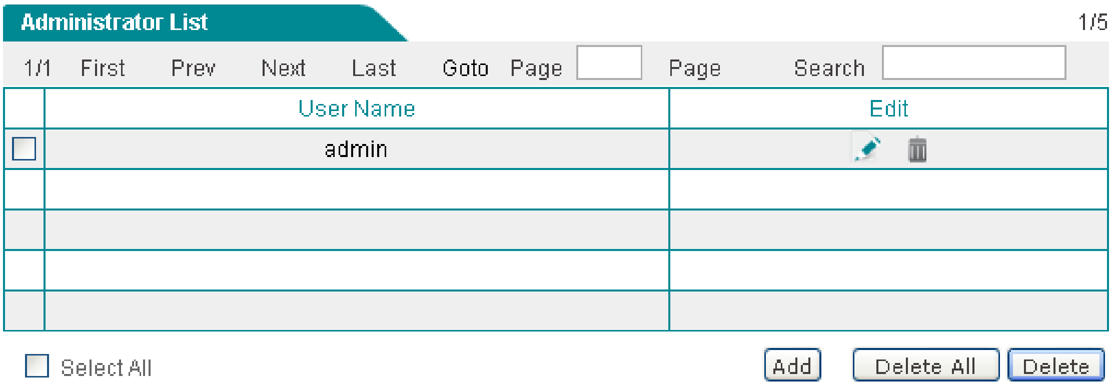
The default administrator’s user name and password are **admin** (case sensitive). To ensure the Device's security, you had better change the default password and remember it. If the password has been changed, you must use the new user name and password to log into the Device.

If you want to change the password, go to **System > Administrator** page, do the following setup:

**Step 1** Click the **Edit** icon with the user name as **admin** to enter into the configuration page.

**Step 2** Modify the factory user name and password.

**Step 3** Click **Save** button to save and apply your settings.

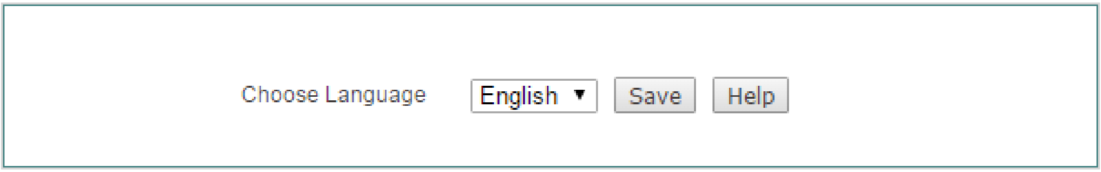


| | User Name | Edit |
|---|---|---|
| □ | admin | ✎ 🗑 |
| | | |
| | | |
| | | |
| | | |

**Figure 11-1 Administrator’s Password Setup**

## 11.2 Language

On the **System** > **Language** page, you can set the system language. Select the language you want to use from the drop-down list and click the **Save** button to save the settings.



Choose Language: English

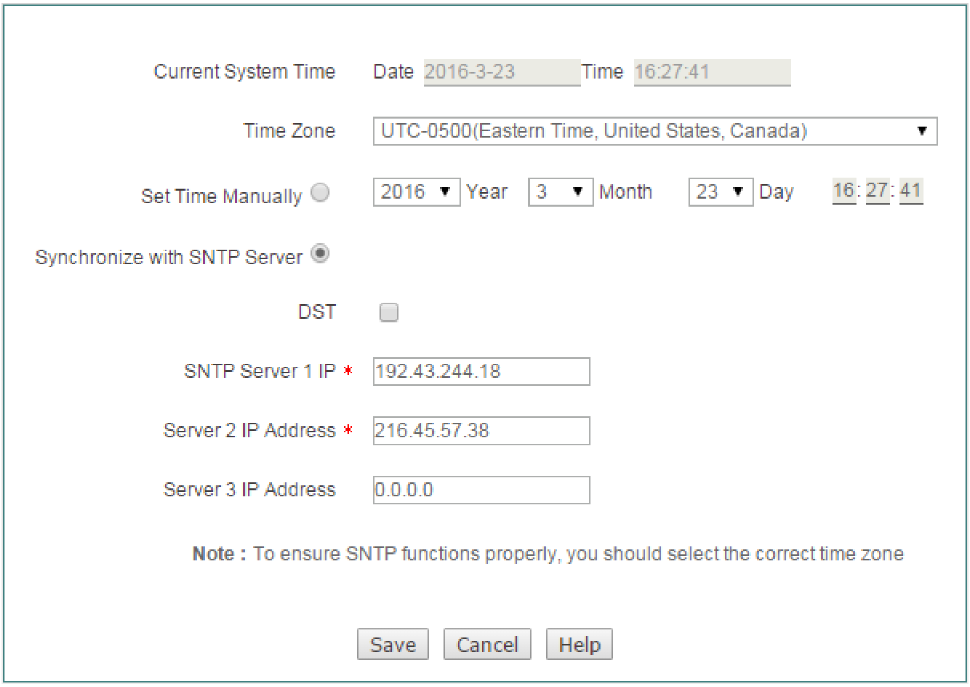
}

**Figure 11-2 Language settings**

## 11.3 Time

In order to guarantee that the functions of the device relating to time work normally, the time of the device needs to be accurately set, to make it synchronize with the local standard time.

The device provides two ways of setting system time, **Setup Time Manually** and **Synchronize with SNTP Server**. It is recommended to use the **Synchronize with SNTP Server** function to obtain the standard time, and the device will automatically get the standard time from the Internet after it connects Internet.



Current System Time Date 2016-3-23 Time 16:27:41

Time Zone UTC-0500(Eastern Time, United States, Canada)

Set Time Manually ○ 2016 Year 3 Month 23 Day 16: 27: 41

Synchronize with SNTP Server ●

DST □

SNTP Server 1 IP * 192.43.244.18

Server 2 IP Address * 216.45.57.38

Server 3 IP Address 0.0.0.0

**Note :** To ensure SNTP functions properly, you should select the correct time zone

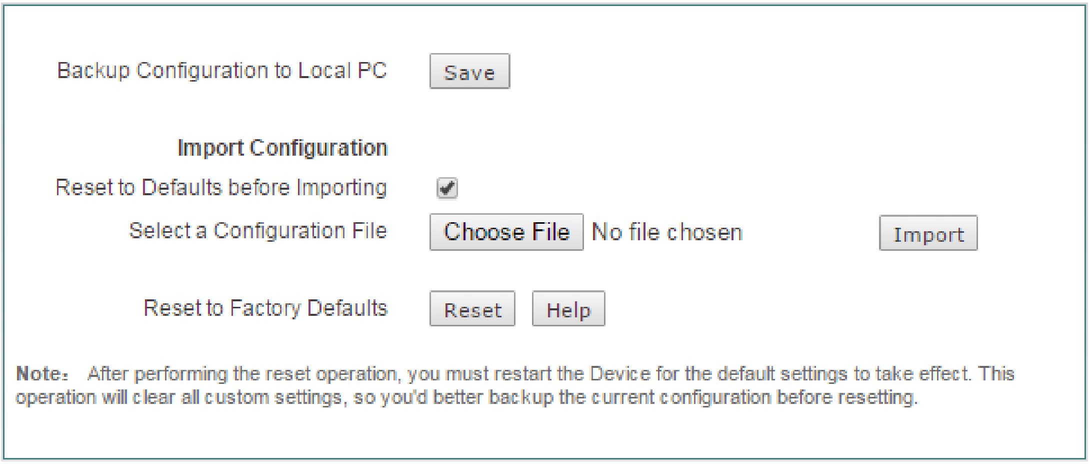
**Figure 11-3 Time Settings**

- **Current System Time**: Displays the current date and time information of the Device (unit: Y-M-D, H:M:S).
- **Time Zone**: Selects the international time zone in which the device resides. Only choosing a correct time zone can the network time synchronization function work properly.
- **Set Time Manually**: Manually enters the current date and time (unit: Y-M-D, H:M:S).
- **Synchronize with SNTP Server:** After using the network time synchronization function to set up the right NTP server, and when the device is connected to the Internet, it will automatically synchronize the time with the set NTP server. The two NTP server addresses preset by the system by default are 192.43.244.18, 216.45.57.38, which generally requires no change. If you need to know more about the NTP knowledge and the server, just visit http://www.ntp.org.

**}**

## 11.4 Configuration

On the **Application > Configuration** page, you can back up the current configuration file to you local PC, import the configuration file to the Device, and reset the Device to factory default settings.



Backup Configuration to Local PC

**Import Configuration**

Reset to Defaults before Importing ☑

Select a Configuration File: No file chosen

Reset to Factory Defaults

**Note:** After performing the reset operation, you must restart the Device for the default settings to take effect. This operation will clear all custom settings, so you'd better backup the current configuration before resetting.

**Figure 11-4 Configuration**

1) Backup Configuration File

In **Application > Configuration** page, click the **Save** button to export and save the Device's current configuration to an XML file on your local computer.

2) Import Configuration File

To restore a previously saved configuration file on your local PC, click **Choose File** to locate and select the configuration file, and then click **Import** to import the configuration file. If you select the **Reset to Defaults before Importing** check box, it will reset the Device to factory default settings before importing the configuration file.

3) Reset to Factory Defaults

To reset the Device to factory default settings, click the **Reset** button. The Device will restart automatically.

**Note:**

1) To avoid any unexpected error, do not power off the Device during importing the configuration file.

2) The reset operation will clear all custom settings on the Device. It is strongly recommended that you backup the current configuration resetting the Device.

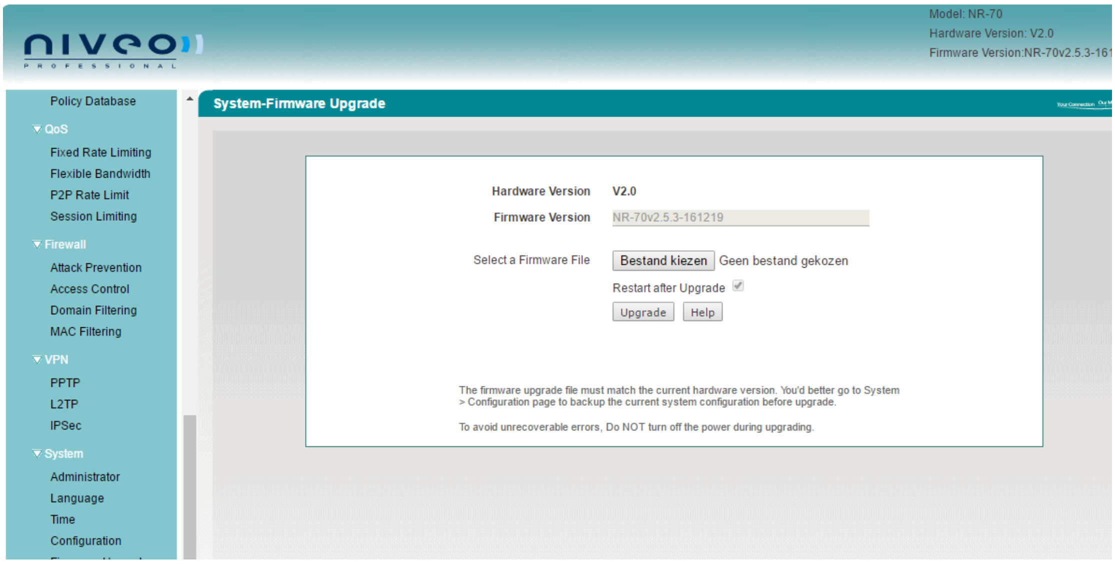
}

3) The default administrator user name and password both are admin (case sensitive). The default LAN IP address is 192.168.1.253 with a subnet mask of 255.255.255.0.

4) After the reset operation is complete, you must restart the Device for the default settings to take effect.

## 11.5 Firmware Upgrade

On the **Application > Firmware** page, you can view the current firmware version information, download the latest firmware from the Niveo Professional website, and upgrade the firmware.



Model: NR-70
Hardware Version: V2.0
Firmware Version:NR-70v2.5.3-161

System-Firmware Upgrade

Hardware Version V2.0
Firmware Version NR-70v2.5.3-161219
Select a Firmware File Geen bestand gekozen
Restart after Upgrade ☑

The firmware upgrade file must match the current hardware version. You'd better go to System > Configuration page to backup the current system configuration before upgrade.

To avoid unrecoverable errors, Do NOT turn off the power during upgrading.

**Figure 11-5 Firmware Upgrade**

- **Firmware Version:** Shows the current firmware version of the Device.
- **Hardware Version:** Shows the current hardware version of the Device.

To upgrade the Device's firmware, follow these steps:

1) Download the firmware

2) Choose the firmware

Click the **Choose File** button to locate and select the firmware you want to upgrade.

3) Upgrade the firmware

Click the **Upgrade** button. In the pop-up window appears, click **OK** to start the

}

upgrade.

⌖ **Note:**

1) As new versions of the Device's firmware become available, you can upgrade the firmware on your Device to take advantage of new features and improved performance.

2) Please download the firmware that matches the model and hardware version of your Device.

3) It is recommended that you go to **Application** > **Configuration** page to backup the Device's current configuration before upgrade. Normally, the upgrade does not affect the current configuration of the Device. However, this situation might happen if the right steps are not followed properly.

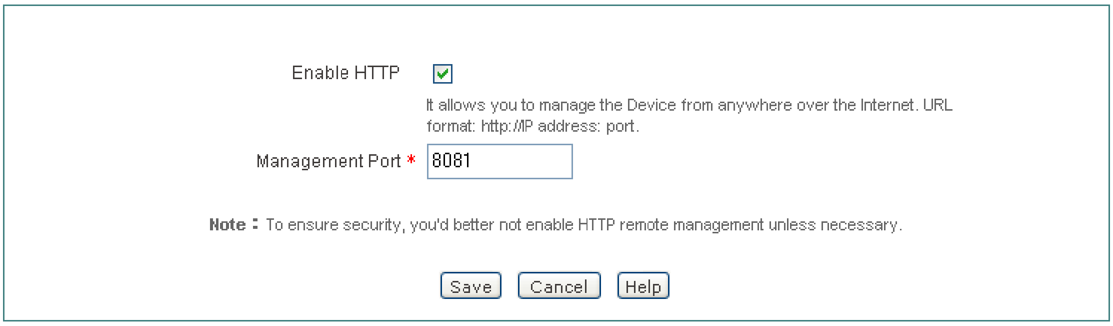
4) It is strongly recommended that you upgrade the firmware when the Device is under light load.

5) During the firmware upgrade, DO NOT power off the Device, press the Reset button, shut down the PC, or interrupt the process in any way until the operation is complete. Doing so may cause unexpected error or even irreparable hardware damage.

6) After the upgrade is complete, the Device will automatically restart for the new firmware to take effect, without human intervention.

## 11.6 Remote Management

If you want to allow HTTP remote management, go to **System > Remote Management** page to setup.



Enable HTTP ☑

It allows you to manage the Device from anywhere over the Internet. URL format: http://IP address: port.

Management Port * 8081

**Note :** To ensure security, you'd better not enable HTTP remote management unless necessary.

**Figure 11-6 Remote Management**

◆ **Enable HTTP:** Select this check box to allow HTTP remote management. When accessing the Device from Internet, you will enter **http://** and enter the Device's WAN IP address, followed by a colon (:) and the port number. For example, if WAN IP address is 218.21.31.3 and the port number is 8081, enter in your browser: **http://218.21.31.3:8081**.

}

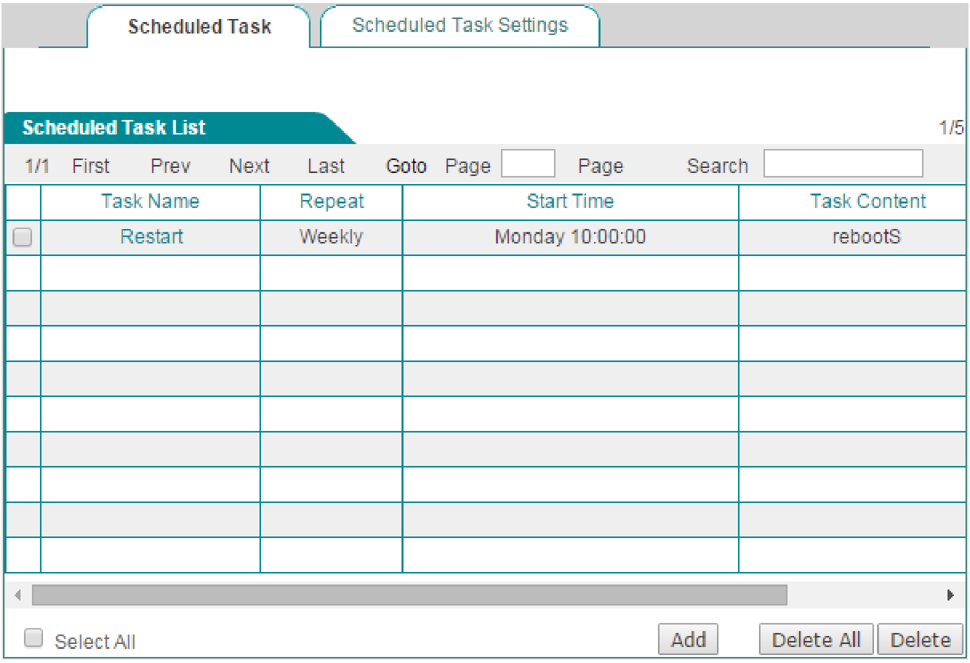
- **Management Port:** Enter the port number for HTTP remote management. The default value is 8081.

**Note:**

To ensure security, it is strongly recommended that you don’t enable remote management functions unless necessary. If you are sure to enable them, you had better change the default password.

## 11.7 Scheduled Task

This section describes **System** > **Scheduled Task** page. By configuring scheduled tasks, administrators can predefine the actions completed by the device at a specified time. The following figure displays the scheduled task you have set.

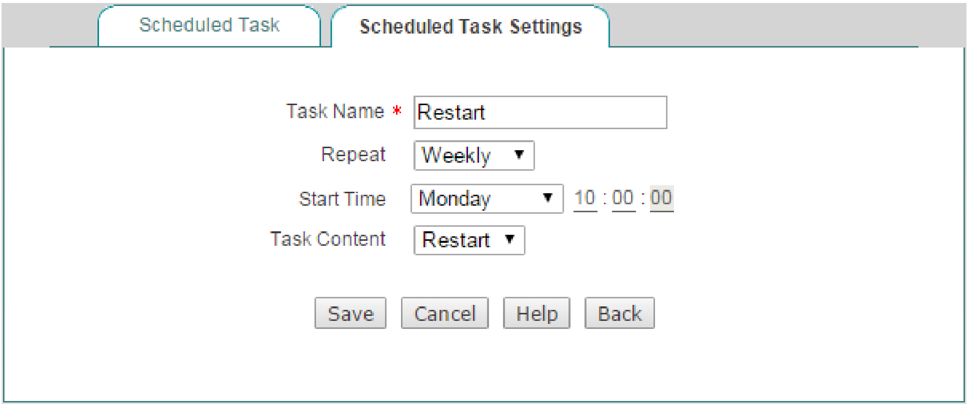


| | Task Name | Repeat | Start Time | Task Content |
|---|---|---|---|---|
| □ | Restart | Weekly | Monday 10:00:00 | rebootS |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Figure 11-7 Scheduled Task List**

You can click the Task Name hyperlink or the Edit hyperlink to change the content of task. Clicking **System** > **Scheduled Task** > **Scheduled Task Settings**, you can add a new scheduled task.

}



Task Name * Restart

Repeat Weekly ▼

Start Time Monday ▼ 10 : 00 : 00

Task Content Restart ▼

**Figure 11-8 Scheduled Task Settings**

- **Task Name**: Name of the custom tasks.
- **Repeat**: Specify the time cycle or when the Device will perform the task. The available options are **Weekly**, **Daily**, **Hourly**, **Minutely**.
- **Start time**: Specify the time at which the Device will start to perform the task. Its settings will change according to the value of **Repeat**.
- **Task Content:** Selects the appropriate task content.

}

# Chapter 12. Status Menu

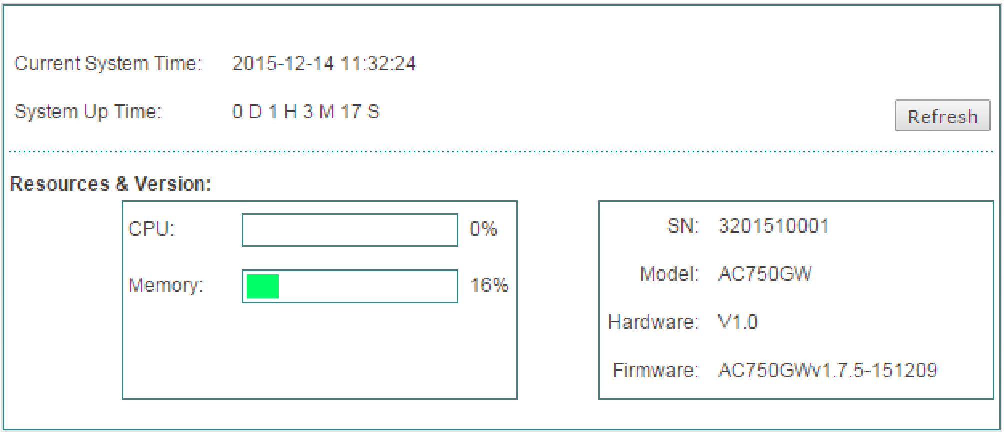
In **Status** menu, you can easily view the running state and the system information of the device.

## 12.1 Interface Status

The Interface Status page described in this section is the same as the description of **Start > Interface Status** page, please refer to the section: Interface Status.

## 12.2 System Information

In the **System > System Information** page, administrators can view system information, such as current system time, system up time, system resources usage information, SN, firmware version, etc. Through system information, administrator can identify and diagnose the source of network problems or potential problems, which helps improve the network performance and enhance network security.



Current System Time: 2015-12-14 11:32:24

System Up Time: 0 D 1 H 3 M 17 S

Resources & Version:

CPU: 0%

Memory: 16%

SN: 3201510001

Model: AC750GW

Hardware: V1.0

Firmware: AC750GWv1.7.5-151209

**Figure 12-1 System Information**

- **Current System Time**: Displays the current date and time information of the Device (Unit: Y-M-D, H:M:S).

- **System Up Time**: Displays the elapsed time (in days, hours, minutes and seconds) since the Device was last started.

- **CPU**: Displays the percentage of the current CPU utilization.

- **Memory**: Displays the percentage of the current memory usage.

}

- **SN**: Displays the internal serial number of product (which may be different from the surface serial number).

- **Model**: Displays the product model of the device.

- **Hardware**: Displays the hardware version number of the device. When the device hardware version is V1.0.

- **Firmware**: Displays the software version number of the device.

**Notes:**

1) The **CPU usage** and **Memory usage** are displayed as a status bar and percentage value. The color of the status bar indicates the usage percentage for each resource.

   - When the percentage is below 1%, the bar is blank.

   - When the percentage is between 1% and 50% (below 50%), the color is green.

   - When the percentage is between 50% and 70% (below 70%), the color is yellow.

   - When the percentage is equal to or above 70%, the color is red.

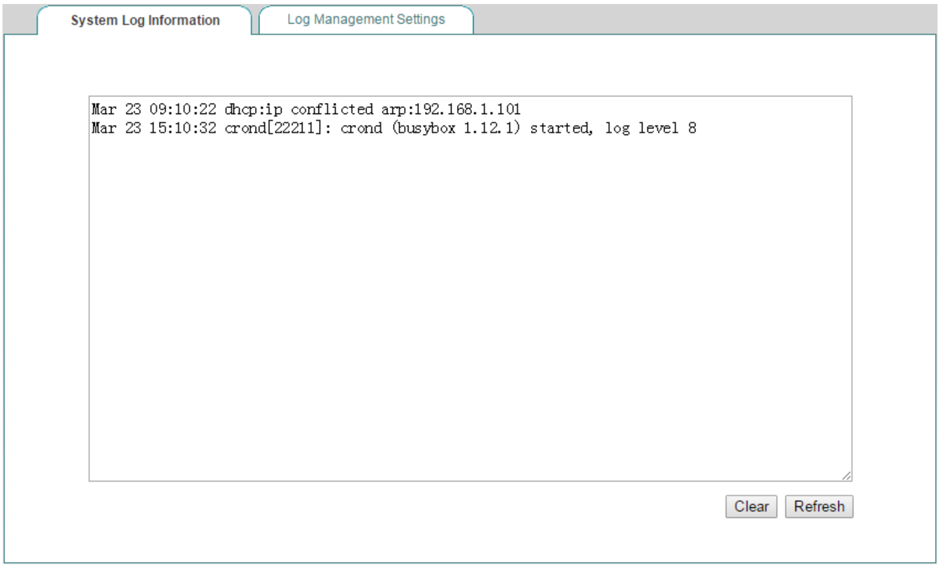
2) The above resources usage information indicates the load of the Device. If the usage percentages are all relatively low, it means that the Device still has the ability to process more tasks. If they are all very high, it means that the Device is nearly under the full load. In this case, the network delays may occur if the Device processes new tasks.

## 12.3 System Log

In the **Status > System Log** page, you can view the system logs; also you can select the types of logs that you want the Device to store and display.

If you have enabled one or more system log features in the **Status > System Log > Log Management Settings** page, you can view the related logs in the **Status > System Log > The System Log Information** page, see the following figure.

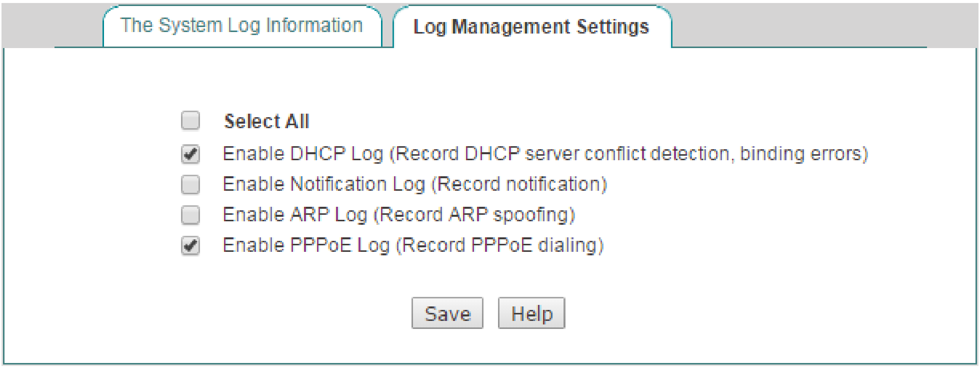
}



```
Mar 23 09:10:22 dhcp:ip conflicted arp:192.168.1.101
Mar 23 15:10:32 crond[22211]: crond (busybox 1.12.1) started, log level 8
```

**Figure 12-2 System Logs**

On the **Status > System Log > Log Management Settings** page, you can set the type of system log you want to display.



□ Select All
☑ Enable DHCP Log (Record DHCP server conflict detection, binding errors)
□ Enable Notification Log (Record notification)
□ Enable ARP Log (Record ARP spoofing)
☑ Enable PPPoE Log (Record PPPoE dialing)

**Figure 12-3 System Log Settings**

- **Select All:** If selected, all the provided system log features will be enabled.

- **Enable DHCP Log:** If selected, the Device will store and display the DHCP related logs in the System Log.

- **Enable Notification Log:** If selected, the Device will store and display the notice related logs in the System Log.

- **Enable ARP Log:** If selected, the Device will store and display the ARP related logs in the System Log.

- **Enable PPPoE Log:** If selected, the Device will store and display the ARP related logs in the System Log.

}

# Appendix A FAQ

**Question 1: How to configure TCP/IP?**

There are two methods of configuring TCP/IP properties: one is to manually configure TCP/IP properties; the other is automatically configuring TCP/IP properties with DHCP. The following describes the configuration procedure of these two methods respectively.

- Method I: Manually Configuring TCP/IP

To configure the TCP/IP protocol manually, do the following:

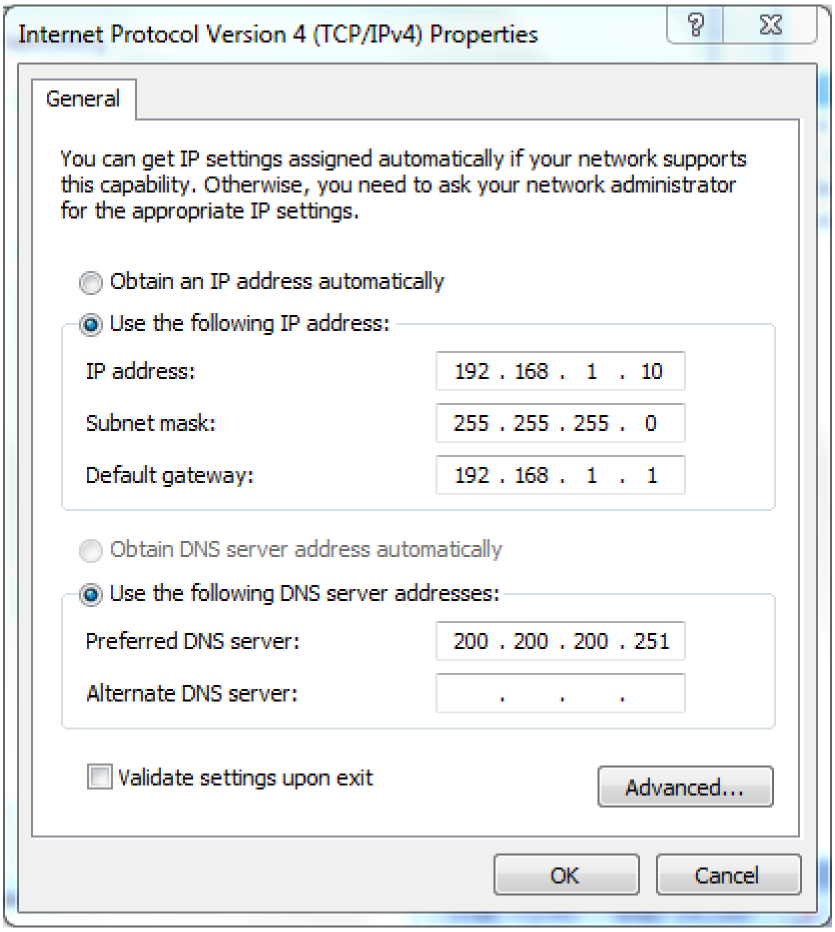
**Step 1** On the Windows taskbar, click **Start > Control Panel > Network and Connection > Local Area Connection**, right click **Local Area Connection**, and choose **Properties**.

**Step 2** In the **Properties** dialogue, double click **Internet Protocol Version 4 (TCP/IPv4)**.

**Step 3** In the **Internet Protocol Version 4 (TCP/IPv4)** dialogue, select the **Use the following IP address** radio button, Enter 192.168.1.x (x is between 2 and 254, including 2 and 254) in the **IP Address** box, enter 255.255.255.0 in the **Subnet Mask** box, and Enter the IP address of the Device’s LAN interface (default value is 192.168.1.1) in the **Default gateway** textbox.

**Step 4** Select the **Use the following DNS server addresses** radio button, Enter the IP address of DNS server into the **Preferred DNS server** textbox.

}



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 200 . 200 . 200 . 251

Alternate DNS server: . . .

□ Validate settings upon exit

**Figure Appendix- 1 Manually configuring TCP/IP**

**Step 5** Click **OK** in the **Internet Protocol Version 4 (TCP/IPv4)** dialogue, this will return you to the **Local Area Connection Properties** dialogue. Click **OK** again. Till now you have finished configuring the TCP/IP properties.

- Method II: Automatically Configuring TCP/IP with DHCP

To ensure that the host can obtain an IP address and other TCP/IP parameters automatically from the Device, you should enable the Device's DHCP server function in **Application > DHCP Server** page.

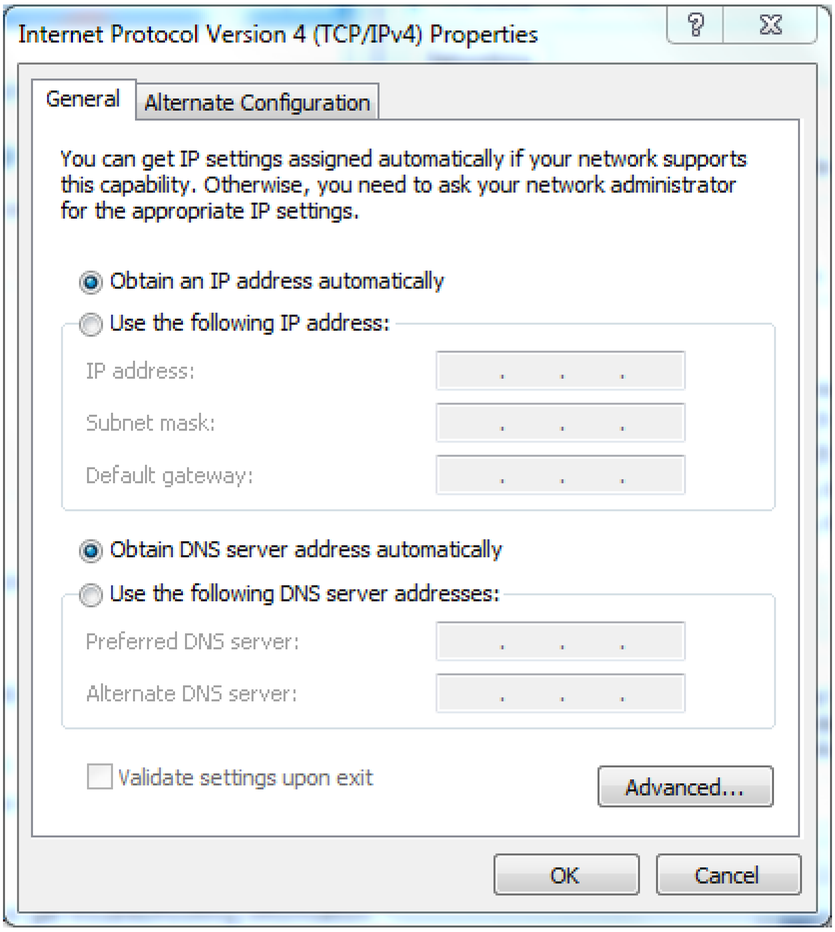
**Step 1** On the Windows taskbar, click **Start > Control Panel > Network and Connection > Local Area Connection**, right click **Local Area Connection**, and choose **Properties**.

**Step 2** In the **Properties** dialogue, double click **Internet Protocol Version 4 (TCP/IPv4)**.

**Step 3** In the **Internet Protocol Version 4 (TCP/IPv4)** dialogue, select the **Obtain an IP address automatically** radio button, and select the **Obtain DNS**

}

**server address automatically** radio button.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Figure Appendix- 2 Automatically Configuring TCP/IP with DHCP

**Step 4** Click **OK** in the **Internet Protocol Version 4 (TCP/IPv4)** dialogue, this will return you to the **Local Area Connection Properties** dialogue. Click **OK** again. Till now you have finished configuring the TCP/IP properties.

**Question 2: How to reset the Device to factory default settings?**

Case I: Know the administrator password

Under normal circumstances, you can directly go to the **System** > **Configuration** page, click **Reset** button, and restart the Device after the reset operation is complete.

Case II: Forget the administrator password

If you forget the administrator password, you can use a pin to press and hold the **Reset** button for more than 5 seconds when the device is on, and then release the button. After that, the Device will restart with factory default settings.

**}**

⌖ **Notes:** The reset operation will clear all custom settings on the Device, so do it with caution.

⌖ **Notes:** The reset operation will clear all custom settings on the Device, so do it with caution.

}

# Appendix B Common IP Protocols

| Protocol Name | Protocol Number | Full Name |
|---|---|---|
| IP | 0 | Internet Protocol |
| ICMP | 1 | Internet Protocol Message Protocol |
| IGMP | 2 | Internet Group Management |
| GGP | 3 | Gateway-Gateway Protocol |
| IPINIP | 4 | IP in IP Tunnel Driver |
| TCP | 6 | Transmission Control Protocol |
| EGP | 8 | Exterior Gateway Protocol |
| IGP | 9 | Interior Gateway Protocol |
| PUP | 12 | PARC Universal Packet Protocol |
| UDP | 17 | User Datagram Protocol |
| HMP | 20 | Host Monitoring Protocol |
| XNS-IDP | 22 | Xerox NS IDP |
| RDP | 27 | Reliable Datagram Protocol |
| GRE | 47 | General Routing Encapsulation |
| ESP | 50 | Encap Security Payload |
| AH | 51 | Authentication Header |
| RVD | 66 | MIT Remote Virtual Disk |
| EIGRP | 88 | Enhanced Interior Gateway Routing Protocol |
| OSPF | 89 | Open Shortest Path First |

# Appendix C Common Service Ports

| Service Name | Port | Protocol | Description |
|---|---|---|---|
| echo | 7 | tcp | |
| echo | 7 | udp | |
| discard | 9 | tcp | |
| discard | 9 | udp | |
| systat | 11 | tcp | Active users |
| systat | 11 | udp | Active users |
| daytime | 13 | tcp | |
| daytime | 13 | udp | |
| qotd | 17 | tcp | Quote of the day |
| qotd | 17 | udp | Quote of the day |
| chargen | 19 | tcp | Character generator |
| chargen | 19 | udp | Character generator |
| ftp-data | 20 | tcp | FTP, data |
| ftp | 21 | tcp | FTP. control |
| telnet | 23 | tcp | |
| smtp | 25 | tcp | Simple Mail Transfer Protocol |
| time | 37 | tcp | timserver |
| time | 37 | udp | timserver |
| rlp | 39 | udp | Resource Location Protocol |
| nameserver | 42 | tcp | Host Name Server |
| nameserver | 42 | udp | Host Name Server |
| nicname | 43 | tcp | whois |
| domain | 53 | tcp | Domain Name Server |
| domain | 53 | udp | Domain Name Server |
| bootps | 67 | udp | Bootstrap Protocol Server |

| | | | |
|---|---|---|---|
| bootpc | 68 | udp | Bootstrap Protocol Client |
| tftp | 69 | udp | Trivial File Transfer |
| gopher | 70 | tcp | |
| finger | 79 | tcp | |
| http | 80 | tcp | World Wide Web |
| kerberos | 88 | tcp | Kerberos |
| kerberos | 88 | udp | Kerberos |
| hostname | 101 | tcp | NIC Host Name Server |
| iso-tsap | 102 | tcp | ISO-TSAP Class 0 |
| rtelnet | 107 | tcp | Remote Telnet Service |
| pop2 | 109 | tcp | Post Office Protocol - Version 2 |
| pop3 | 110 | tcp | Post Office Protocol - Version 3 |
| sunrpc | 111 | tcp | SUN Remote Procedure Call |
| sunrpc | 111 | udp | SUN Remote Procedure Call |
| auth | 113 | tcp | Identification Protocol |
| uucp-path | 117 | tcp | |
| nntp | 119 | tcp | Network News Transfer Protocol |
| ntp | 123 | udp | Network Time Protocol |
| epmap | 135 | tcp | DCE endpoint resolution |
| epmap | 135 | udp | DCE endpoint resolution |
| netbios-ns | 137 | tcp | NETBIOS Name Service |
| netbios-ns | 137 | udp | NETBIOS Name Service |
| netbios-dgm | 138 | udp | NETBIOS Datagram Service |
| netbios-ssn | 139 | tcp | NETBIOS Session Service |
| imap | 143 | tcp | Internet Message Access Protocol |
| pcmail-srv | 158 | tcp | PCMail Server |
| snmp | 161 | udp | |
| snmptrap | 162 | udp | SNMP trap |
| print-srv | 170 | tcp | Network PostScript |
| bgp | 179 | tcp | Border Gateway Protocol |

| | | | |
|---|---|---|---|
| irc | 194 | tcp | Internet Relay Chat Protocol |
| ipx | 213 | udp | IPX over IP |
| ldap | 389 | tcp | Lightweight Directory Access Protocol |
| https | 443 | tcp | MCom |
| https | 443 | udp | MCom |
| microsoft-ds | 445 | tcp | |
| microsoft-ds | 445 | udp | |
| kpasswd | 464 | tcp | Kerberos (v5) |
| kpasswd | 464 | udp | Kerberos (v5) |
| isakmp | 500 | udp | Internet Key Exchange |
| exec | 512 | tcp | Remote Process Execution |
| biff | 512 | udp | |
| login | 513 | tcp | Remote Login |
| who | 513 | udp | |
| cmd | 514 | tcp | |
| syslog | 514 | udp | |
| printer | 515 | tcp | |
| talk | 517 | udp | |
| ntalk | 518 | udp | |
| efs | 520 | tcp | Extended File Name Server |
| router | 520 | udp | route routed |
| timed | 525 | udp | |
| tempo | 526 | tcp | |
| courier | 530 | tcp | |
| conference | 531 | tcp | |
| netnews | 532 | tcp | |
| netwall | 533 | udp | For emergency broadcasts |
| uucp | 540 | tcp | |
| klogin | 543 | tcp | Kerberos login |
| kshell | 544 | tcp | Kerberos remote shell |

|  |  |  |  |
|---|---|---|---|
| new-rwho | 550 | udp |  |
| remotefs | 556 | tcp |  |
| rmonitor | 560 | udp |  |
| monitor | 561 | udp |  |
| ldaps | 636 | tcp | LDAP over TLS/SSL |
| doom | 666 | tcp | Doom Id Software |
| doom | 666 | udp | Doom Id Software |
| kerberos-adm | 749 | tcp | Kerberos administration |
| kerberos-adm | 749 | udp | Kerberos administration |
| kerberos-iv | 750 | udp | Kerberos version IV |
| kpop | 1109 | tcp | Kerberos POP |
| phone | 1167 | udp | Conference calling |
| ms-sql-s | 1433 | tcp | Microsoft-SQL-Server |
| ms-sql-s | 1433 | udp | Microsoft-SQL-Server |
| ms-sql-m | 1434 | tcp | Microsoft-SQL-Monitor |
| ms-sql-m | 1434 | udp | Microsoft-SQL-Monitor |
| wins | 1512 | tcp | Microsoft Windows Internet Name Service |
| wins | 1512 | udp | Microsoft Windows Internet Name Service |
| ingreslock | 1524 | tcp |  |
| l2tp | 1701 | udp | Layer Two Tunneling Protocol |
| pptp | 1723 | tcp | Point-to-point tunnelling protocol |
| radius | 1812 | udp | RADIUS authentication protocol |
| radacct | 1813 | udp | RADIUS accounting protocol |
| nfsd | 2049 | udp | NFS server |
| knetd | 2053 | tcp | Kerberos de-multiplexor |
| man | 9535 | tcp | Remote Man Server |