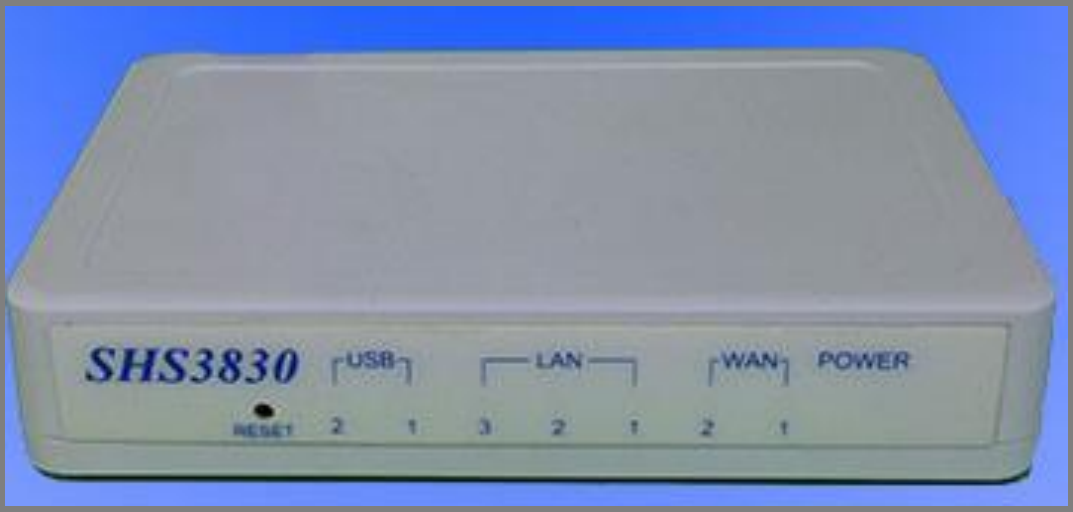
2014

SHS 3830

User Manual

SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features.



Avadesign Technology Co. Ltd
www.avadesign.com.tw
2014/11/25

WELCOME

Congratulations on purchasing the SHS 3830. The SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features. The SIP-based IP-PBX can create telephony systems for home and small-to-medium enterprises.

Manual version V1.00 25-11-2014

Avadesign Technology Co. Ltd

4F.-10, No.351, Sec. 2, Zhongshan Rd., Zhonghe Dist., New Taipei City 23504, Taiwan R.O.C.

www.avadesign.com.tw

Table of Contents

Chapter 1 Introduction

SHS 3830 is an embedded server that provides IP-PBX functions and two WAN ports Router features. The Firewall and QoS improves VoIP network voice quality.

The IP-PBX module of SHS 3830 is a SIP-based IP-PBX that can create telephony systems for home and small-to-medium enterprises. It is also designed to operate on a variety of VoIP applications, such as auto-attendant, call transfer, and IP-based communications. Since it supports industry-standard SIP, it works with all SIP-supported products and devices available today. The key features of SHS 3830 are quiet, power saving, stability and small volume box.

1.1 SHS-3830 Specification

1.1.1 SIP IP-PBX Function

- RFC3261 compliance
- SIP UDP/TCP Protocol
- MD5 Digest Authentication (RFC2069/RFC2617)
- Allow FXO/FXS gateway, IP Phone and the DP-104 SIP IP video door phone to register.
- Support 50 registered extensions
- Easy install APP on smart phone to become SIP IP-PBX client extension
- Support SIP Trunk
- Support Audio Codec G.711 A-law/μ-law
- Support pass through Video Call
- Out Band DTMF (RFC4733, RFC2833 / SIP INFO)
- Adaptive Jitter Buffer
- Automatic voice attendant
- Record your own greeting voice messages via voice file up-load from Web
- NAT Traversal configurable
- Blind Transfer
- Configurable Call and Pickup group
- Block Anonymous Call
- Call Hold
- Call Transfer
- Call Park
- Call Queuing
- Call Routing (DID & ANI) (in dial-plan function)
- Caller ID
- Route by Caller ID (in dial-plan function)
- Music On Hold
- Music On Transfer

- Time and Date
- Flexible Dial Plan
- Support Multi call rule to configure
- Outgoing Routing Rule (Drop, Replace, Add) and Routes selection
- Incoming Routing Rule (Drop, Replace, Add)
- Dial Group Setting
- Call Group, Pick up group setting
- Configure maximum concurrent SIP calls
- RTP Routed or Direct mode selection
- SIP Trunk setting
- Cellular Phone resonance setting
- Video preview setting
- Flexible Routing Plan
- Voice broadcasting over IP Phone with separated group
- Provide CDR log file

1.1.2 IP Network connection

- IPv4 (RFC 791) for WAN and LAN ports
- IP/ICMP/ARP/RARP/SNTP
- NTP Server and Time Zone setting
- WAN: DHCP, Fixed, PPPoE, DDNS
- LAN : Static Private IP or DHCP Server
- NAT allows users to surf internet by means of a single broadband user account
- Multiple DMZ Host (PPPoE, static IP)
- Multiple Virtual Server
- Multiple NAT function
- Protocol Route Control (IP Binding Function, by IP & port number)
- Protocol Bandwidth Control (by application protocol port number)
- IP/URL Blocking
- User Bandwidth control Function (by user IP address)
- Outgoing wan link selected (by user IP address)
- Remote Configuration through Internet
- Mail Alert: H32 WAN up
  WAN down
  System Log
- System Log: local event logging – log send to remote server
- Firewall
- Backup / Restore Router configuration file from PC
- Outbound Load Balance: provide 2 working mode: (1) session (2) weight round robin
- Inbound Load Balance: provide 2 working mode: (1) session (2) weight round

robin

- TCP/UDP (RFC 793/768)
- RTP/RTCP (RFC 1889/1890)

1.1.3 Management

- Administrative HTTP and port number configuration
- Subscriber information display
- HTTP port and user ID, Password control
- Firmware and Library upload
- Configuration Backup/Restore
- Reset to Factory default setting
- Soft-Reset or Reboot System
- Status display: Network, Line, SIP Trunk status

1.1.4 Environmental

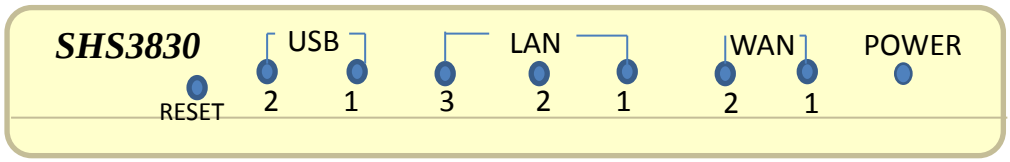
- Dimensions**:** 155(W) x 106(H) x 29(D) mm
- Weight: 300g
- Power Adaptor: INPUT: AC100V~240V, 50/60Hz 0.8A
  OUTPUT: DC 12V, 2.0A

1.1.5 Approvals

- CE
- FCC
- RoHS

1.2 Hardware Overview

1.2.1 Front Panel and LED Indicator



RESET: If SHS 3830 encounters any system crash, you may press this button to reload factory default value as press the button over 3 seconds or reset back to latest configuration file while pushing the button.

USB: SHS 3830 provides two USB 2.0 ports. Light on when SHS 3830 detects USB device and active.

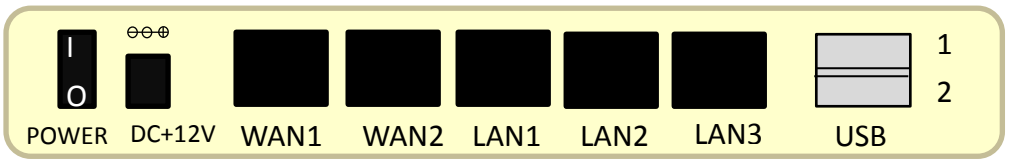
LAN: SHS 3830 provides three RJ45 type LAN ports connecting to your computer or network device such as Hub/Switch via RJ45 cable. Light on means link 100 Mbps. Flash when data is transmitting or receiving with 100 Mbps. Light off means

disconnected or undetected.

WAN: SHS 3830 provides two RJ45 type WAN ports connecting to broadband transmission equipment such as ADSL or Fiber or CABLE Modem via RJ45 cable. Light on means link 100 Mbps. Flash when data is transmitting or receiving with 100 Mbps. Light off means disconnected or undetected.

POWER: Light on when SHS3830 is powered by on.

1.2.2 Back Panel



POWER: A switch for power on or off

DC 12V/2A: Connecting to AC adapter. Input AC 100V~240V, 50/60Hz 0.8A; Output DC12V 2.0A

LAN/WAN: RJ-45 socket, complied with Ethernet 10/100base-T.

USB: USB 2.0 ports, USB Type A.

Chapter 2 Start to configure SHS3830

2.1 Unpacking

Unpack the items. Your package should include:

- One SHS 3830
- One external power adaptor INPUT: AC100V~240V, 50/60Hz 0.8A
  OUTPUT: DC 12V, 2.0A

If items are missing or damaged, notify your Avadesign representative. Keep the carton and packing material.

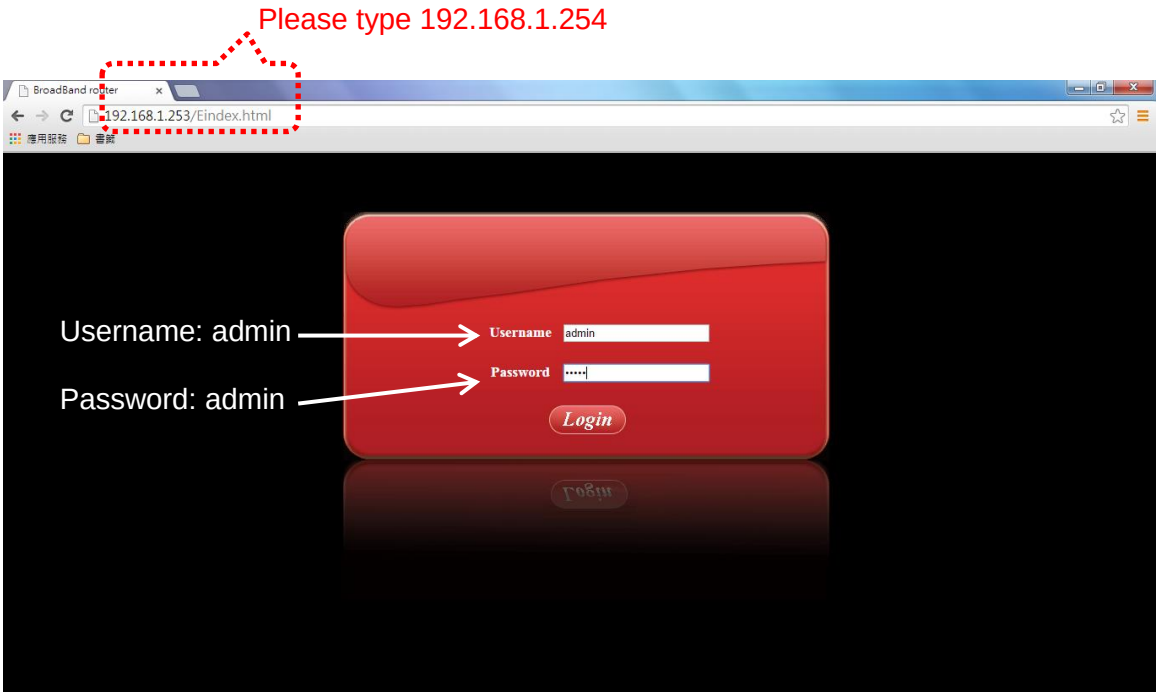
2.2 Plug in DC power adapter to SHS 3830

2.3 Connect to LAN Port

LAN port of SHS3830 connects to user's computer or Hub/Switch port via RJ45 cable. Then plug in AC power cord to power source and switch on the SHS 3830.

2.4 Open Web Browser

Type the default IP address **http://192.168.1.254** in the address bar of the Chrome browser to open web configuration. The screen shows as below:



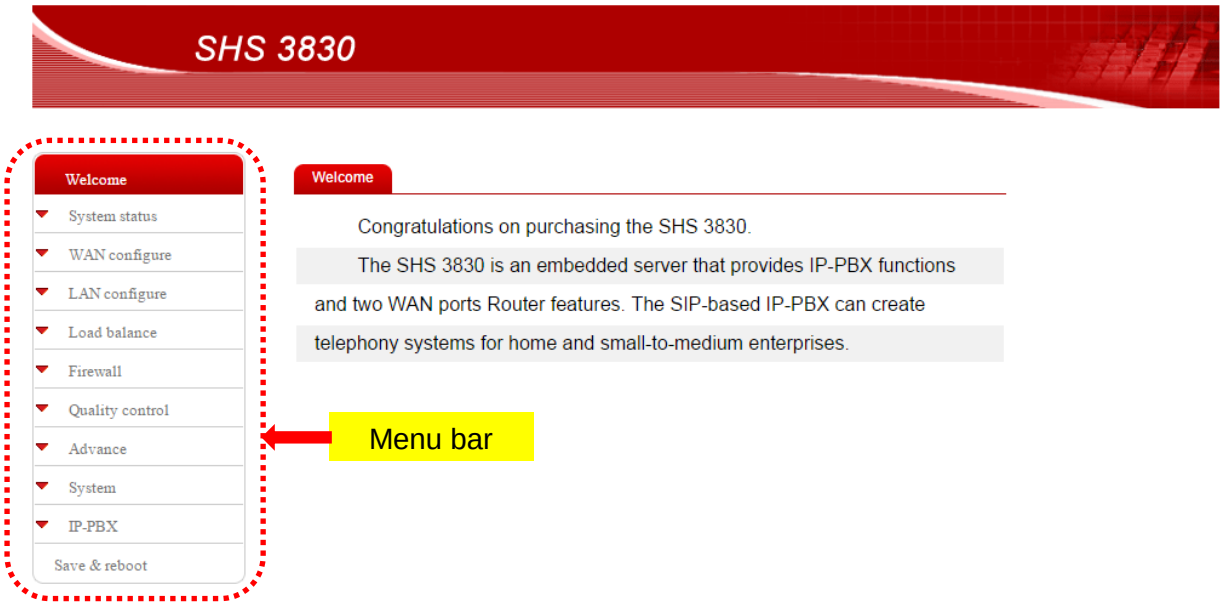
Please input with username: admin and password: admin then click "Login" button on the screen. After login SHS3830, user can start to do basic and advance configurations.

After Login SHS 3830 user will see screen as below, and there are ten main categories, user can click on each category to extend detail items.

- Welcome
- System Status
- WAN configure
- LAN configure
- Load balance
- Firewall
- Quality control
- Advance
- System
- IP-PBX
- Save & reboot

The various configuration menus are explained below. You can select various function listed in the left side of Welcome page display.

Welcome Home Page



2.5 Basic and Advance Configurations for IP-PBX

To make SHS 3830 work smoothly you have to set up some basic and advance configurations that include router and IP-PBX features.

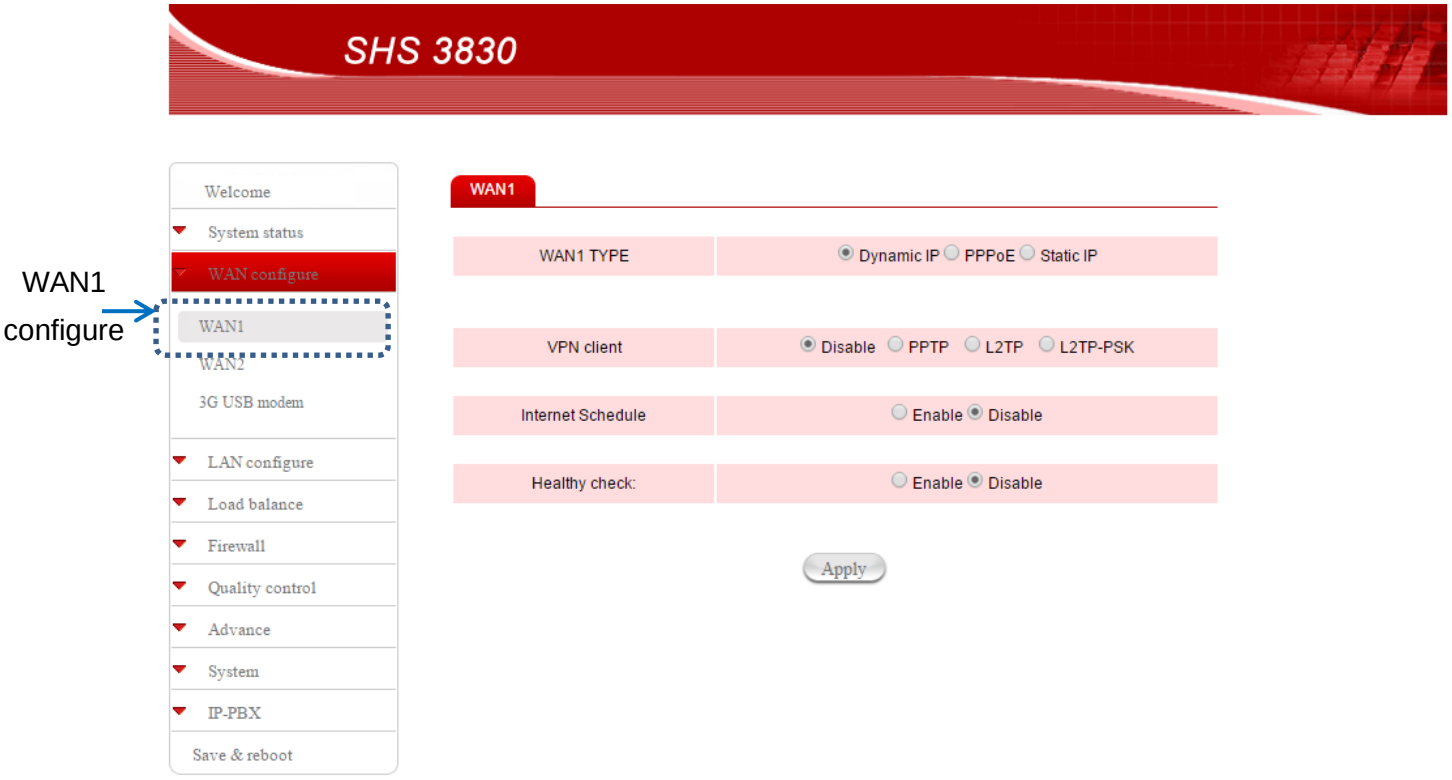
The first, you have to configure WAN and LAN IP for network enable.

2.5.1 WAN configuration

There are two WAN ports for the SHS 3830. You can select “WAN configure” in the menu bar on the left side of screen to configure WAN1/WAN2 as shown below.

There are several WAN functions can be made in this display, you can configure functions to each WAN port separately.

WAN Configure – WAN1 – Dynamic IP



WAN1/WAN2 TYPE

Three kinds of WAN types to let you select for each WAN port:

1. Dynamic IP - connect to Cable Modem.

   Obtain an IP address from ISP automatically. Usually it's used to connect CABLE modem. You won't need to assign an IP address. The SHS 3830 will get the IP address for user automatically.

2. PPPoE - connect to Dial Up DSL

   Some ISPs require use of PPPoE to connect to their service. Connect to ISP via dial-up connecting, ISP will assign a legal IP to you after the user ID and password had been passed when the connection is made (The user ID and password here are provided by your ISP.)

3. Static IP - Connect to Leased DSL

   ISP assigns you a static IP address. When used the leased line of ADSL. ISP will provide you the relative IP, Subnet Mask, Gateway and DNS. You need to indicate the static IP manually.

VPN Client

User can select either Disable or PPTP or L2TP or L2TP over IPSec. With PPTP/L2TP/L2TP-PSK dial up features to help construct a complete Client/Server topology for need of enterprise network, it improves security in connecting links in public network.

Internet Schedule

This function allows you to control each WAN port link up/down time by

daily/weekly. Available time: WAN port link up time. For example : The link time is from AM 9:30 – PM 6:30. User can fill 09:30 : 18:30

Select Weekly: choose by day

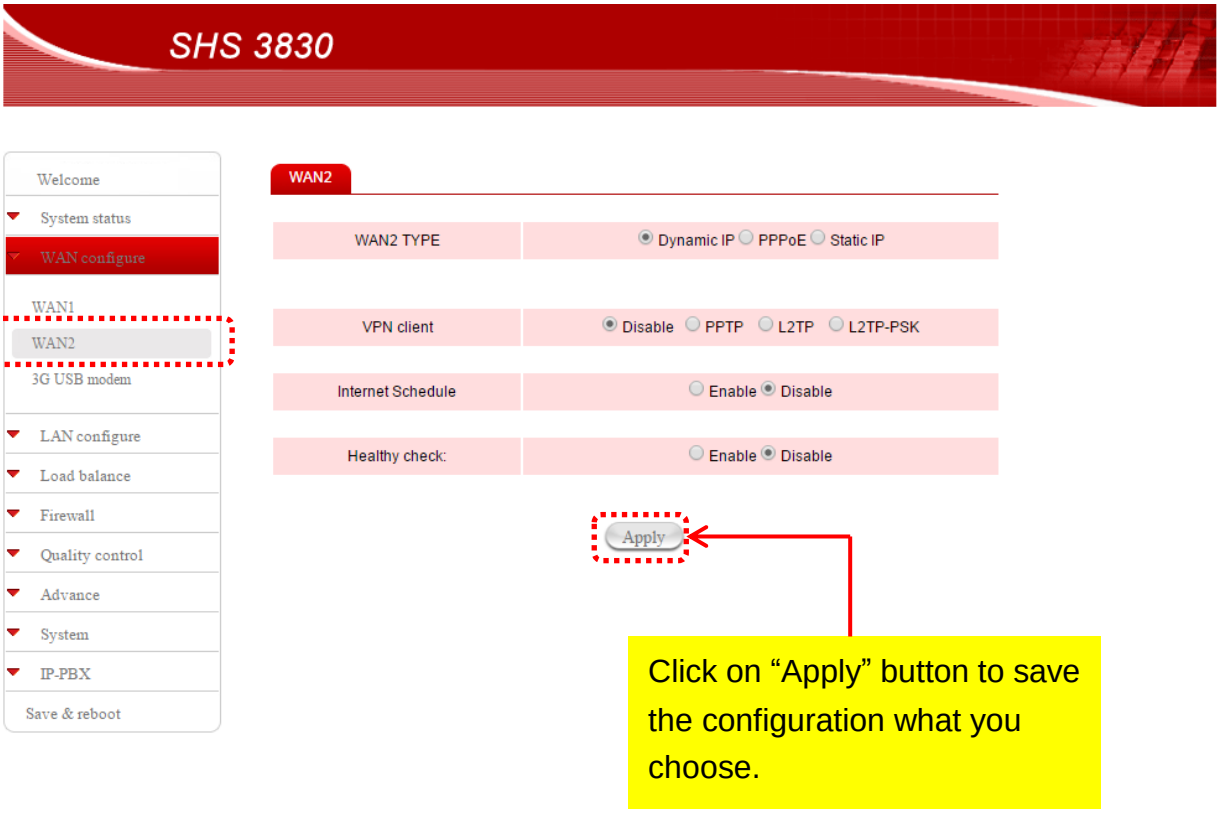
Note: When enable SCHEDULE function, the line will up/down following the timer set, no matter DOD function is enable or not.

Healthy check

User can select either Enable or Disable.

When choose Dynamic IP, you only need to save this selection by clicking on "Apply" button shown as below. When finish setting all parameter, reboot SHS 3830.

WAN Configure – WAN2 – Dynamic IP



The content and usage of WAN2 is the same as WAN1.

WAN Configure – WAN1 – PPPoE

PPPoE/Dial up DSL Type

Select “PPPoE” and you will need to enter the ID and Password. Sometimes you also need to input the Service Name if ISP requires for it. Max Idle Time is using to disconnect the ADSL connection automatically after the idle period you define. The unit is minute and the default is 0. This default value let SHS 3830 remain connecting all the time unless disconnected by user manually or ISP. If you define the period as 3 and the SHS 3830 will auto disconnect after idling 3 minutes. Supposing that you don’t have the Service Name, you may ask your ISP for it.

Account: User Name, provide by ISP, up to 60 characters can be enter.

Password: provide by ISP, up to 60 characters can be enter.

Max Idle Time: 0 =no check, check by minutes

Connect mode:

- ***Manual:*** You need to initiate WAN connection manually, by clicking "WAN1 connect" or "WAN2 connect" button in "System Status" - "Link status" menu. However, power up or reset also can initiate the WAN connection.
- ***Dial-on-demand:*** Whenever a user is trying to access the Internet from his computer, this WAN port will start connection automatically if it is disconnected.
- ***Always-on:*** The WAN port will try to establish the connection as long as it is disconnected, no matter this port is used or not.

LCP echo: To send LCP (Link Control Protocol) echo request at regular interval to ISP for checking PPPoE connection active.

Interval: Editable for need between 0 ~ 65535.

Counter: the number of LCP echo request to be sent.

about "always on " function, normally you need to combine "Health check " function together, then "always on" will be work more prefect because there have a ADSL modem between router & ISP equipment. in physical layer, if ADSL line fail but ADSL modem still alive , SHS 3830 can't detect line is broken unless ISP send a disconnect packet to SHS 3830 so if ADSL line is in abnormal up-down, sometimes router module of SHS 3830 does not get disconnect message from ISP, so connected line is deemed to still connection by SHS 3830.

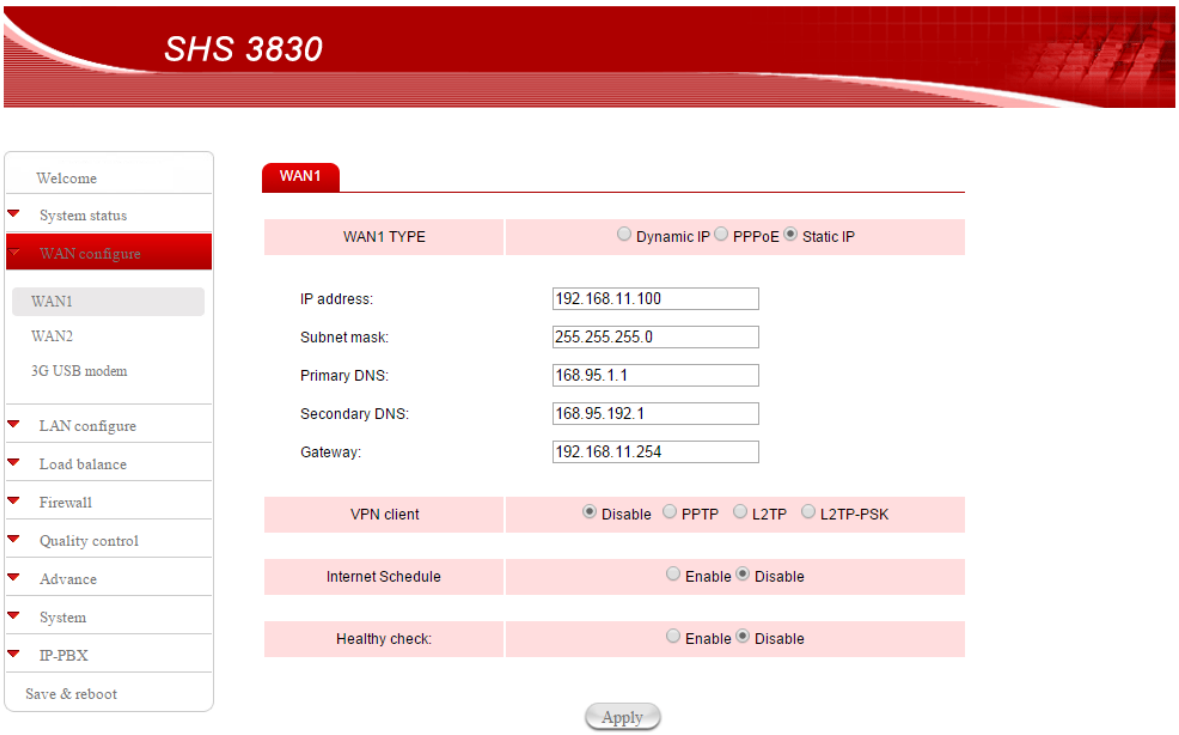
If you enable "Health check " in each line. then the SHS 3830 can automatically send packet out through WAN to detect whether line is active or not (1 packet/30 sec) this function will cover entire network to secure packet will not lose in defect-line , include router-->ADSL modem--> ADSL line--> ISP Equipment---> Interest.

It's better to enable at least 2 options in "Health Check", in order to avoid misjudgments when only 1 option selected and that "option Server fail".

Static IP/Leased DSL Type

If you select **"**Static IP", you will need to input the IP address, Subnet Mask, Primary DNS, Secondary DNS and Gateway provided by your ISP. The picture below is an example of static IP's settings.

WAN Configure – WAN1 – Static IP



3G Access (3G USB Modem)

In order to prevent any case in losing wired line connections, 3G wireless line for backup seems the best way to keep line alive to make your business not affected. Just a few steps for configured page as below, and then it soon can be online with no obstacle.

Disable/Enable of 3G USB modem is subject to be deactivated or activated all the time since the device turns on, so make sure 3G USB modem attached before device power on. All necessary parameters for configuration can be acquired from ISPs offering for account.

WAN configure – 3G USB modem configure

PPTP Dial Up

PPTP dial up for WAN access type as below, need some parameters from ISPs to complete configuration page.

Ensure to key in user name and password as same as ISP offering. PPTP Server IP can be URL type or IP address that both are acceptable for device due to able to distinguish which one of them.

WAN Configure – WAN1 – Dynamic IP - PPTP

Below status shown established PPTP links for example.

L2TP Dial Up

If ISPs ask for L2TP for dial up, then user can choose and enable it just follow below page to fill in necessary items to launch Internet service.

WAN Configure – WAN1 – Dynamic IP – L2TP

L2TP over IPSec. Dial up (L2TP-PSK) (Option)

It is L2TP over IPSec. dial up to offer a better protection for Internet access. Although not many devices support the feature in market, it is a choice for user to adopt for specific requirement if necessary.

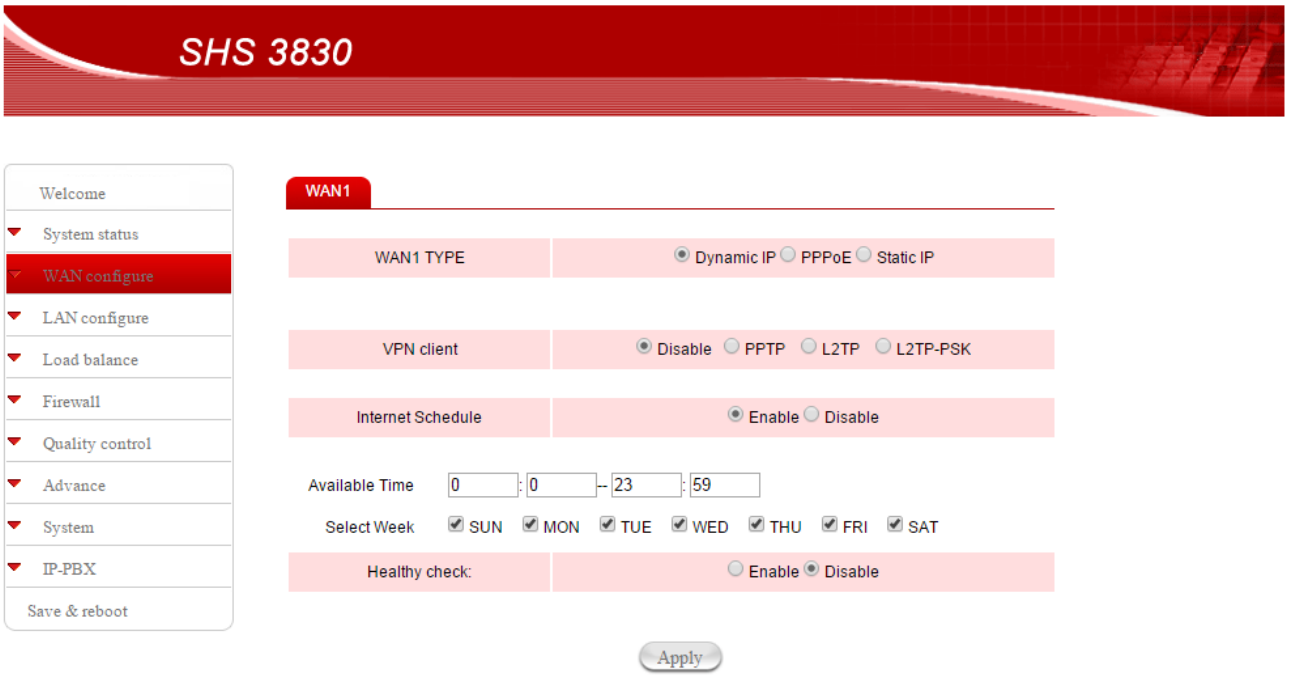
Regarding above various VPN Clients for dial up to Server to establish secured connection to access data or contents, many of them have been wildly adopted by enterprises for their resources share no matter in between branch and headquarter , or employee carry portable devices outside to online import and export data for business.

Basically, the SHS 3830 does NOT provide this feature. User has to pay for this option.

Internet Schedule

Scheduling Internet connection with time period to save cost and manage access internet for workers to improve efficiency.

WAN Configure – Internet schedule



Healthy check

1. Enable:

   SHS 3830 will check ADSL link automatically to check whether link alive or not ,if link fail, the Router will switch packet to another exist link(except TCP packet), the router will switch back to ADSL link again after router check ADSL line link again.

   SHS 3830 provides 3 methods to check ADSL link. You can choose it with each method or both as follows:

   - ✓ DNS : test DNS in Internet
   - ✓ Ping IP : to test IP in Internet
   - ✓ Time Server

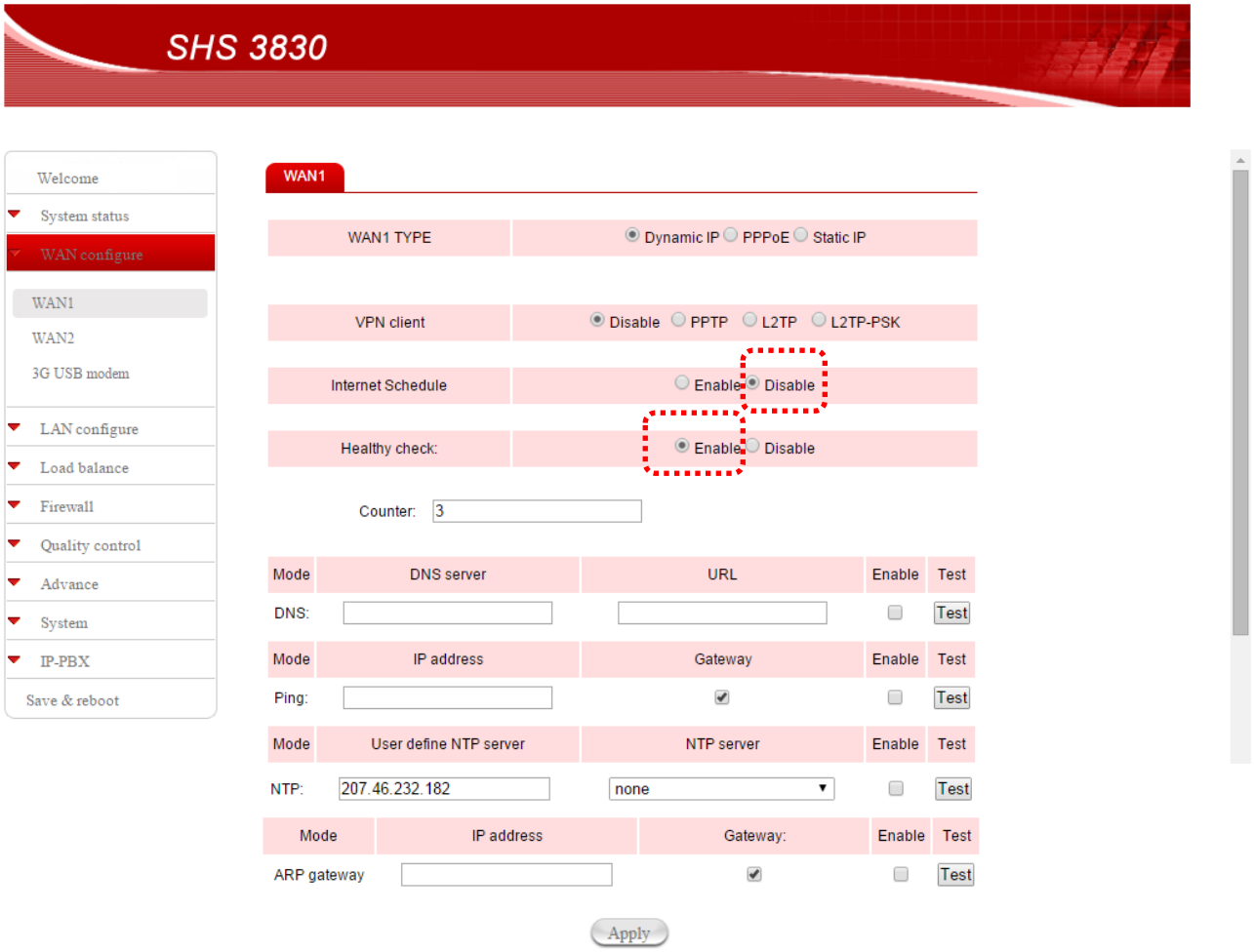
   Suggest select at least 2 method to check ADSL link, in order to avoid router making wrong action due to Internet Server disable.

2. Disable: no Healthy check function

   If without “Time Server” existing, this function will disable automatically.

   Healthy check can be set up to test 3 different destination IP, in order to avoid wrong operation (in case destination server is fail).

WAN Configure – Healthy check



2.5.2 LAN configuration

LAN configure includes two functions. One configures LAN port. Include DHCP. The other set the DHCP Reserved IP.

2.5.2.1 LAN Configure

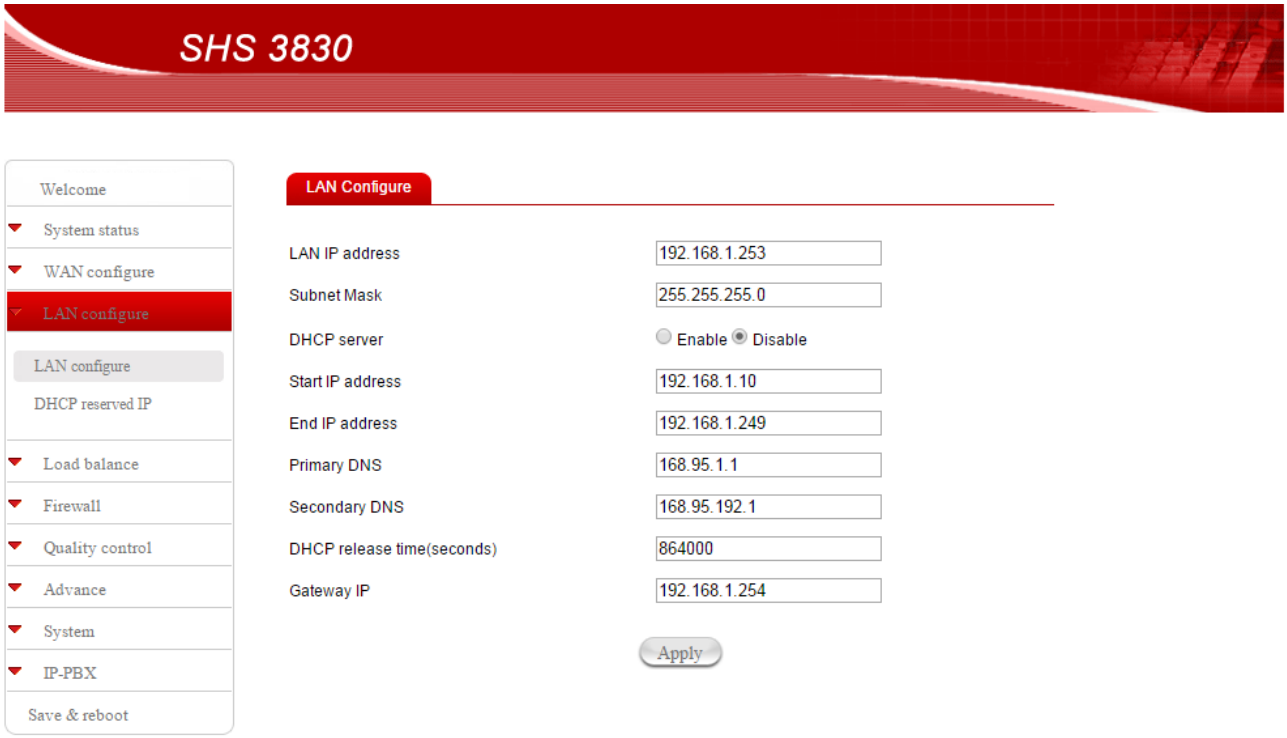
This function configures the LAN ports

- IP address
- Subnet Mask
- DHCP.

You can choose using DHCP server or not, the Dynamic Host Configuration Protocol (DHCP) allows the SHS 3830 to dynamically assign IP addresses to network devices. Dynamic IP assignment alleviates the need for the network administrator to maintain and monitor IP address assignments and simplifies IP use because the IP addresses are automatically and dynamically assigned when a station powers-on. You will need to indicate the range of DHCP server and DNS address if you enable DHCP server function.

When enable DHCP Server in “From”, ”TO” field, user **assigns** class A,B,C IP which suit for network topology. Fill in local DNS Server IP address in “**DNS Address”** field, you can ask your local ISP to provide this information.

LAN Configure – LAN Configure



LAN IP address: Input IP address for LAN port of SHS 3830. If user set up SHS 3830 be static IP mode, user need to input IP address of LAN and Subnet Mask.

Subnet Mask: Input Subnet Mask for LAN port of SHS 3830.
DHCP server: User can select either Enable or Disable.
Start IP address: Input Start IP address.
End IP address: Input End IP address.
Primary DNS: Input Primary DNS address.
Secondary DNS: Input Secondary DNS address.
DHCP release time (seconds): Input the number of seconds
Gateway IP: If user set up SHS 3830 be static IP mode, user need to input IP address of Gateway. The default Gateway IP address is 192.168.1.254
At last, user needs to click on “Apply” button to save configuration.

2.5.2.2 DHCP reserved IP

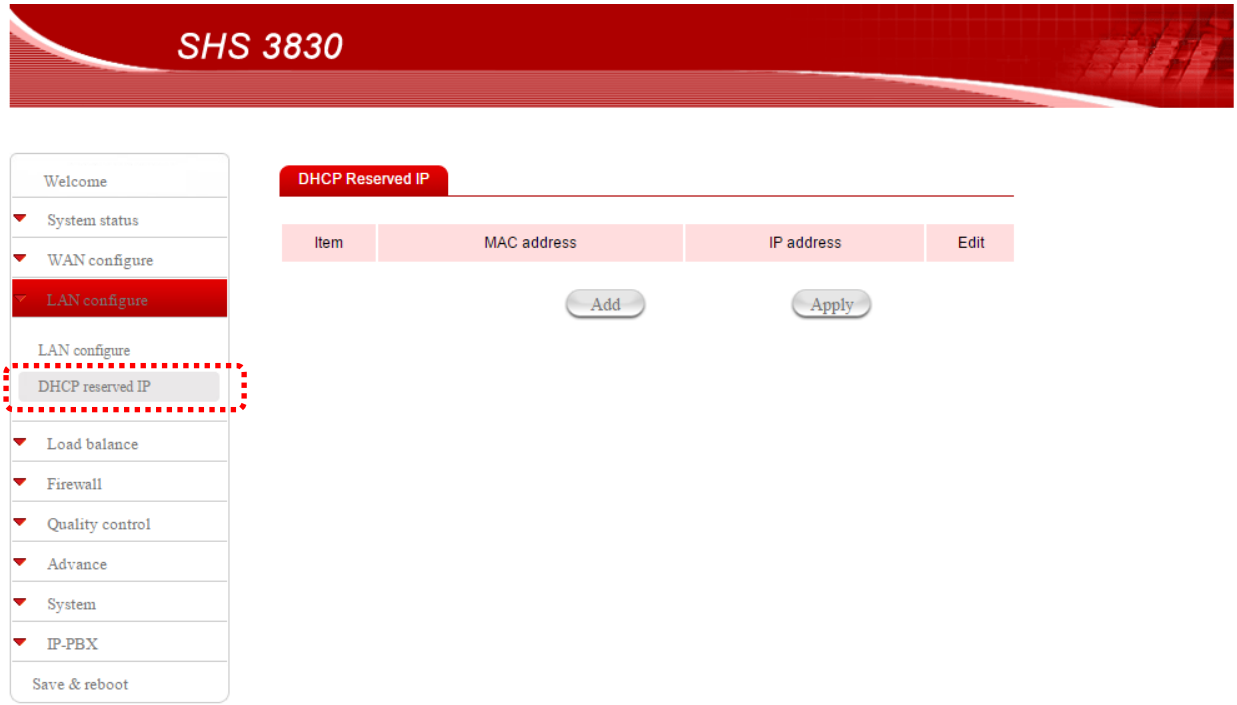
The second submenu of LAN configure is DHCP reserved IP.

You can also reserve some IP’s to specific computers. You need to enter the name (MAC address) of the network card installed in your computer to assign a particular IP to it. Click **ADD** to enter a new web page for adding a reserved IP.

For example : Add a new item.

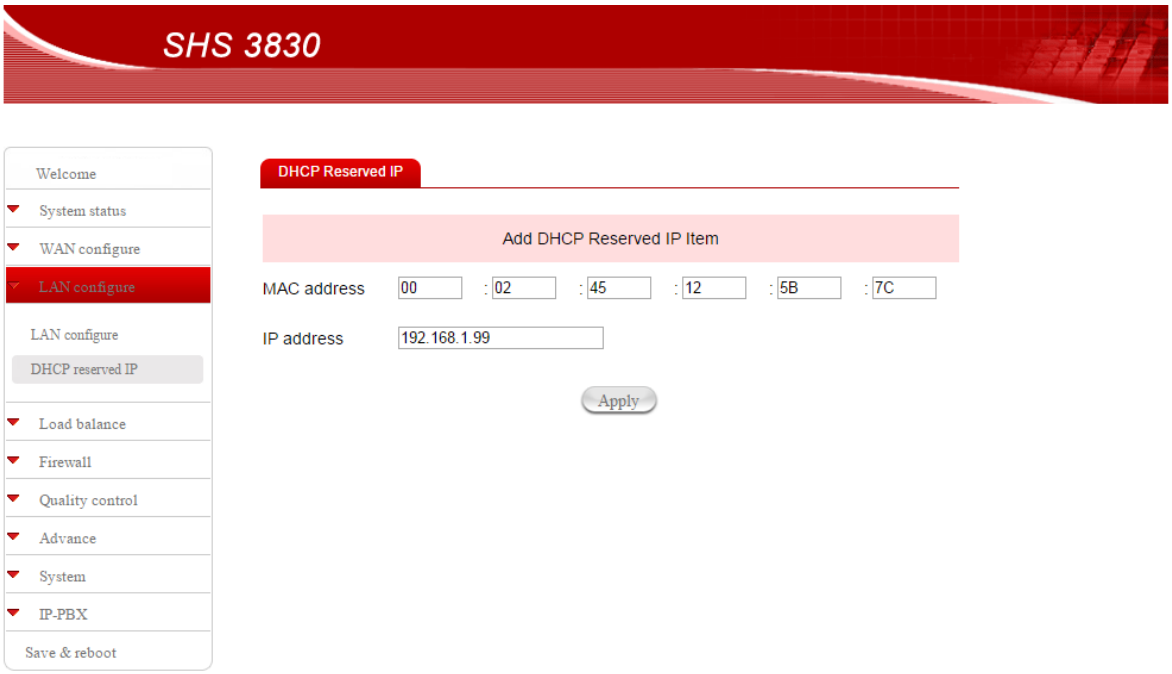
Step 1: Enter **DHCP reversed IP** web page. Then click “Add” to enter the added page.

LAN Configure – DHCP reserved IP

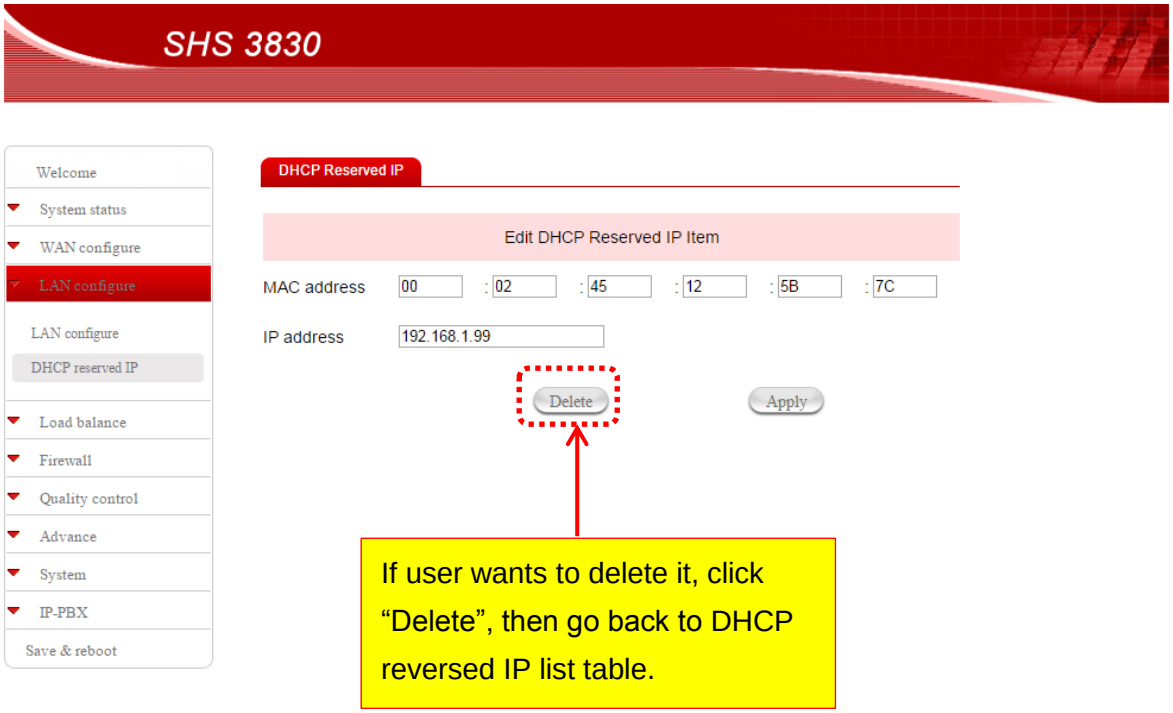


Step 2: Fill data to MAC address and IP. Then Click “Add” then SHS 3830 goes back to **DHCP reversed IP** list table. The input screen shows as follows.

LAN Configure – DHCP reserved IP – ADD



Step 3: Then click “Apply” to save. You will see the screen of DHCP reversed IP list table as below.



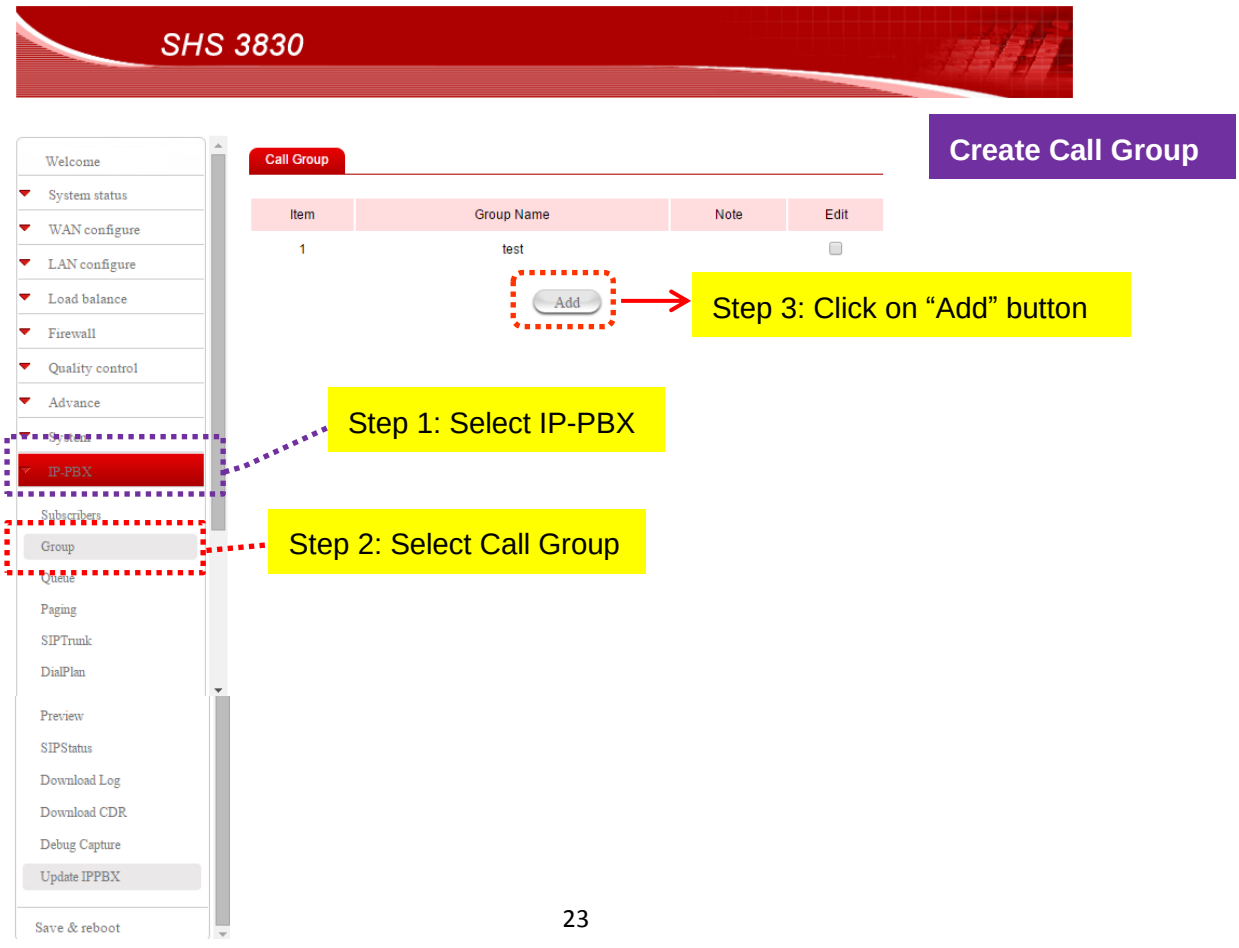
2.5.3 IP-PBX

At first, user needs to create call group. User can select "IP-PBX" in the menu bar on the left side of screen as shown below.

2.5.3.1 Group

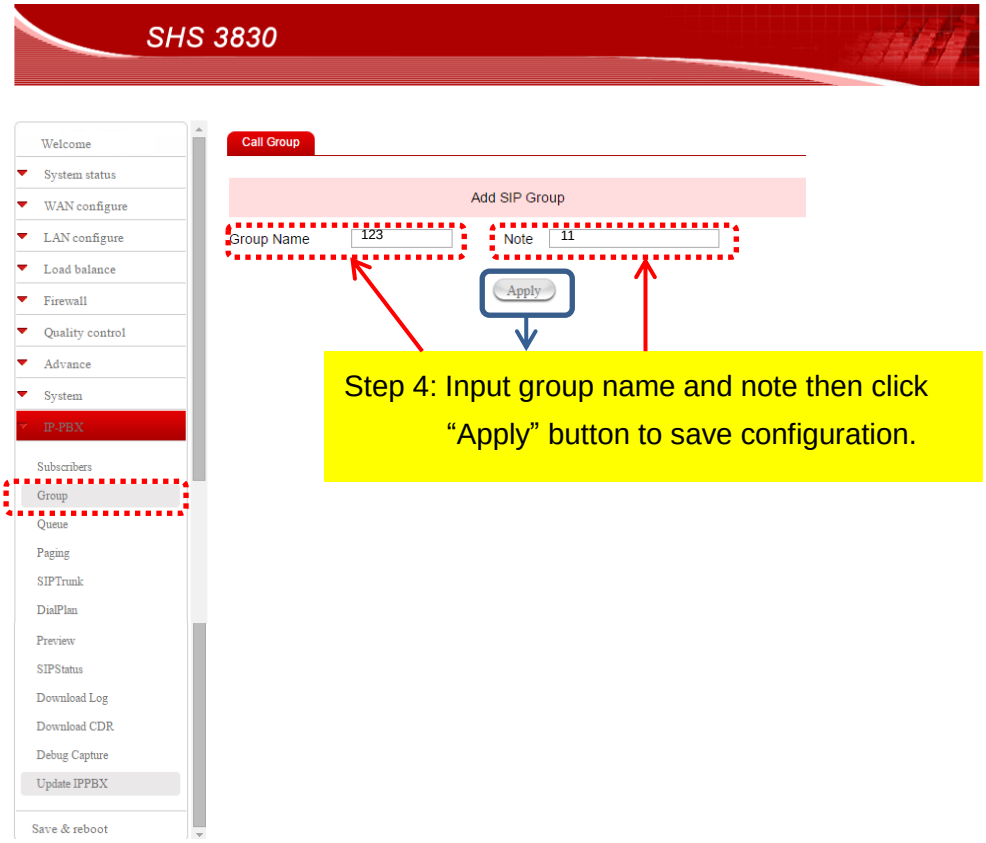
Then step by step to set up call group as shown below.

IP-PBX – Group

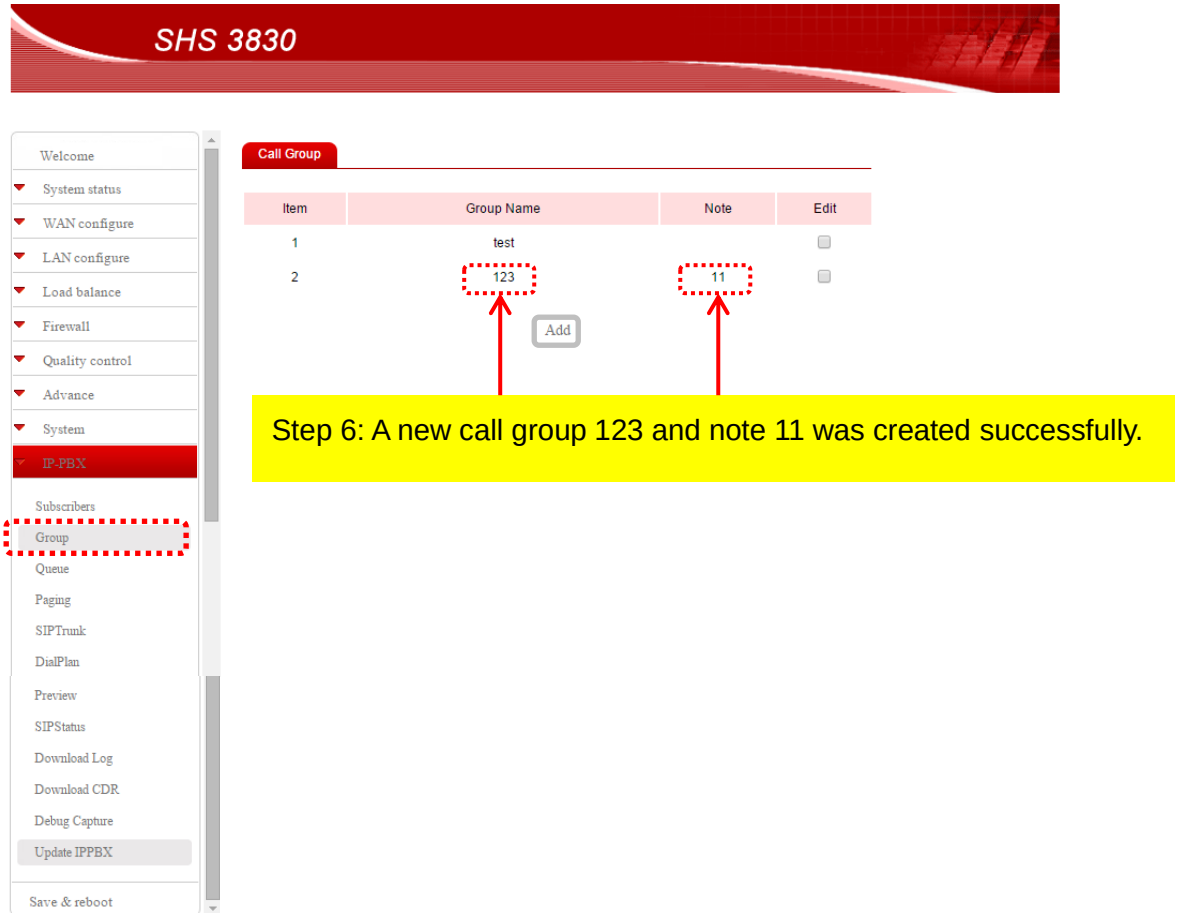


Then user will see the screen of add SIP group. Please input group name and note to create a SIP group.

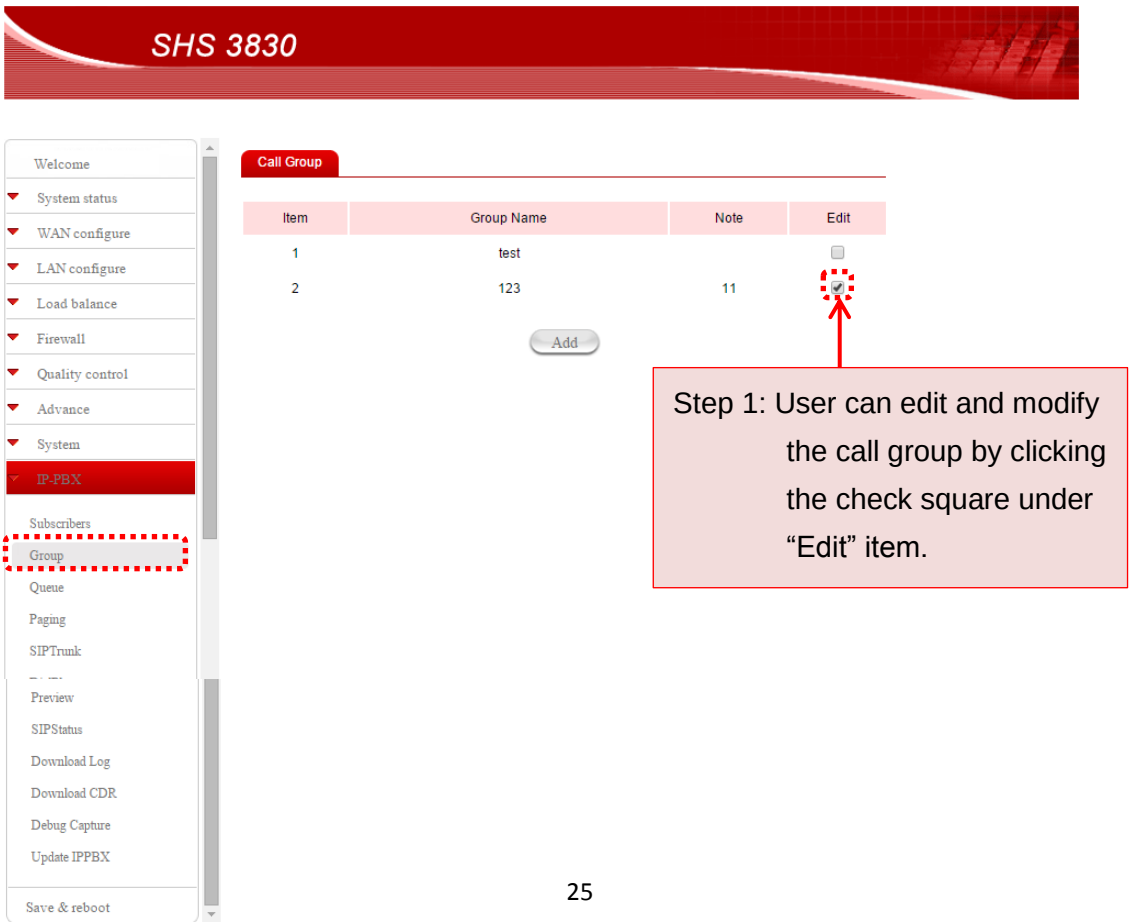
IP-PBX – Group – Add SIP Group



Then user will see a new call group and note was created successful and display on the screen as below.

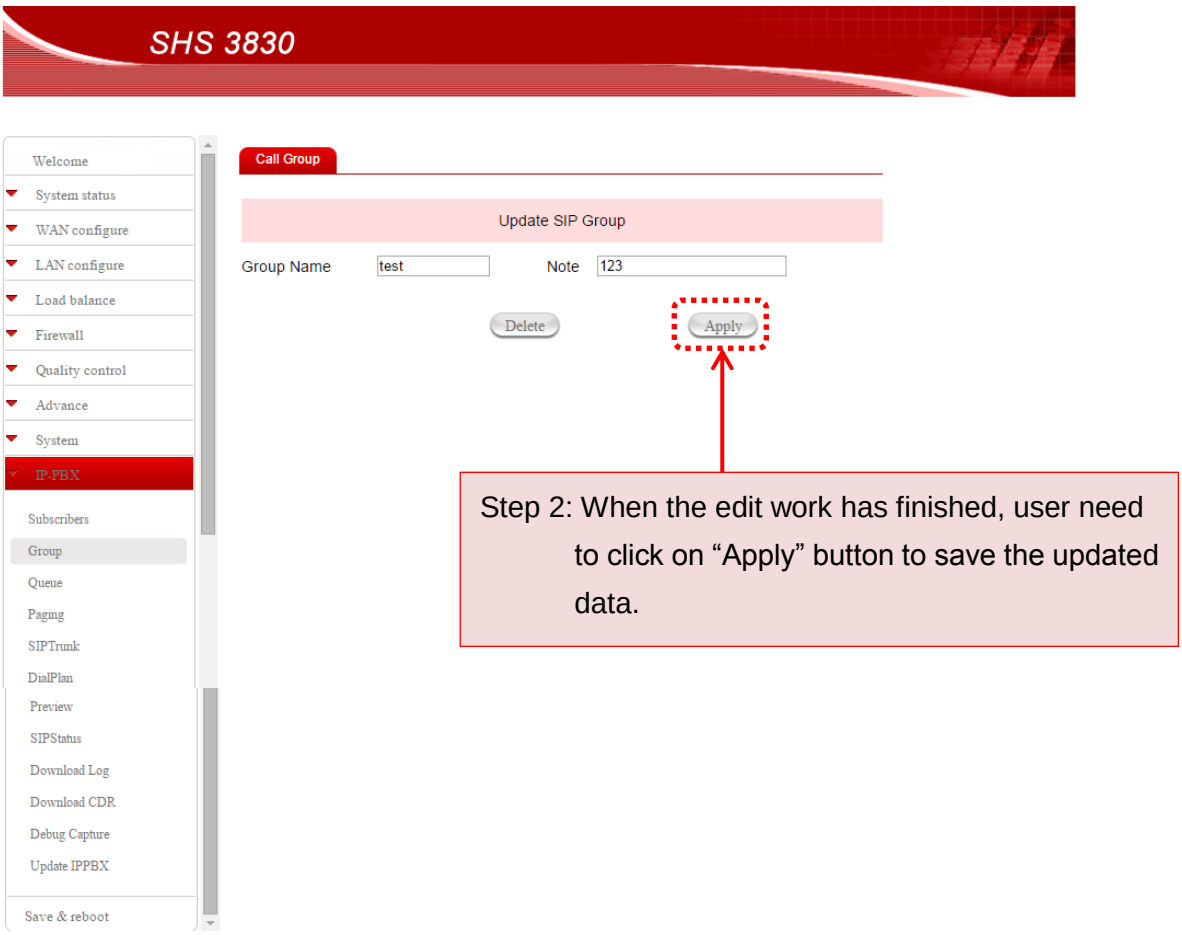


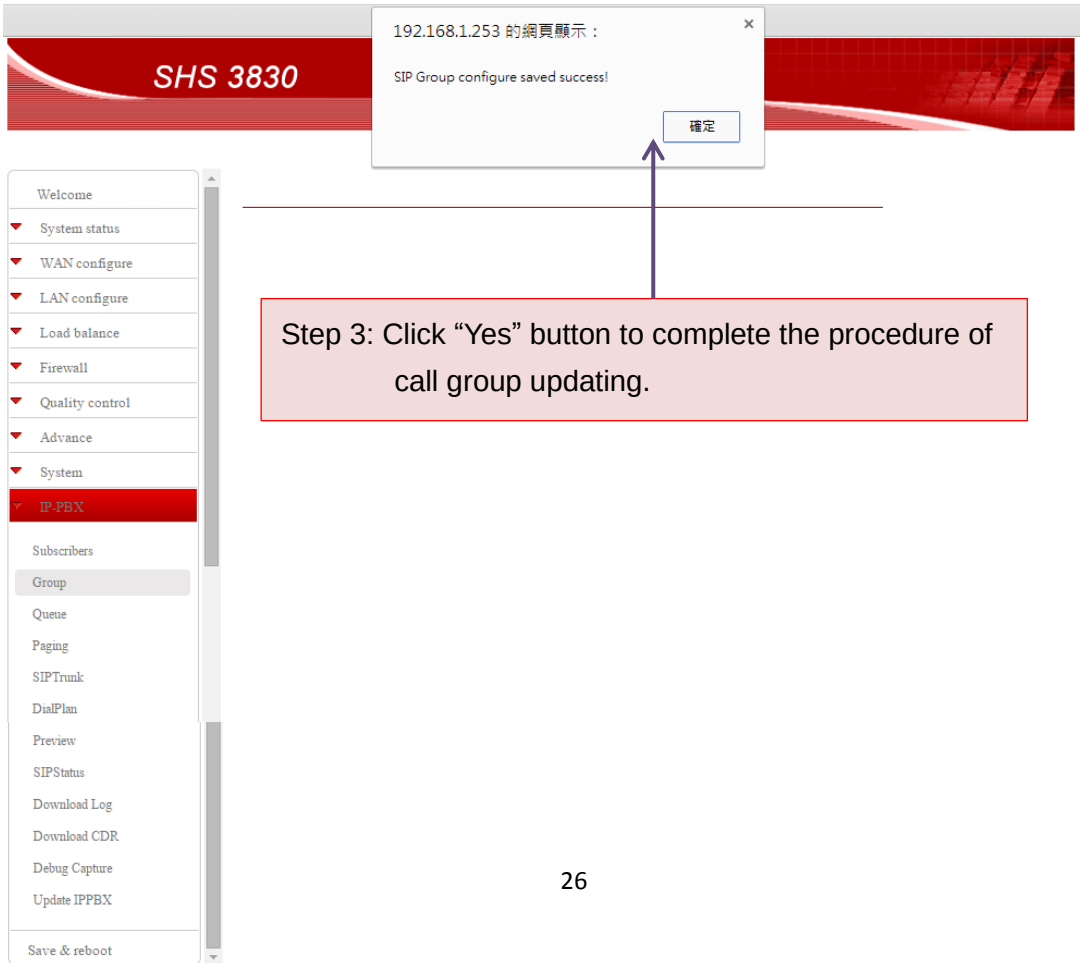
User also can edit and modify the call group by clicking the check square under “Edit” item.



Then user can see the screen of update SIP group as below. User can modify or delete the group to meet user's requirement. When the edit work has finished, user need to click on "Apply" button to save the updated data.

IP-PBX – Group – Updated SIP Group

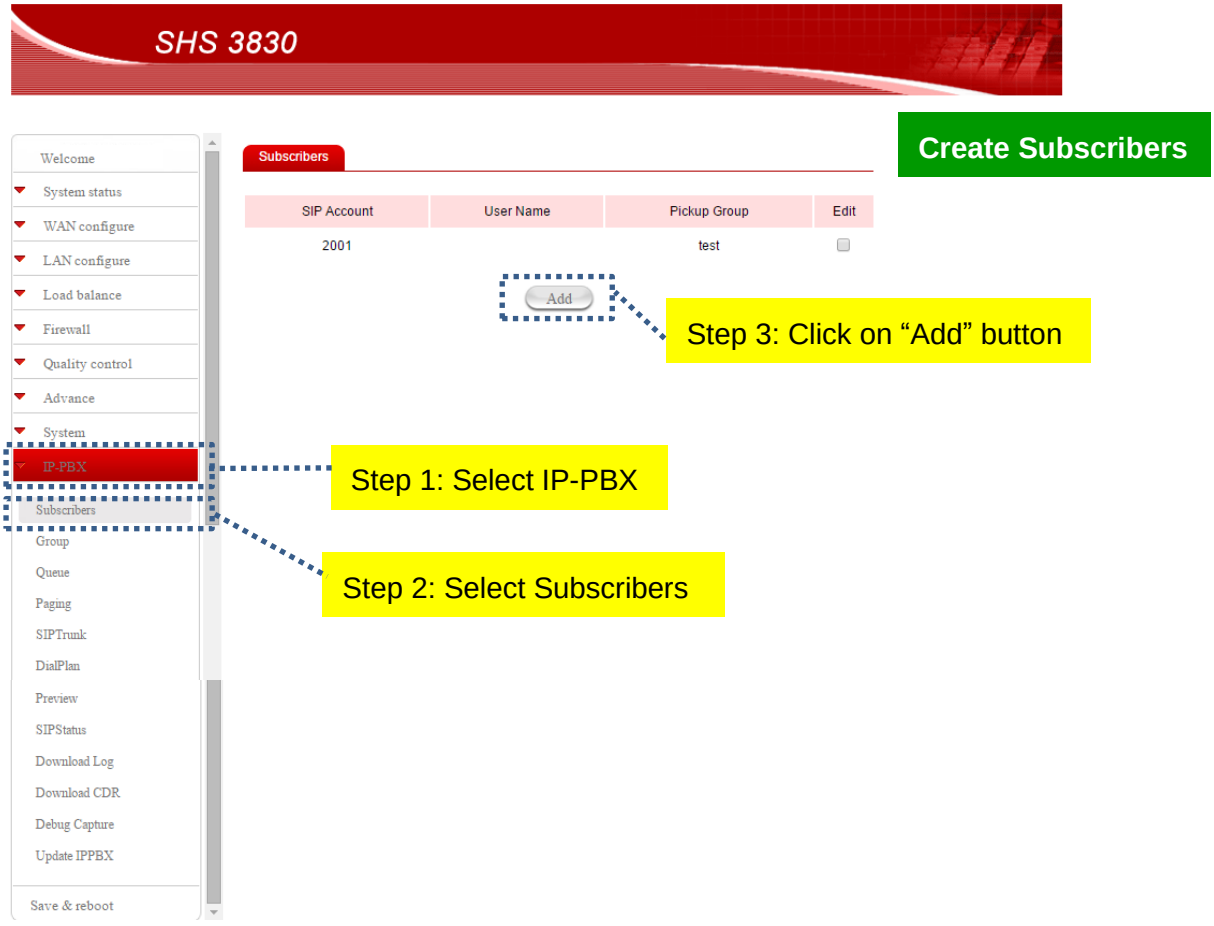




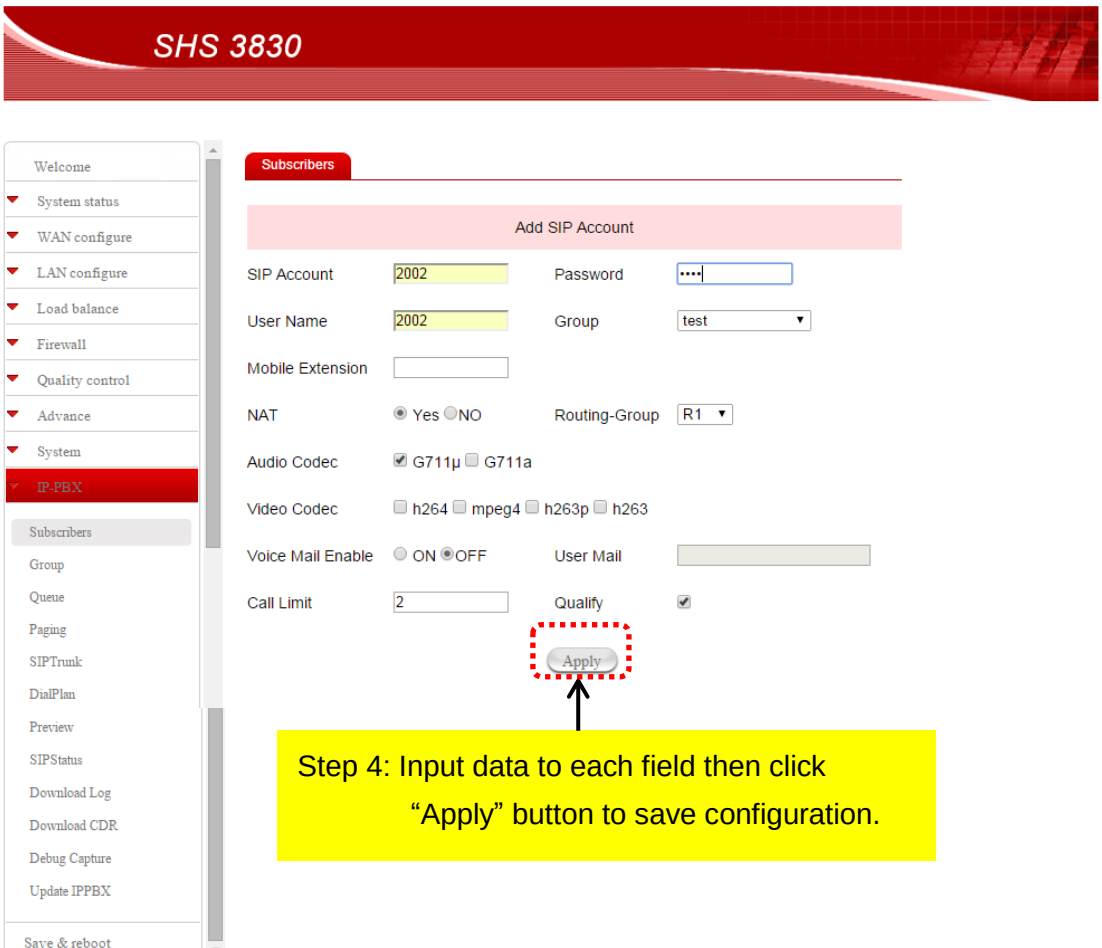
2.5.3.2 Subscribers

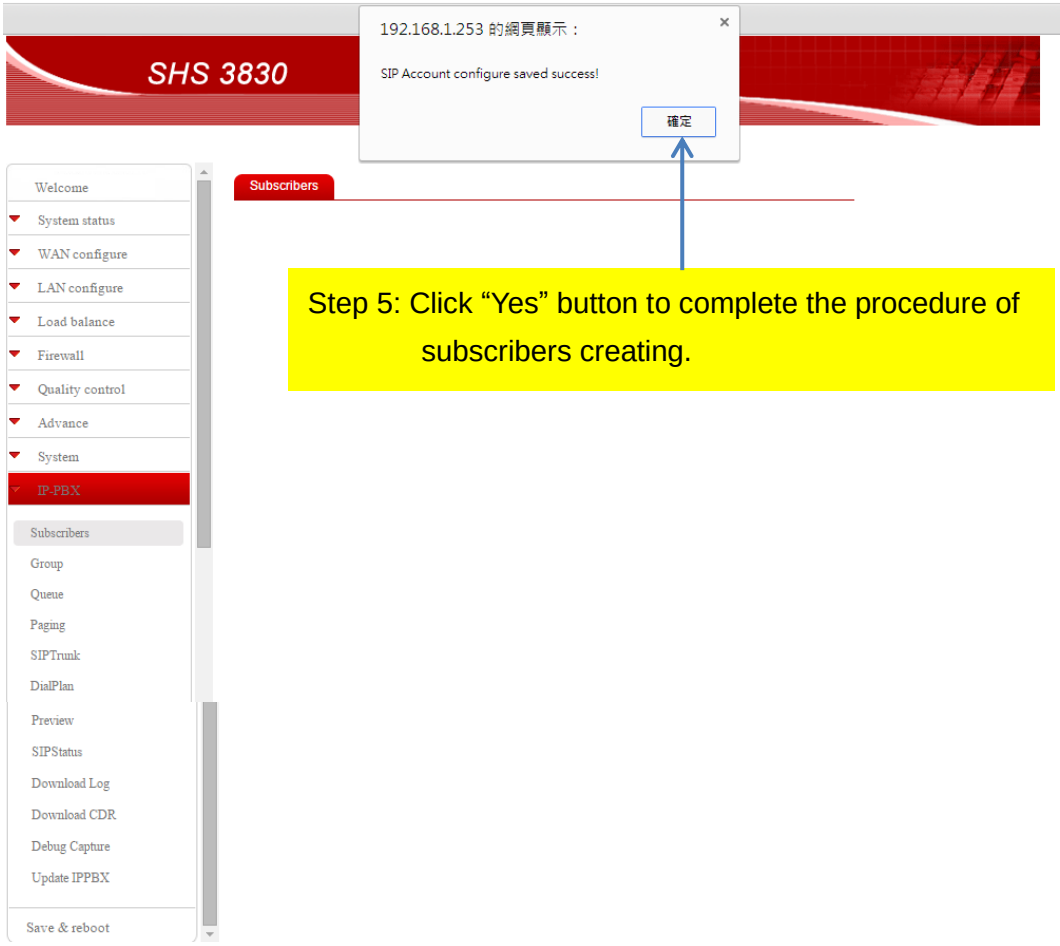
In the next step, user has to create new subscriber for IP-PBX operating. The operation procedure is shown as following diagrams.

IP-PBX – Subscribers



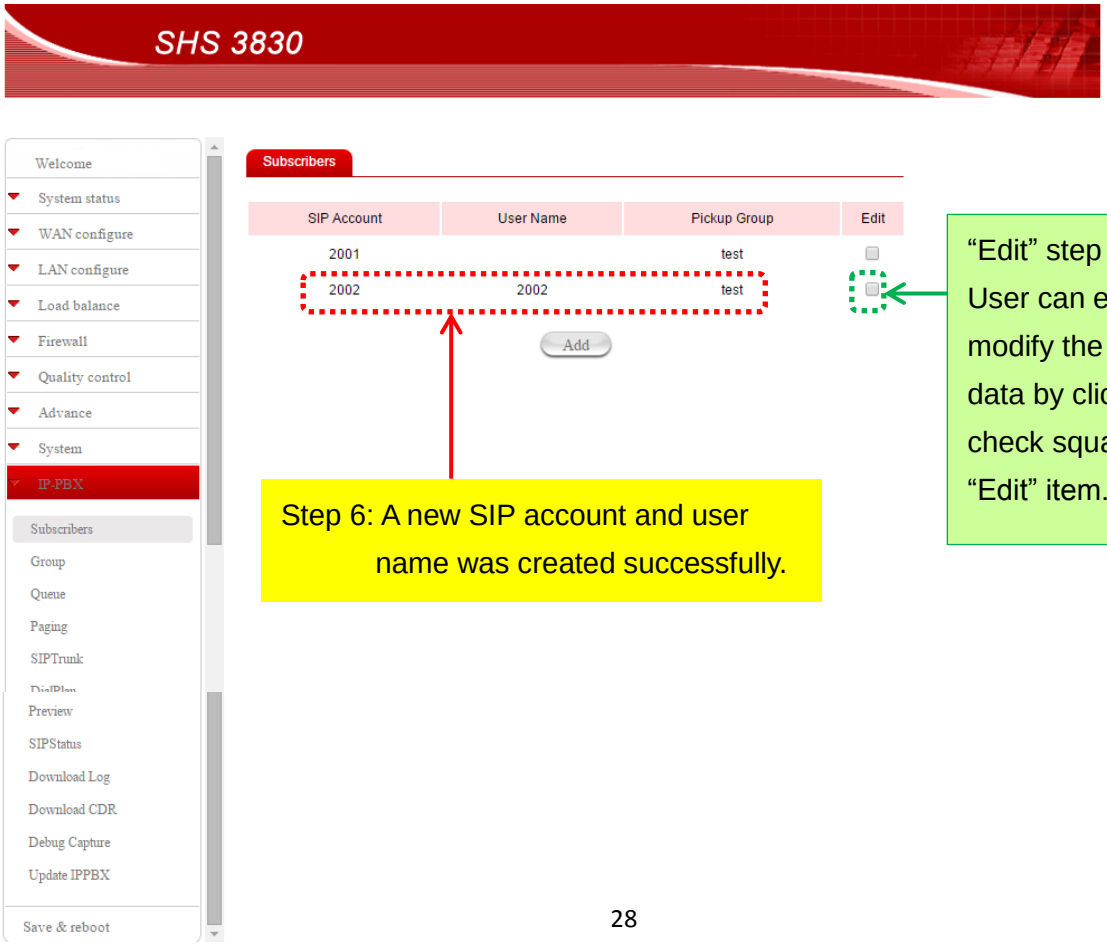
After click “Add’ button, user can see the screen as below.





Step 5: Click “Yes” button to complete the procedure of subscribers creating.

Then user will see a new SIP account with user name and pickup group was created successful and display on the screen as below.

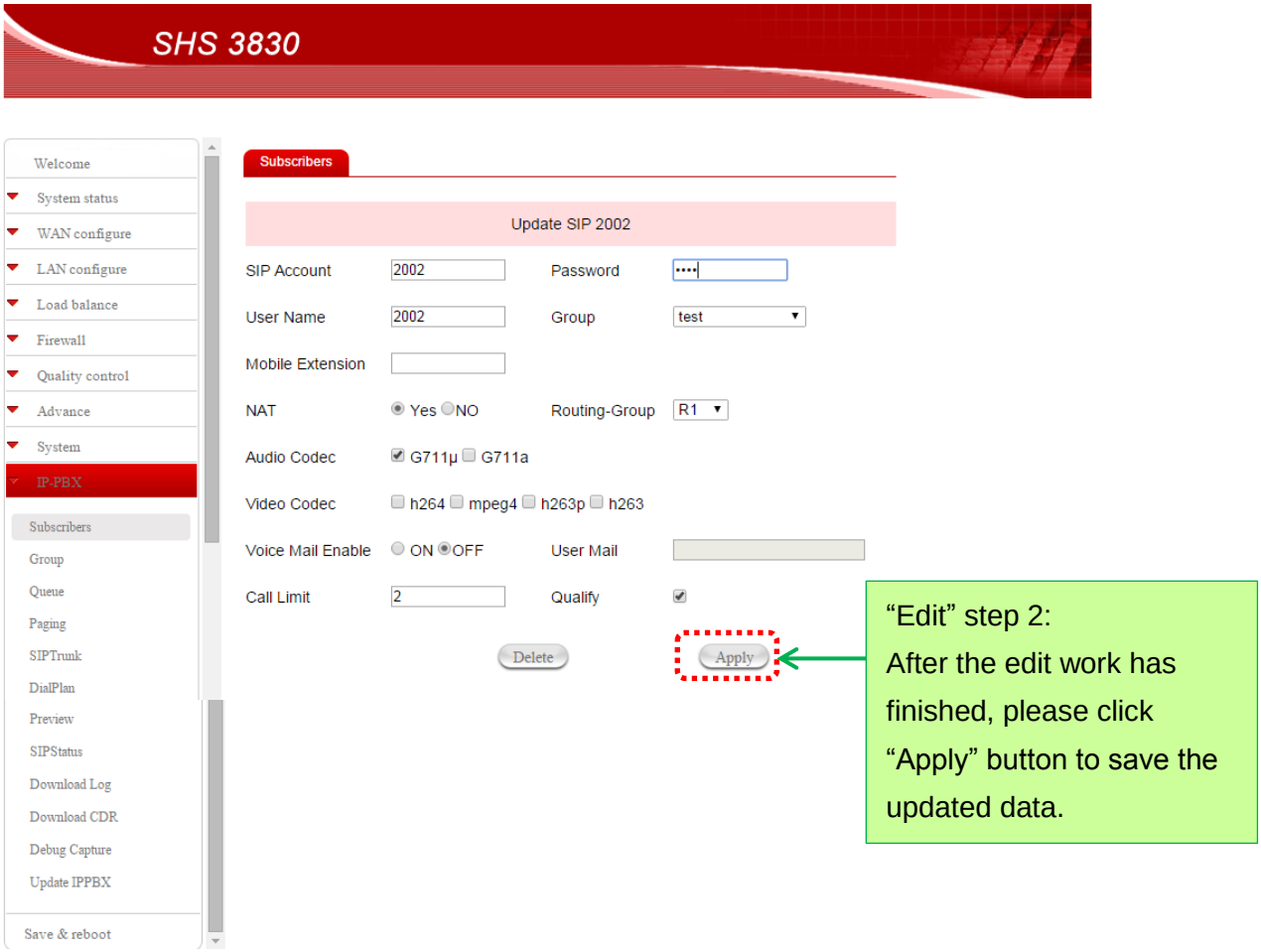


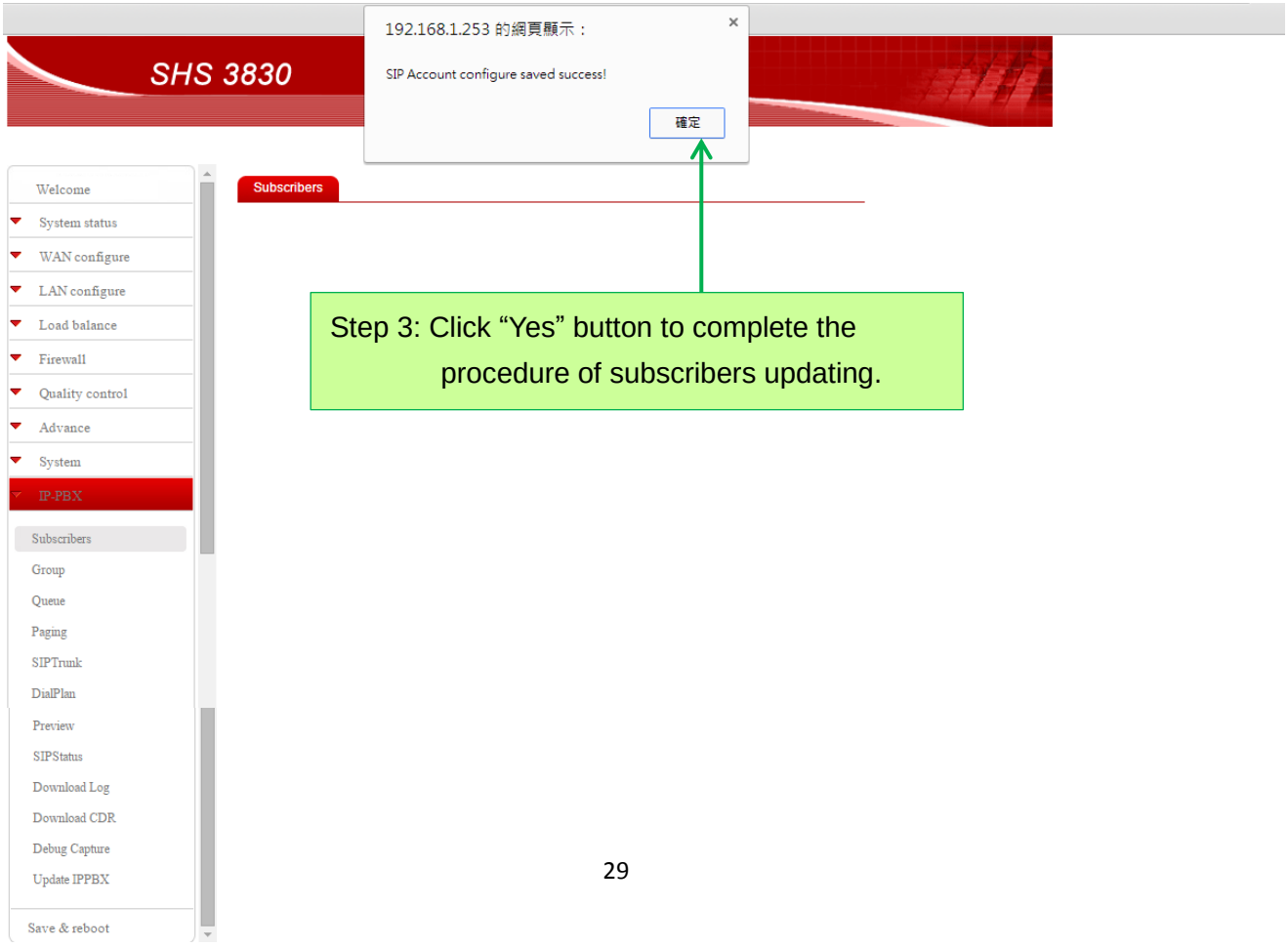
Step 6: A new SIP account and user name was created successfully.

“Edit” step 1:
User can edit and modify the subscriber data by clicking the check square under “Edit” item.

User can edit and modify the subscriber data by clicking the check square under “Edit” item as shown above. Then user will see the screen of update SIP account as below.

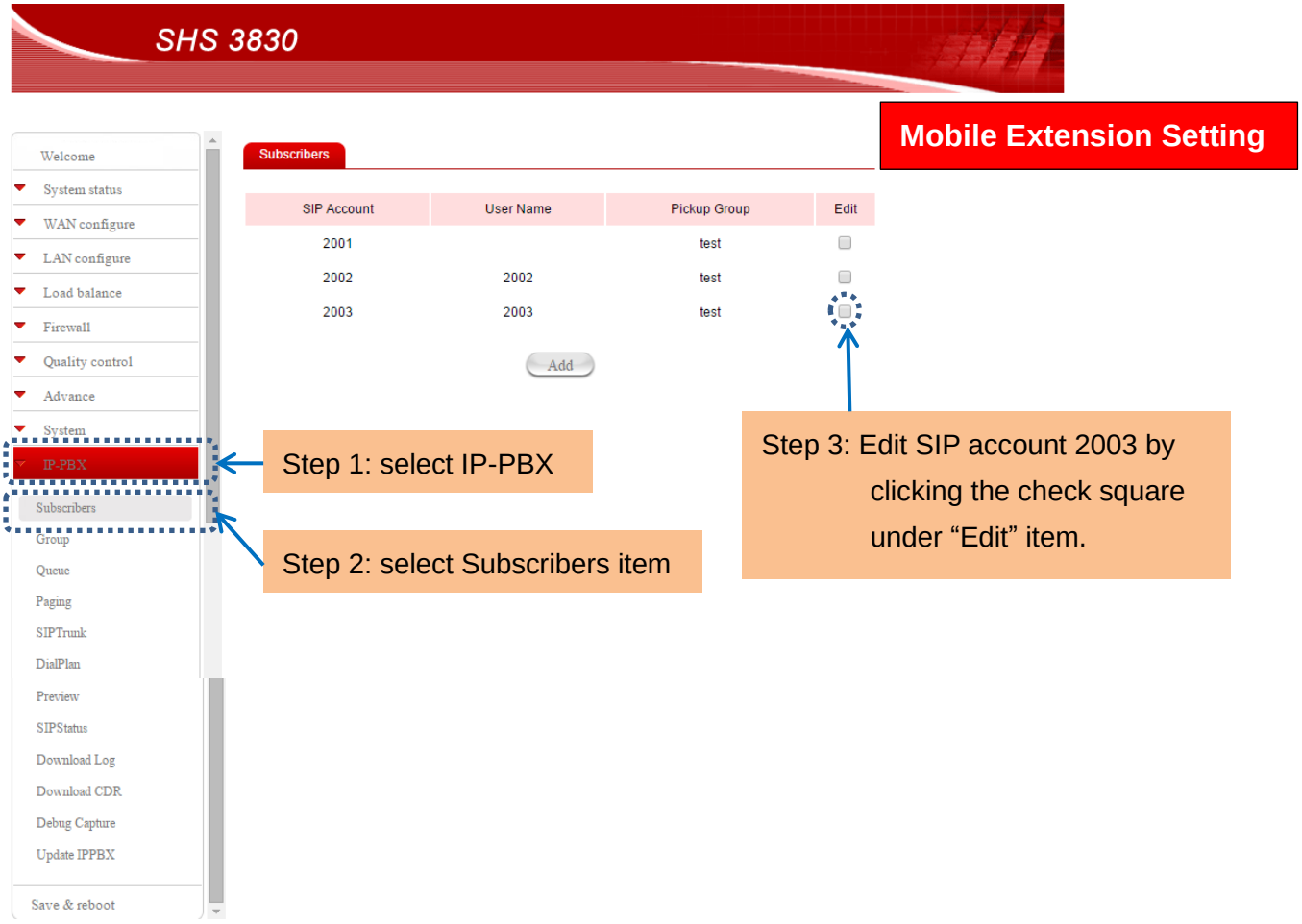
IP-PBX – Subscribers – Update SIP account

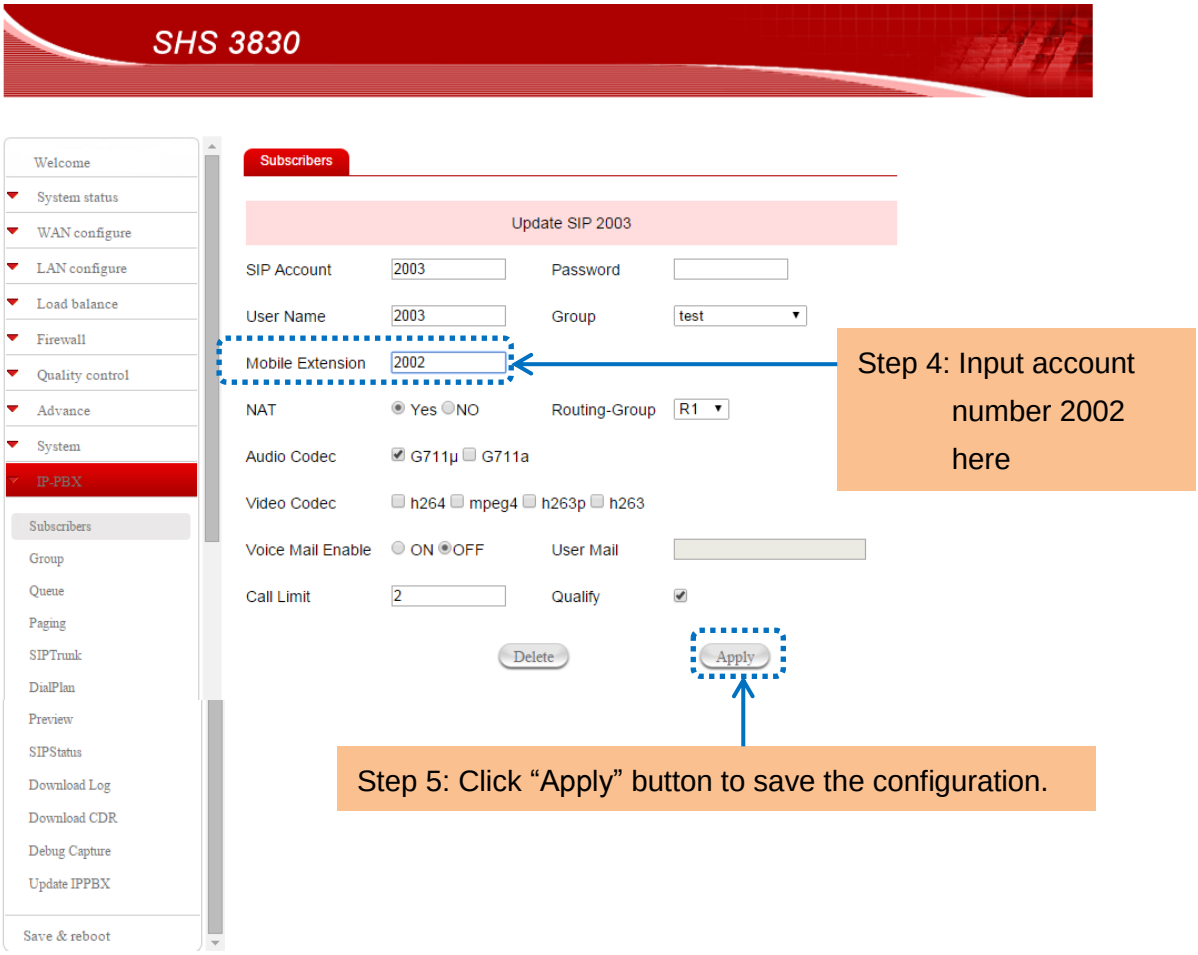




Mobile extension setting

Except create and edit subscribers as above description, now we would like to introduce how to set up mobile extension for user. For example, there are two SIP account 2002 and 2003. ***If user wants to use account 2002 as mobile extension***, please set up it as following steps.





Once user has finished above configuration, someone call 2003, the extension 2002 will ring too. One of call answer, the other call will hang up automatically.

Call Transfer

The SHS 3830 supports call transfer now. During talk over the phone, you can press ***** and **9** for call transfer. After hearing the transfer voice, dial the extension number that you want to transfer.

Blind Transfer

The SHS 3830 supports blind transfer now. You can press ***** and **0** for blind transfer.

Call Group

You can use the Call Group parameter to assign an Extension to one or more groups.

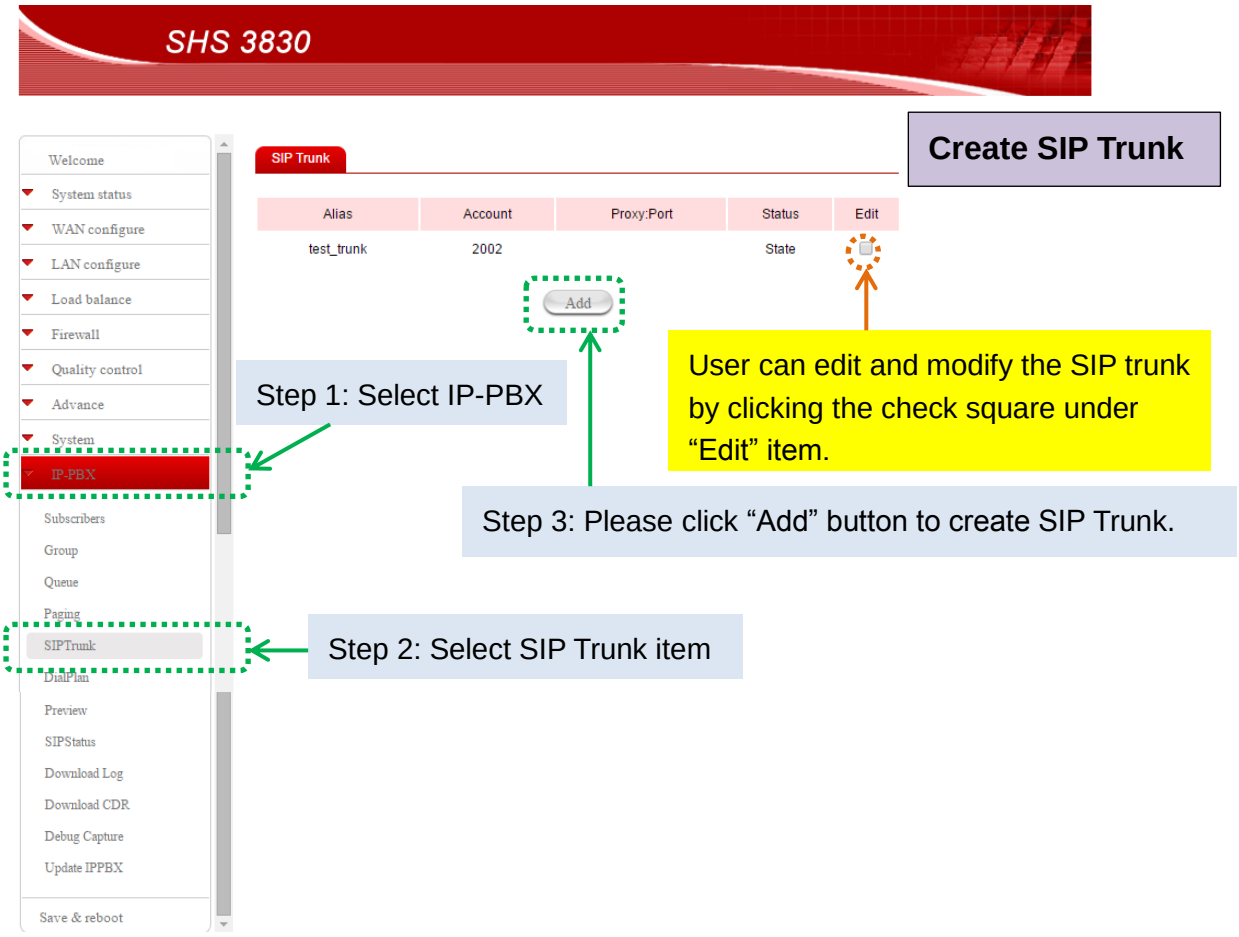
Pick up Group

The SHS 3830 supports call pickup to allow a ringing phone to be answered from another extension. If you set up some extensions in the same group, one of extension is ringing, but nobody answer, then you can pick up this call on your extensions by press *8 to answer. For example: Ext-A is ringing, Ext-B can press ***** and **8** for call pick up.

2.5.3.3 SIP Trunk

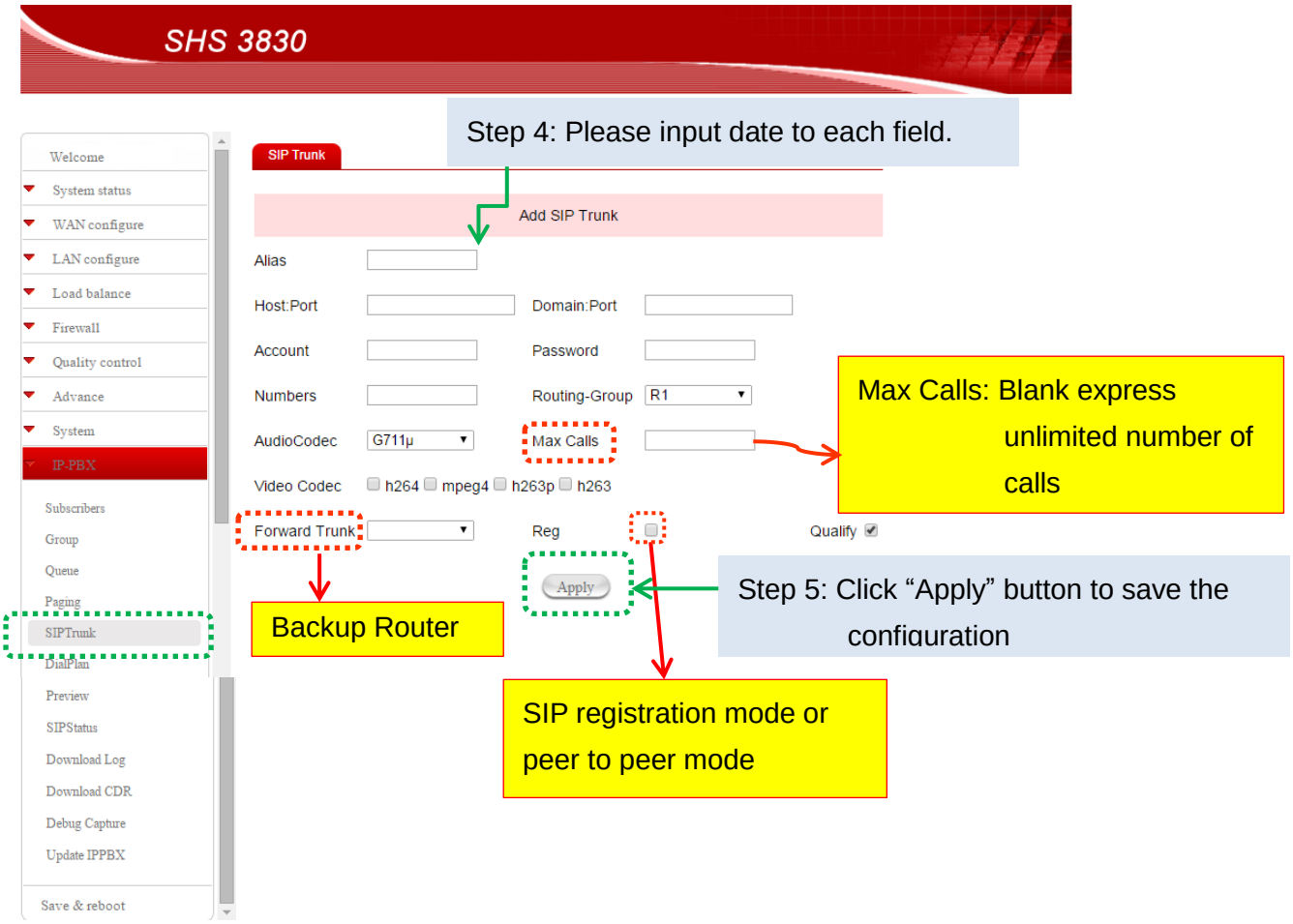
User has to set up set up some necessary configuration for SIP trunk. Please select “SIPTrunk” under IP-PBX item of menu bar. Then click “Add” button as below. Alias is also a Trunk name. User also can click the check square of **Edit** to delete the specified Trunk or modify configured Trunk data.

IP-PBX – SIP Trunk



Then user will see the following screen:

IP-PBX – SIP Trunk – Add SIP Trunk



2.5.3.4 Dial Plan

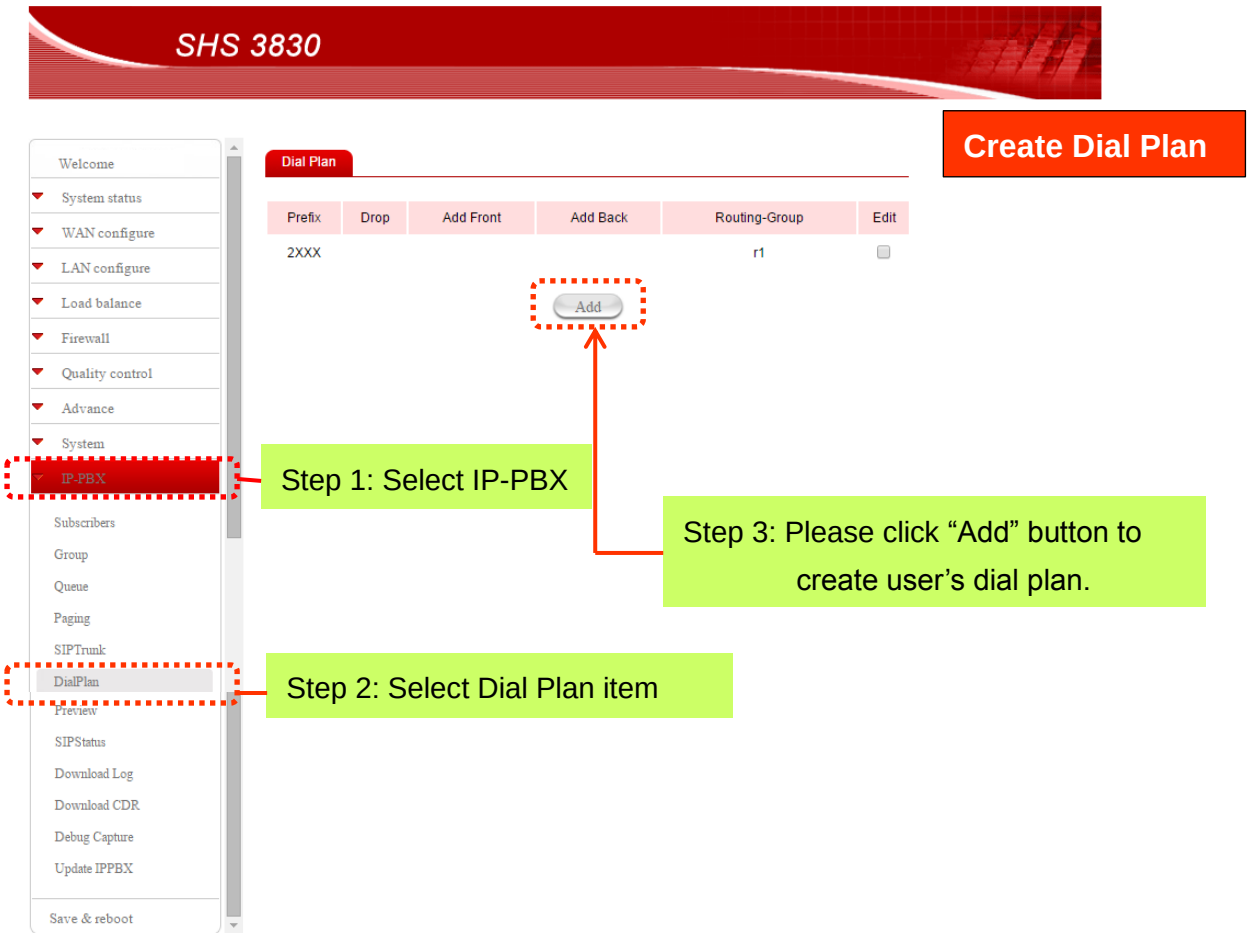
Define the dialing plan for Extension. It specifies the location of the instruction used to control what the phone is allowed to do, and what to do with incoming calls for this extension.

When users want to create their dial plan, please select “DialPlan” under IP-PBX item of menu bar. Then click “Add” button.

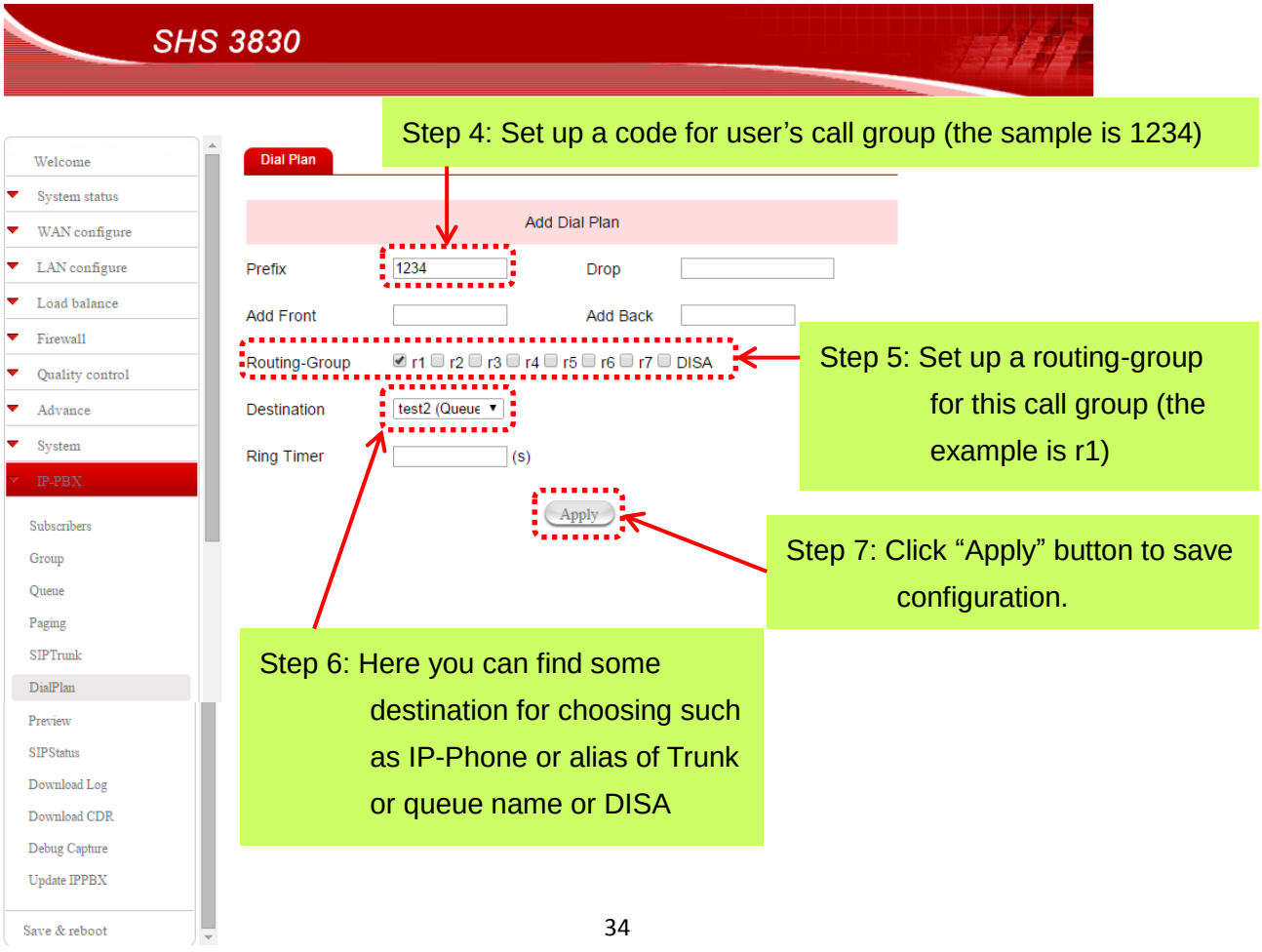
In the Dial Plan page, you should define the destination of prefix route. When you define the prefix route, you should set the Alias (Trunk ID) in the SIP Trunk page first; then you could input the correct Trunk ID in the Destination field. You also can input IP-Phone or Queue name or DISA.

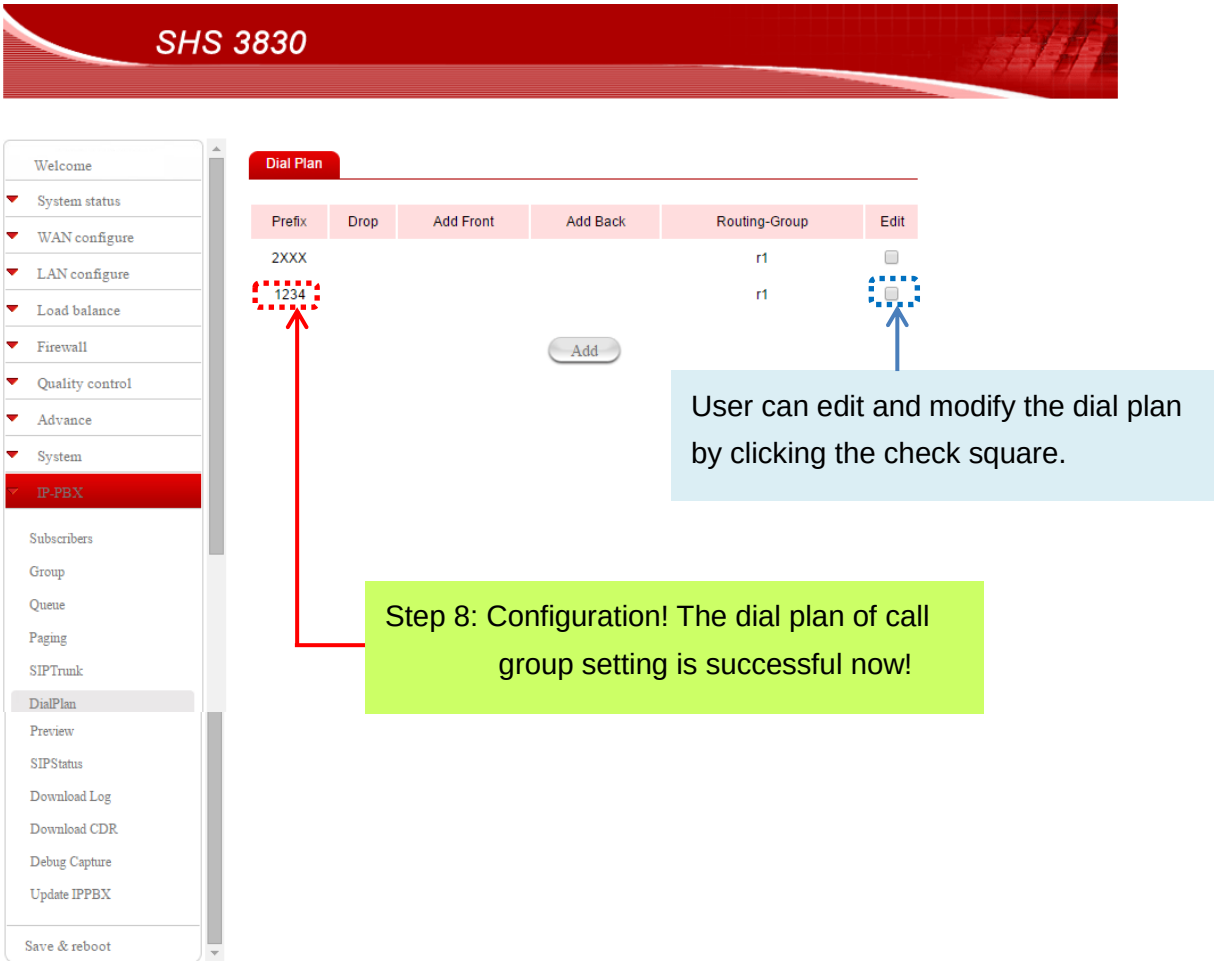
Routing group allows you to set up call routing from route level 1 to 7 and DISA. The application of DISA performs as automated attendant. The SHS 3830 supports Automated Attendant. You can record the default greeting and the other announcements, for example: invalid call or call is busy or no answer, for use. And click the check square of DISA. So the caller will hear greeting because the called number will be routed to auto attendant.

IP-PBX – Dial Plan

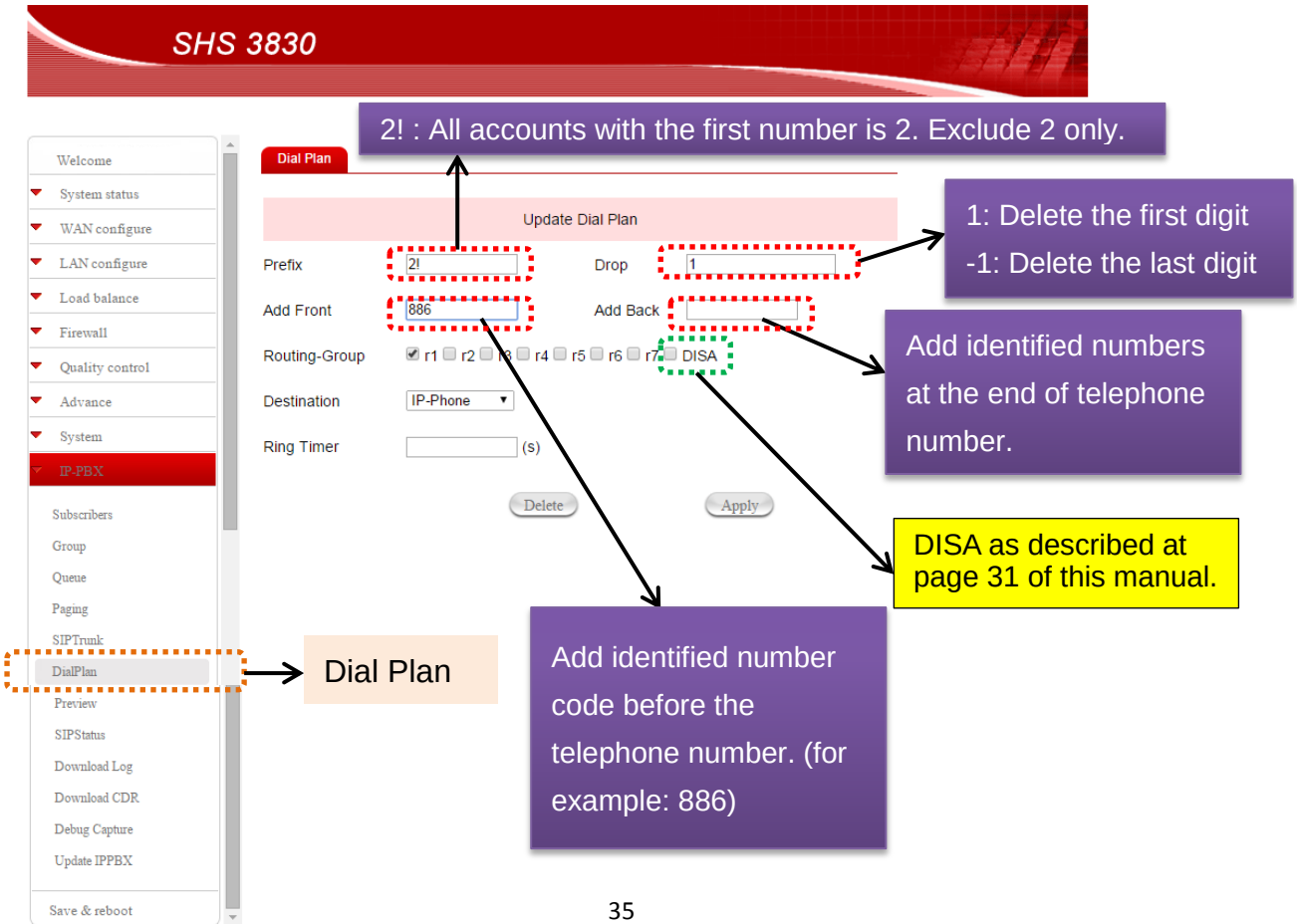


Then user will see the following screen “Add Dial Plan”:





Now we described each field of Dial Plan page as follows.



The rule of Prefix is described as follows.

0 ~ 9: number for telephone number

x: any number from 0 to 9. For example: 02 2222 12xx means the telephone number range is from 02 2222 1200 to 02 2222 1299.

2!: all accounts (i.e. telephone number) with the first digit is 2 and exclude 2 only.

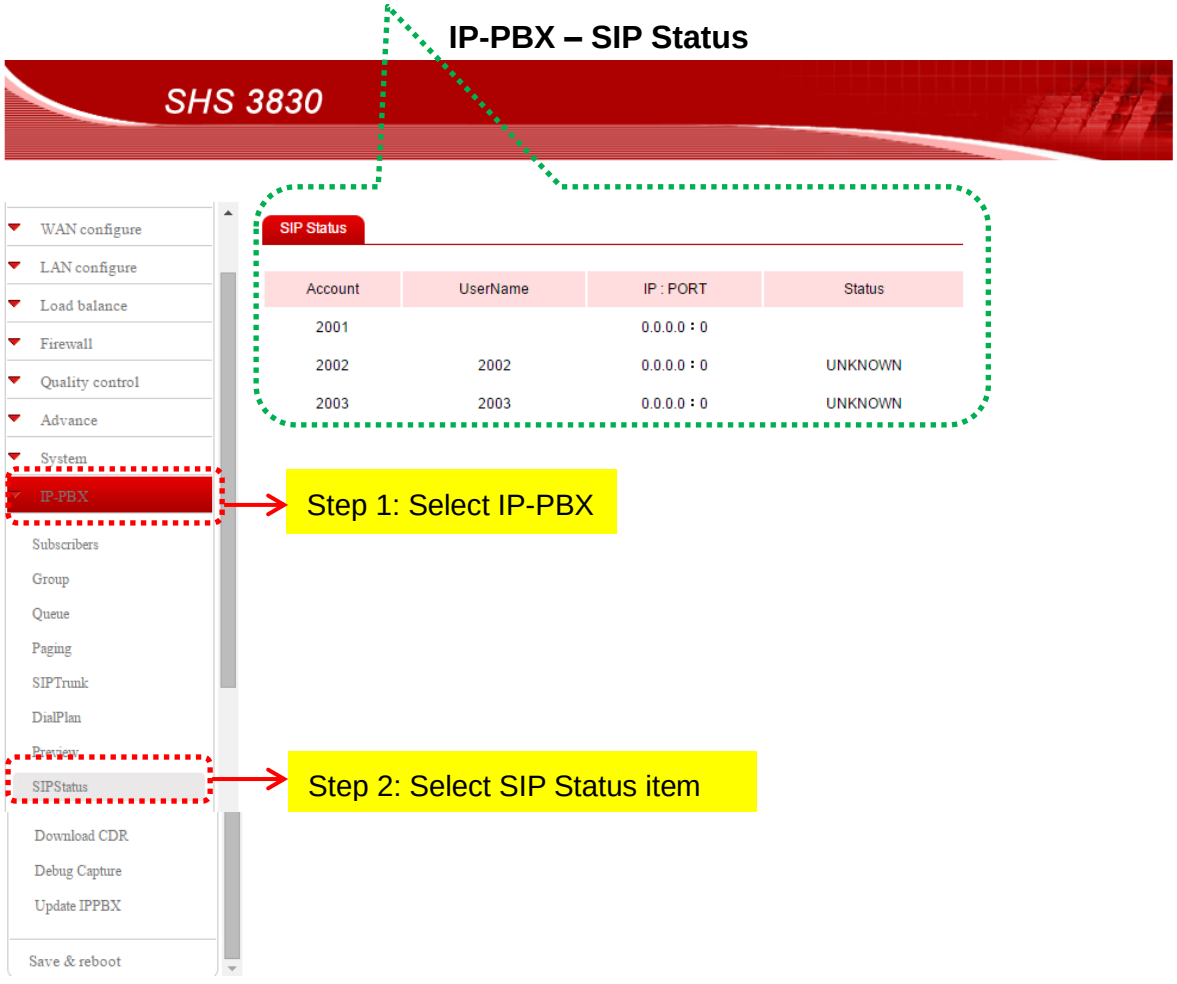
2.: all accounts (i.e. telephone number) with the first digit is 2 and include 2.

Add Front: To add assigned number before the telephone number. For example, you set 886 here and the called number is 0222221266, the SHS 3830 will add 886 then send 8860222221266 as the called number.

Add Back: To add assigned number at the end of telephone number. For example, you set 66 here and the called number is 02222212, the SHS 3830 will add 66 then send 0222221266 as the called number.

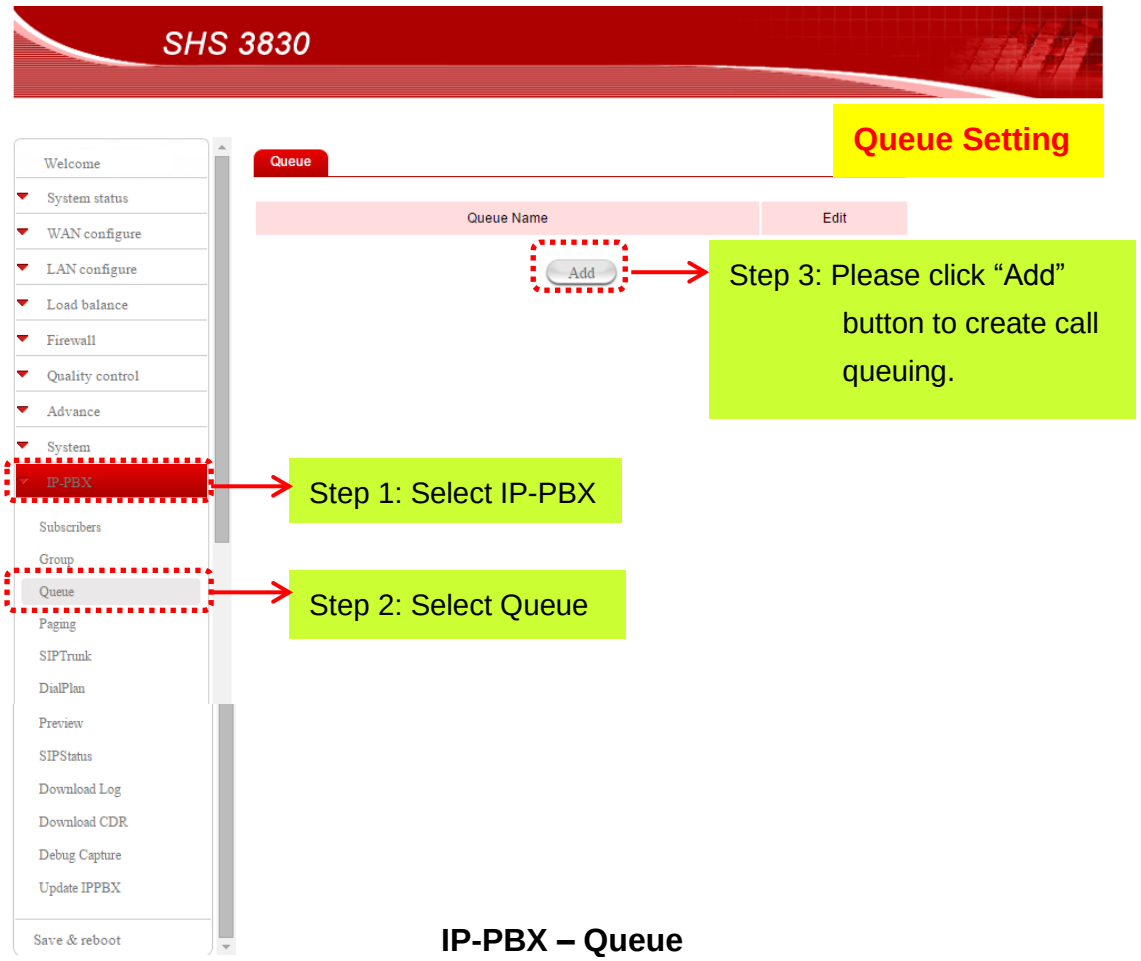
2.5.3.5 SIP status

User can select "SIP status" to look all of accounts on line.

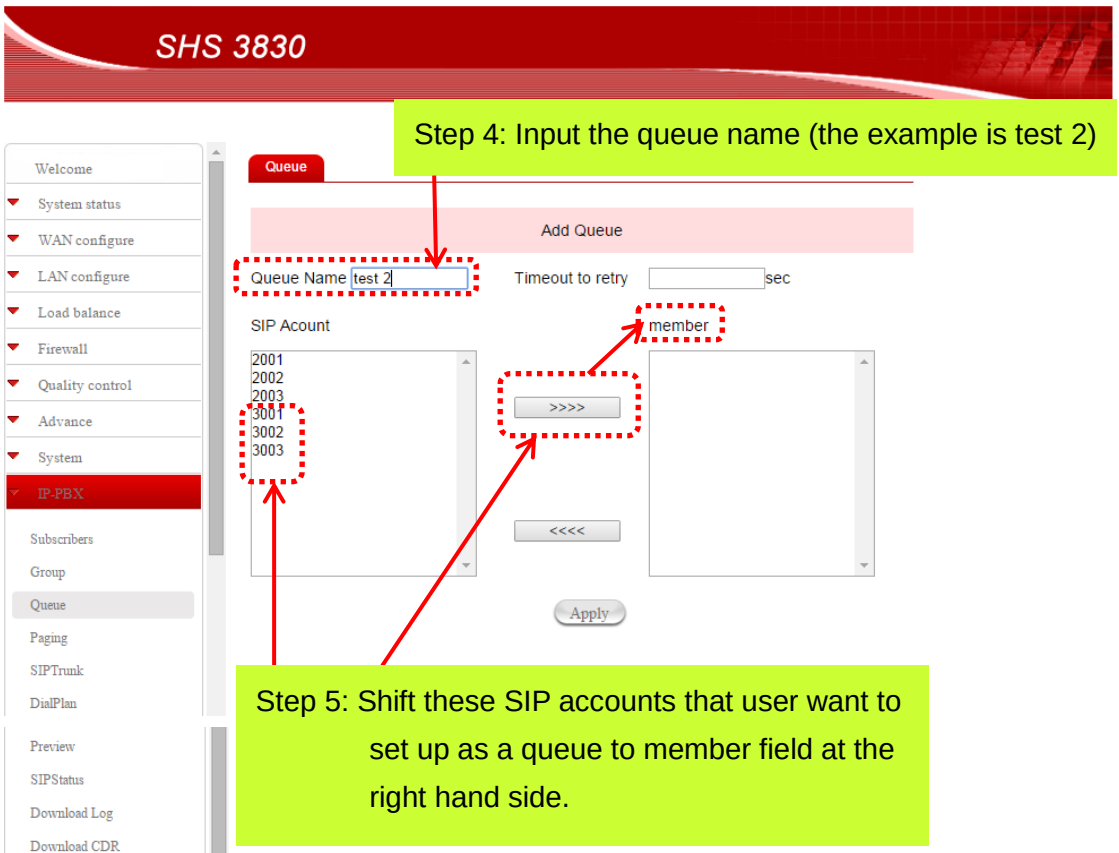


2.5.3.6 Queue

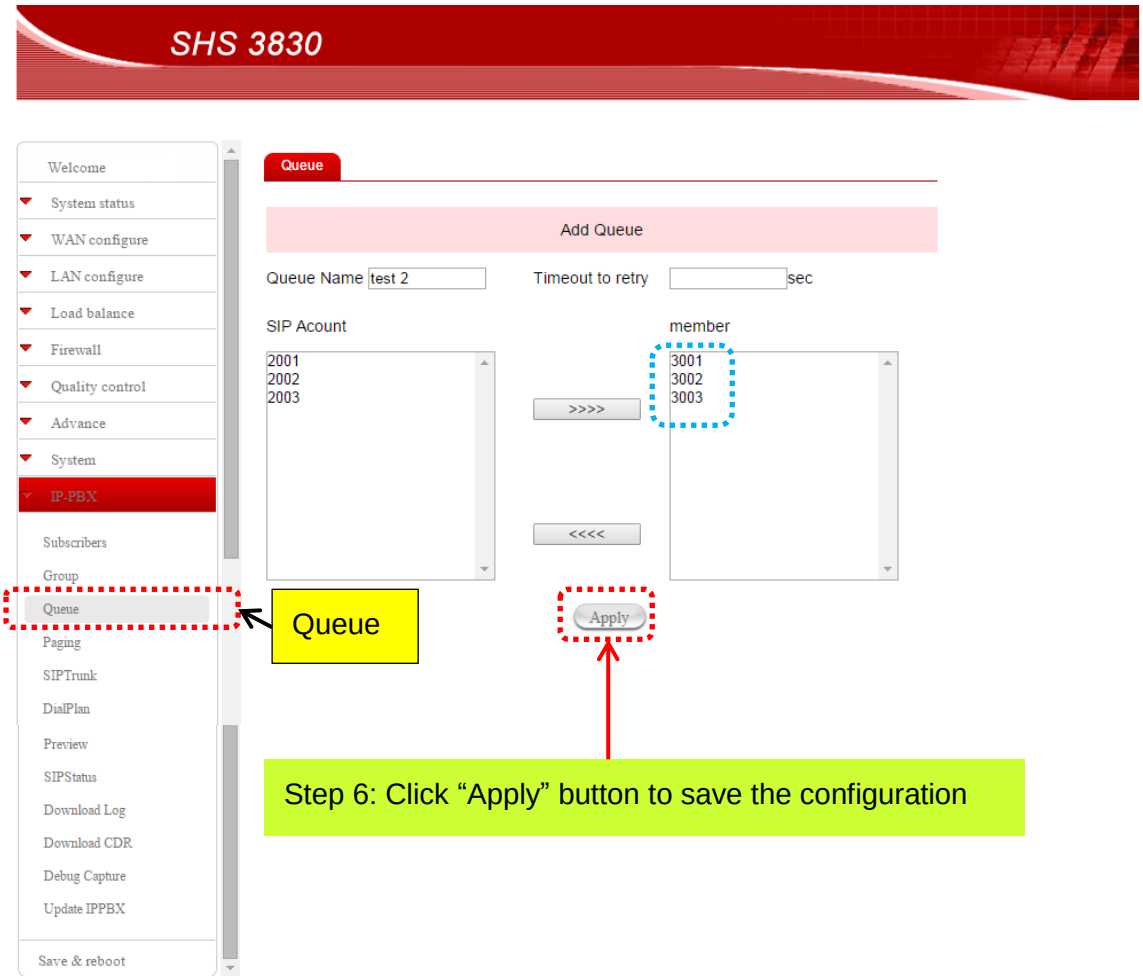
You can set up some extensions in the queue. When a call is coming, all extensions in the queue will ring together. You can pick up anyone of extensions to answer. The other extensions will hang up automatically.



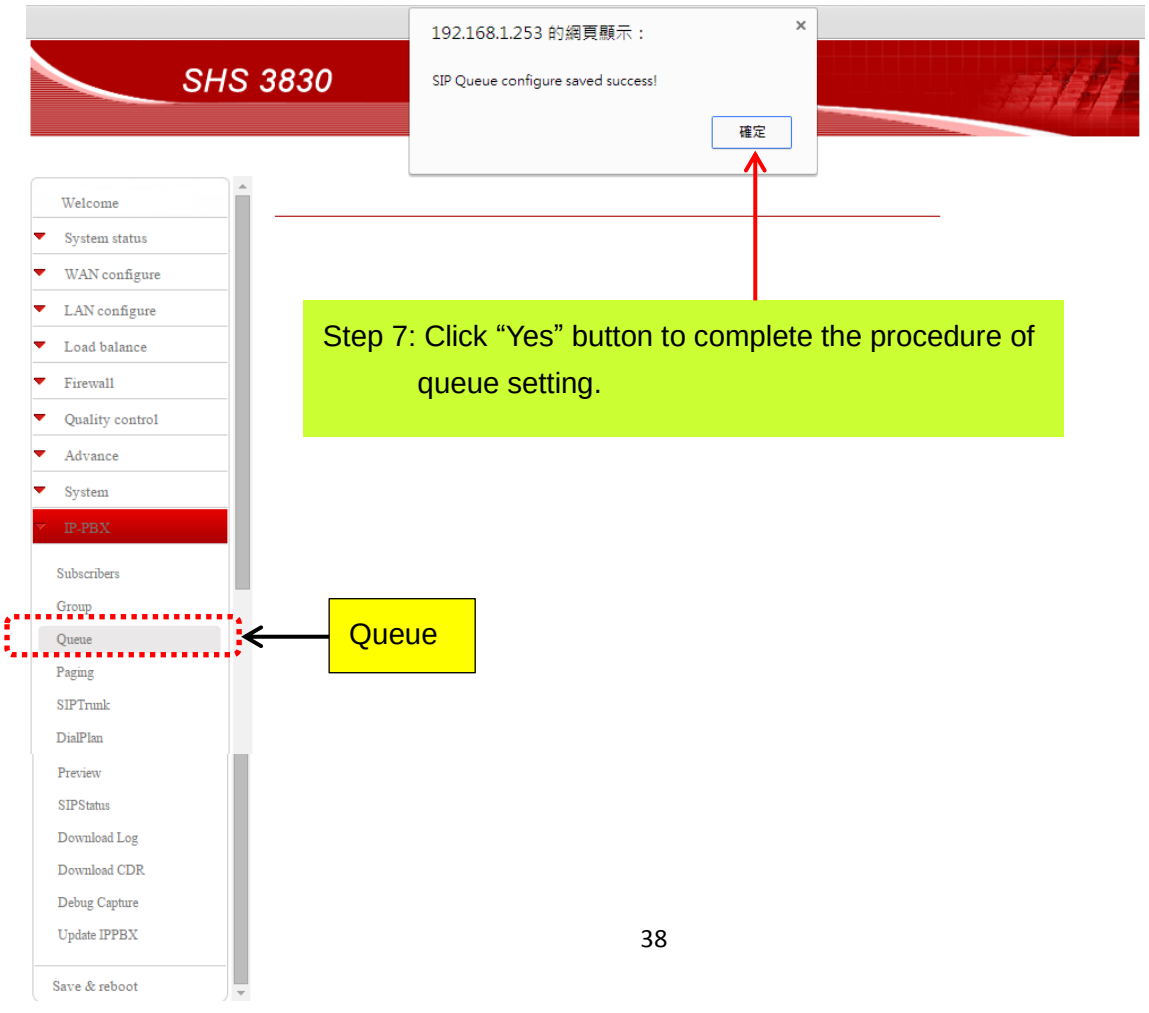
IP-PBX – Queue



Then user will see the result as below.



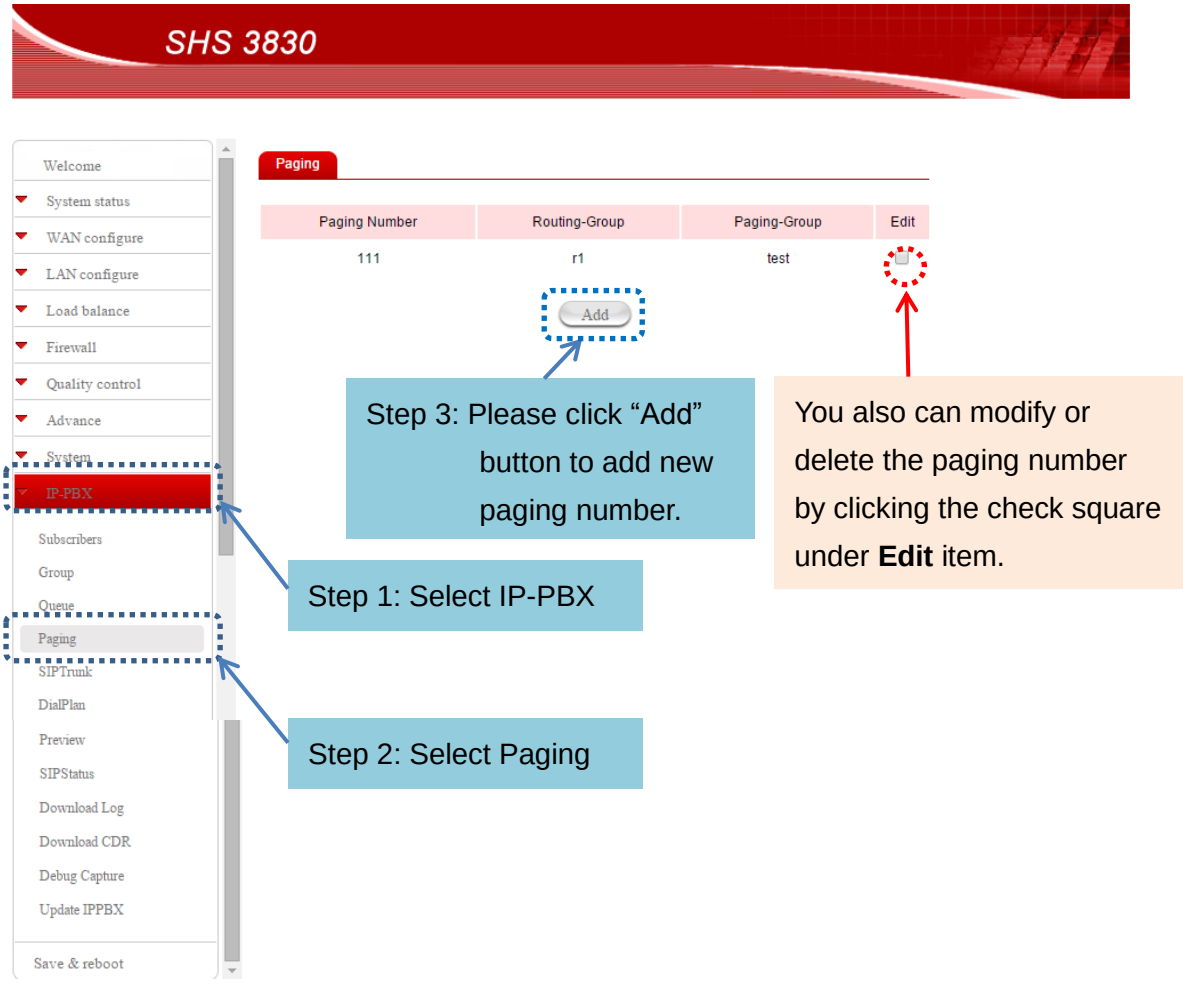
IP-PBX – Queue



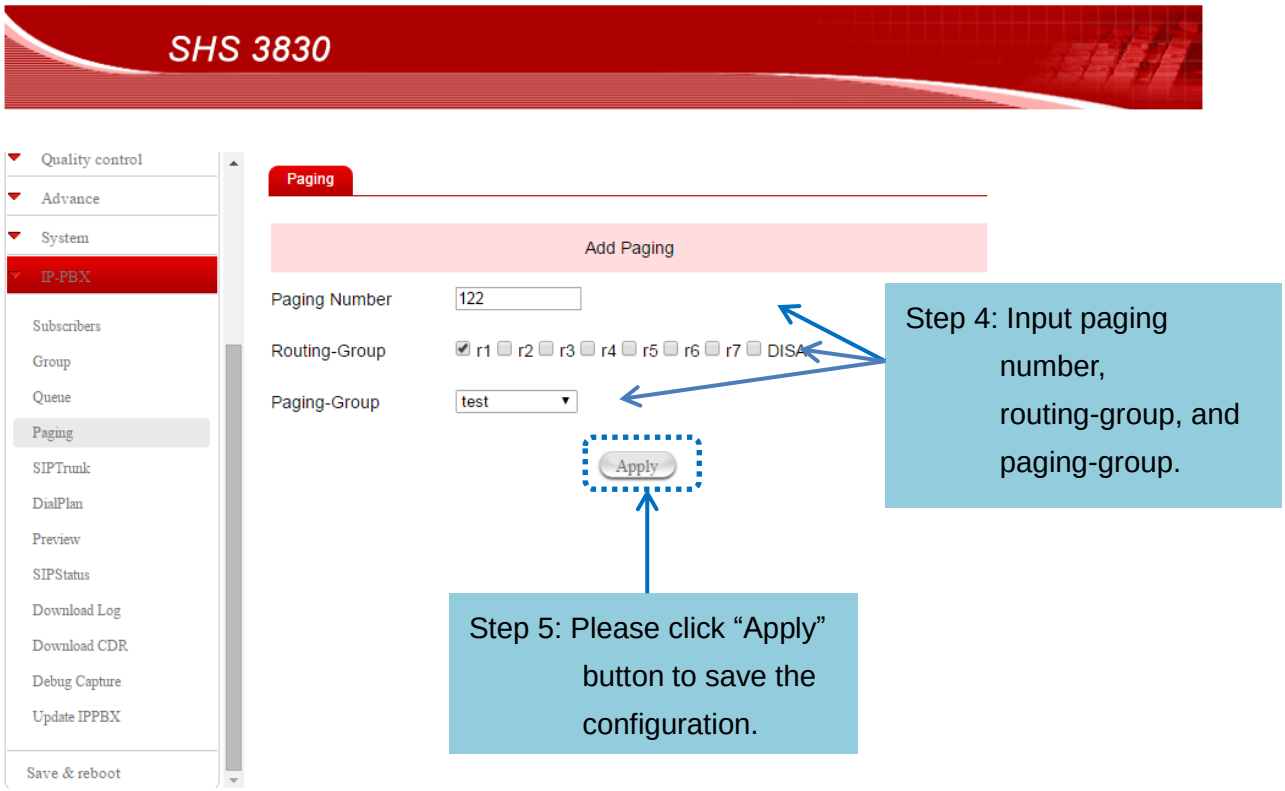
2.5.3.7 Paging

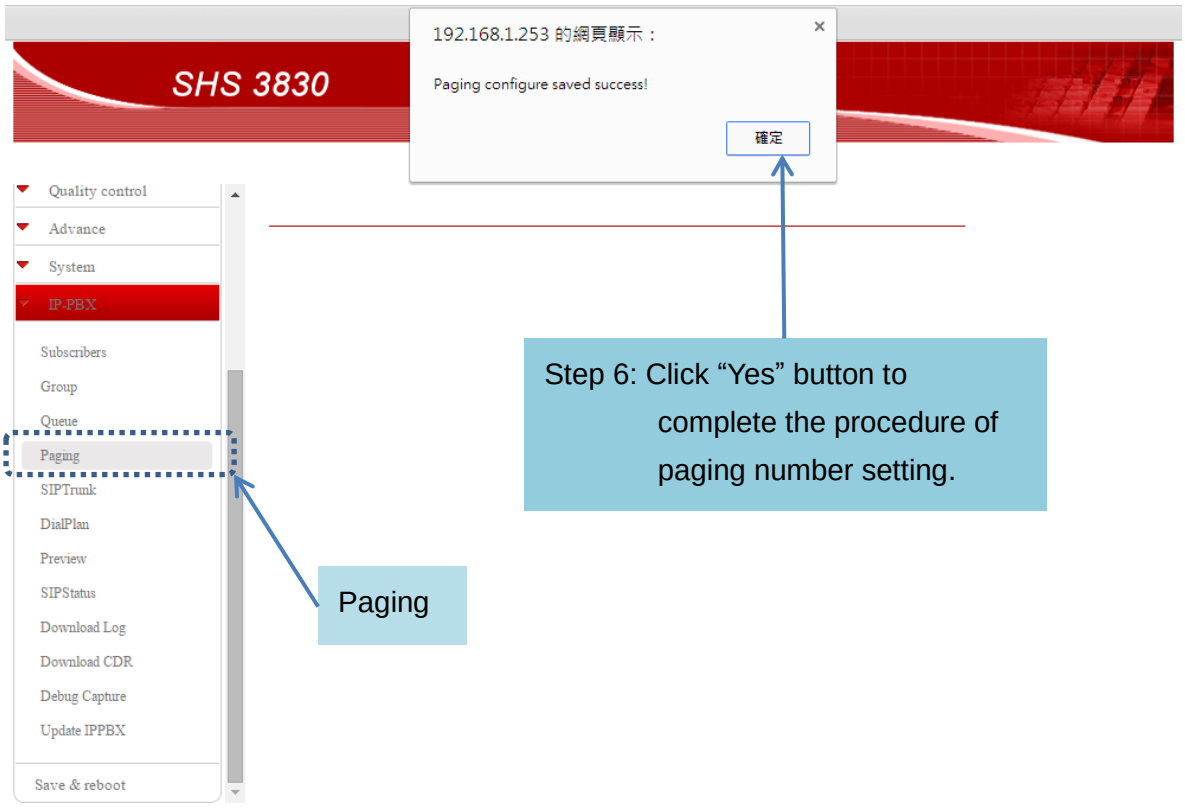
In the page item of IP-PBX menu, you can add the extension number to perform broadcast function.

IP-PBX – Paging

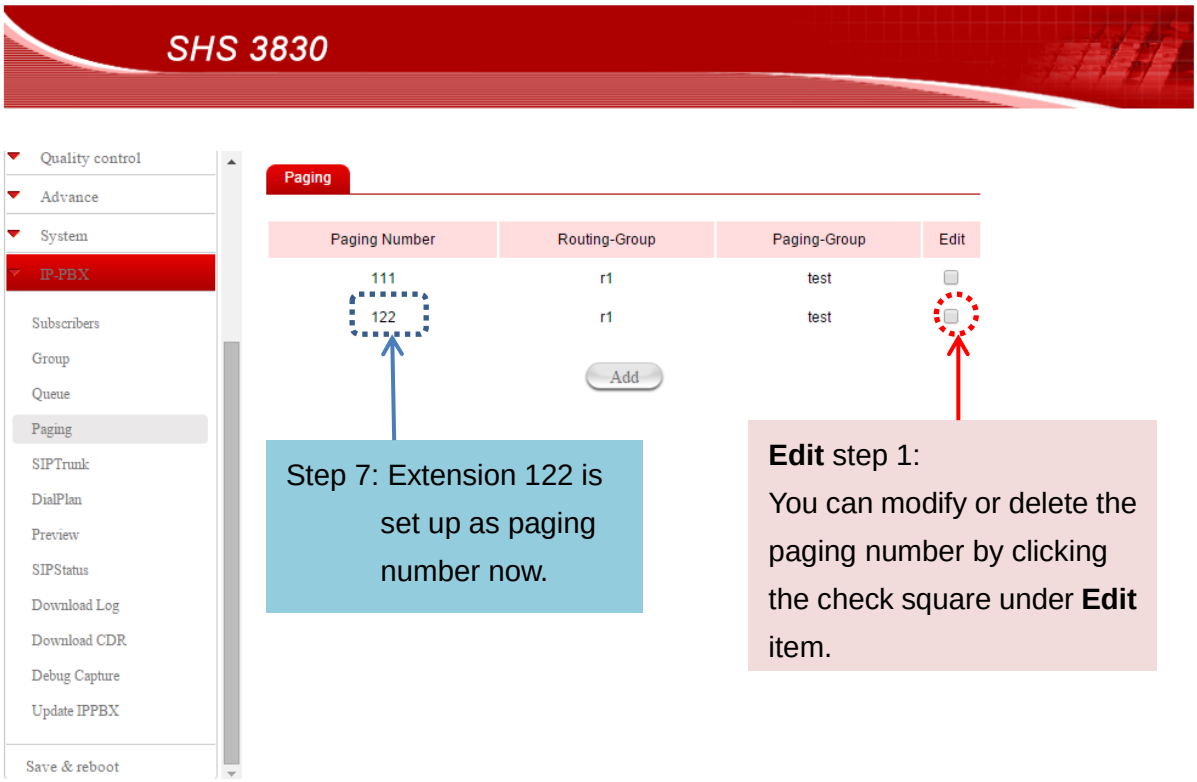


Then you will see the screen as below.



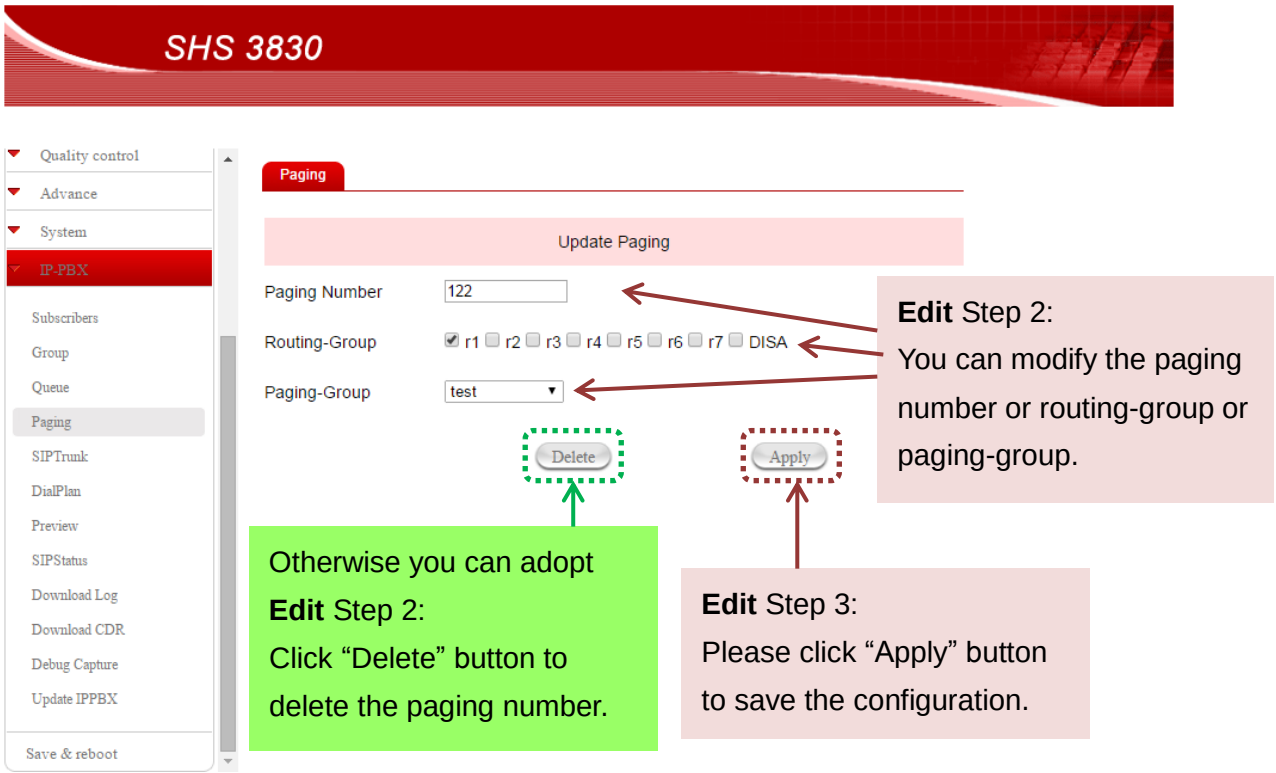


Then you will see the extension 122 set up as paging number successfully that display on the screen as below.

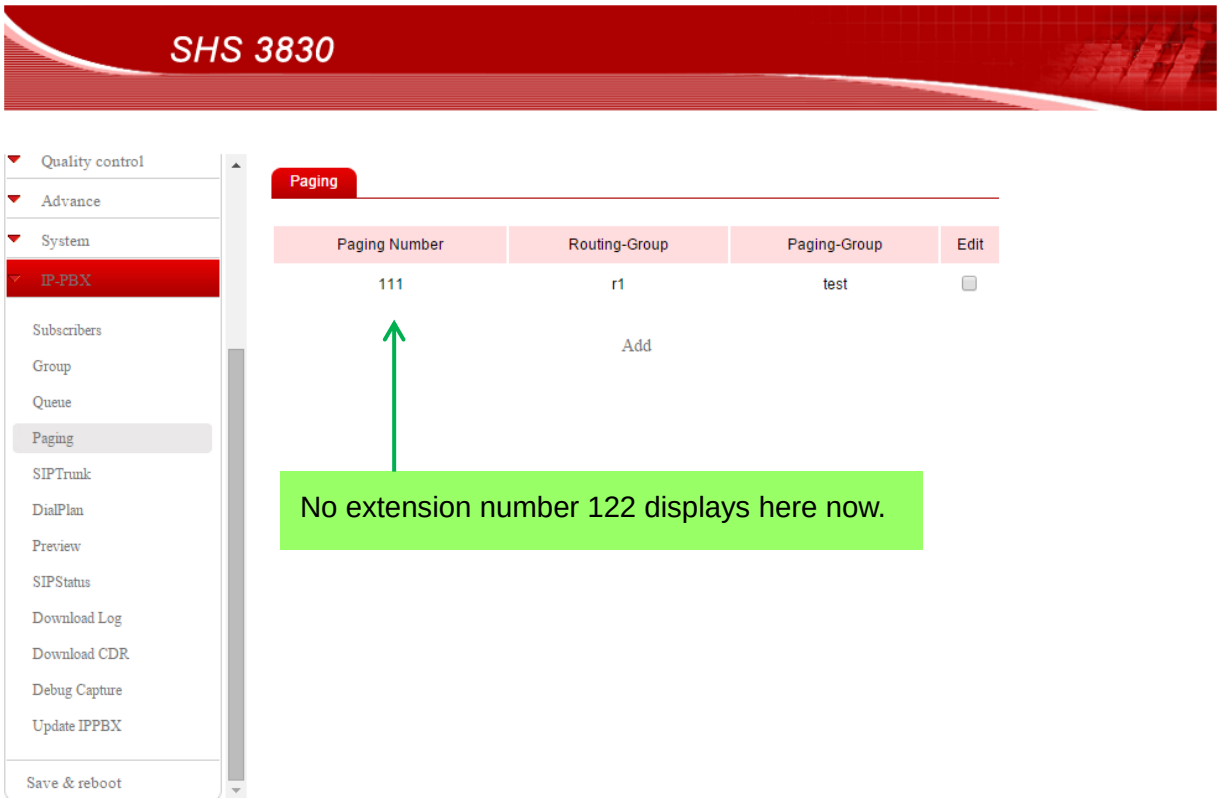


You also can modify or delete the paging number by clicking the check square under **Edit** item.

IP-PBX – Paging – Update Paging



Then you will see the extension 122 was already deleted from paging number listing



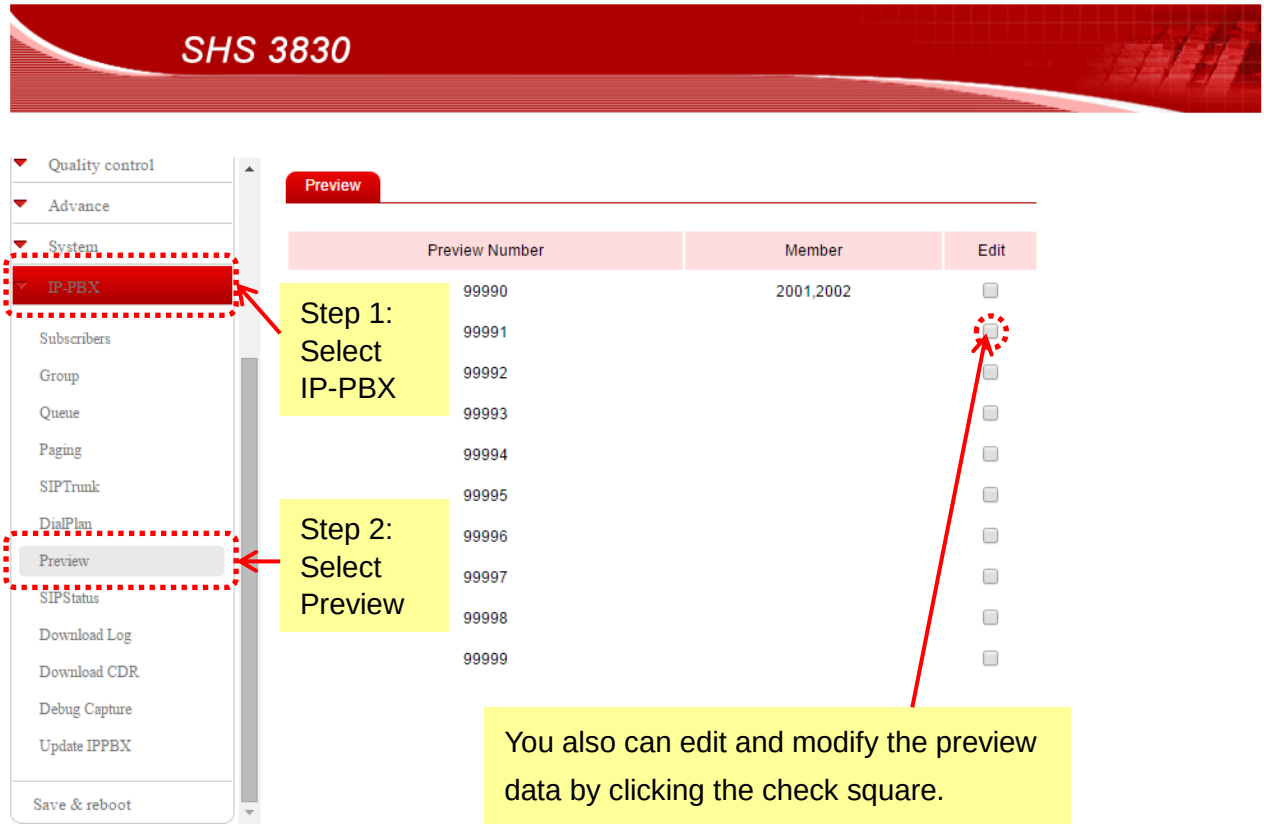
2.5.3.8 Preview

The preview function is used with IP door phone. You can arrange some

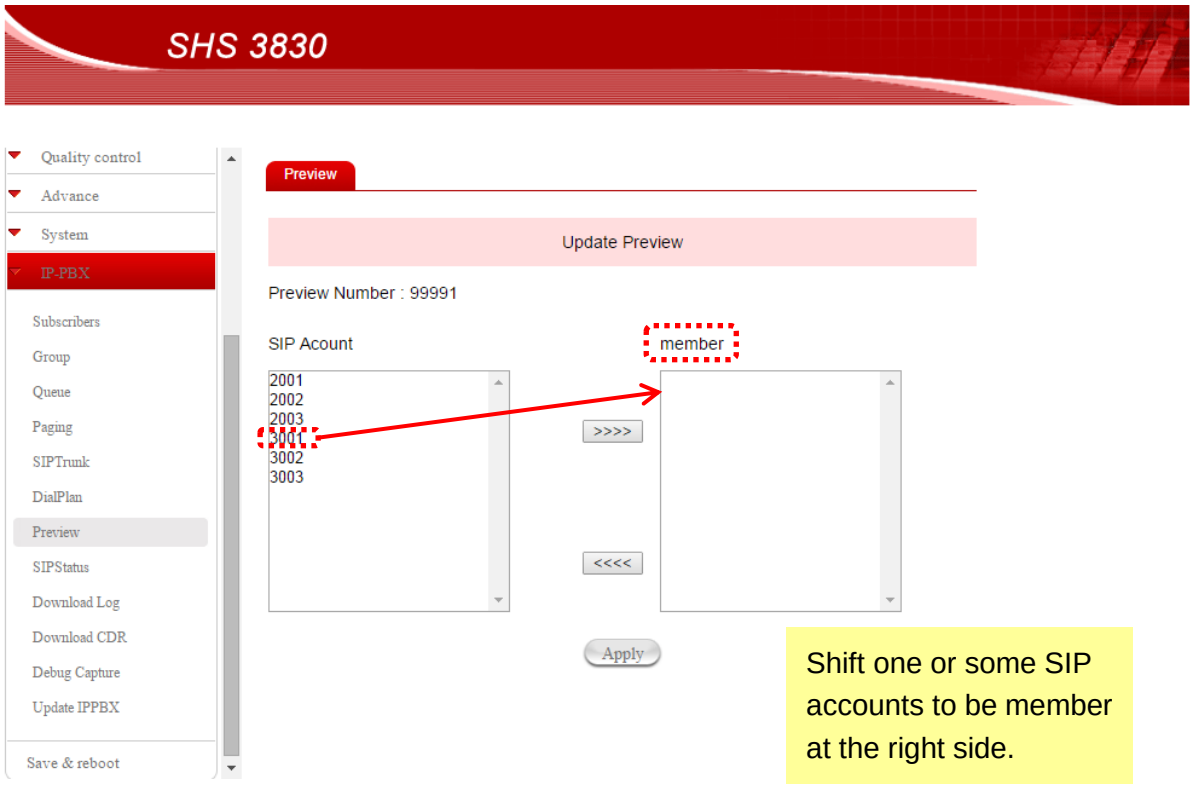
extensions as member of preview group. You need to give a preview name for a preview group. The preview name listing is shown as below diagram.

When an IP door phone dial to a preview group, all of extensions, member, will ring. And you can answer the call from IP door phone by anyone of extensions to talk the person who at your door and open the door. The other extensions will hang up automatically.

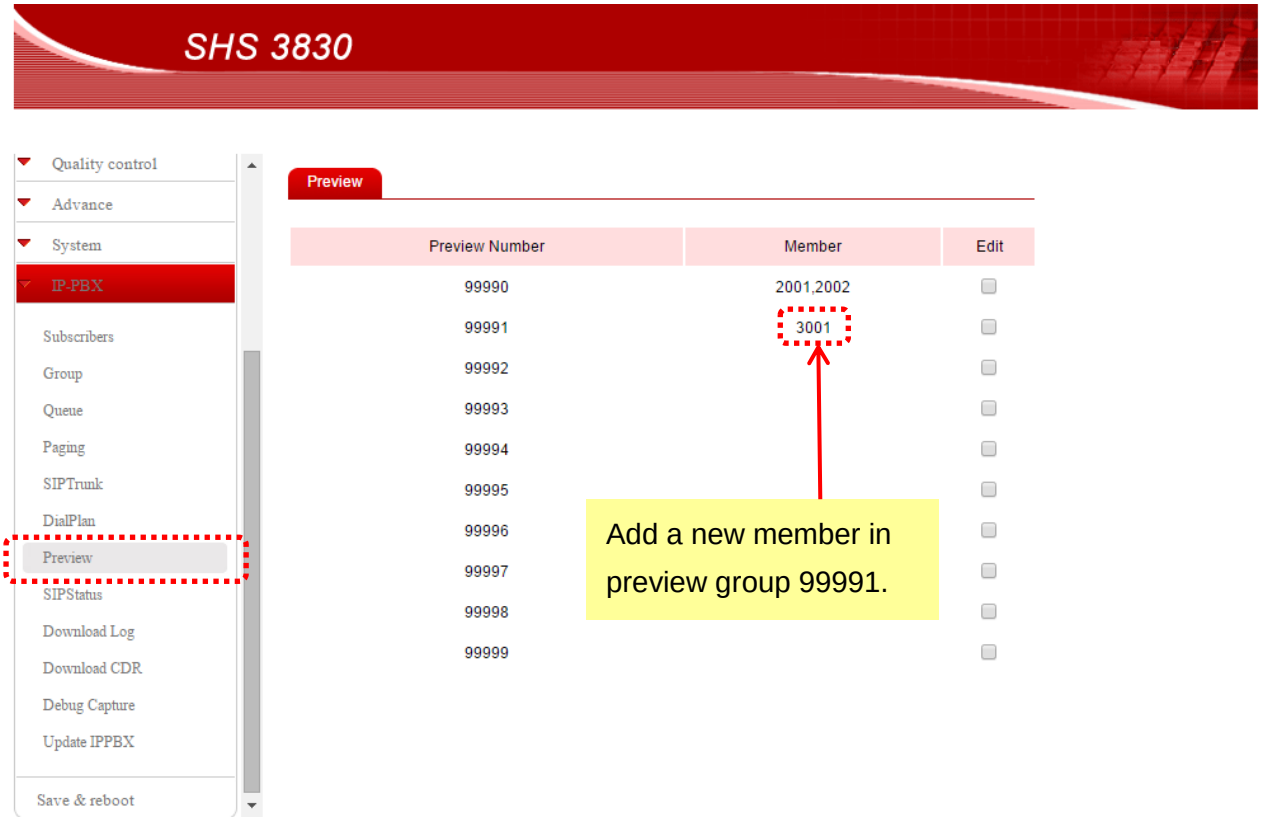
IP-PBX – Preview



IP-PBX – Preview – Update Preview



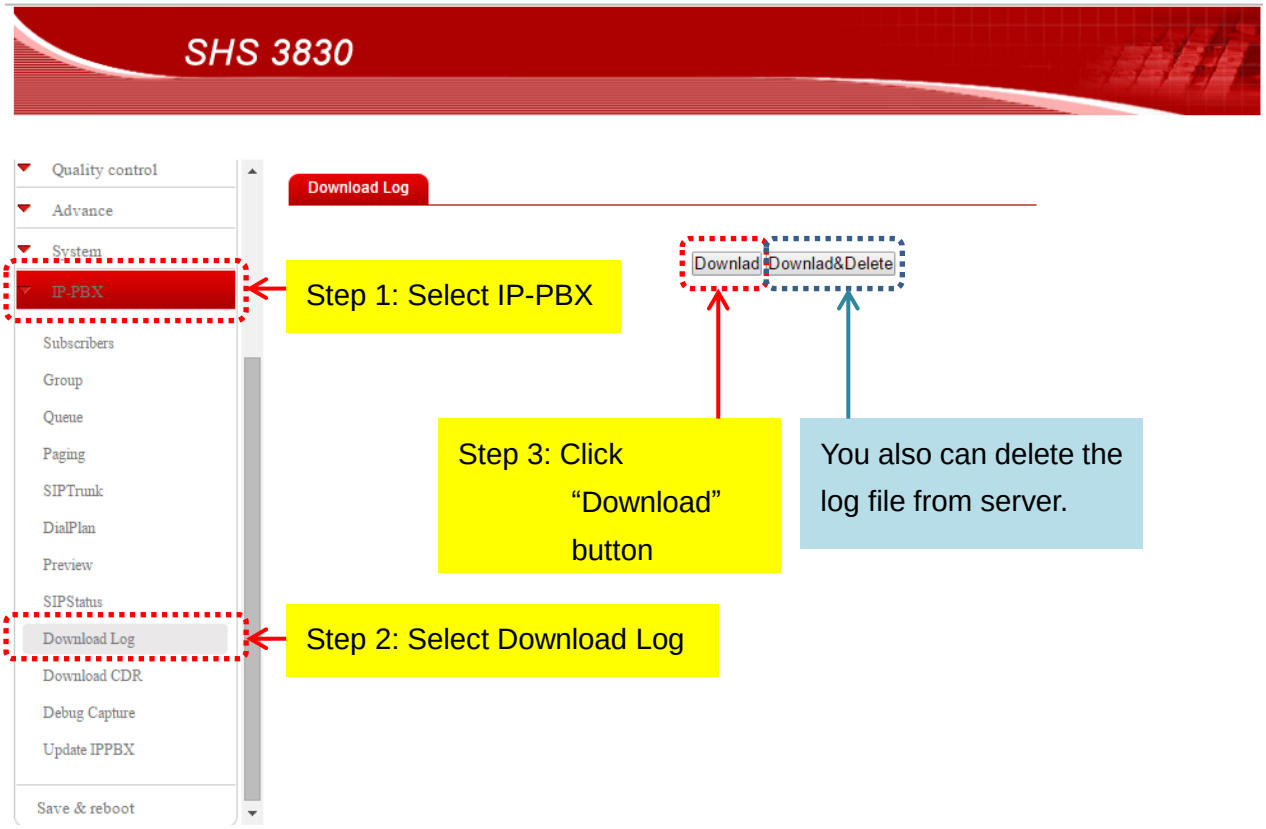
Then you will see a member 3001 already add on the screen.



2.5.3.9 Download Log

You can download the log file of system by clicking “Download” button.

IP-PBX – Download Log



The log file is shown as below for your reference. The maximum number of records is 1,000.

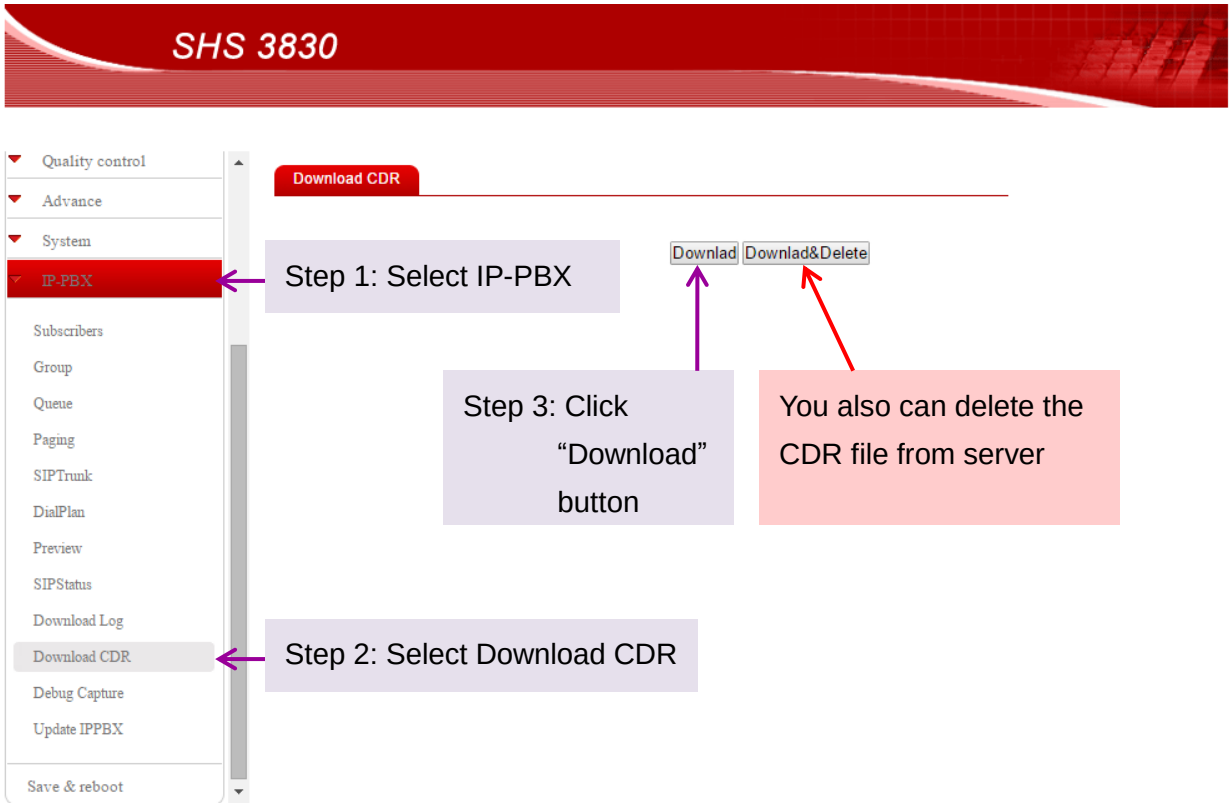
Example of System Log file

```
[Jan 31 22:25:51] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:26:51] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:26:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:27:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
[Jan 31 22:27:52] NOTICE[1772] chan_sip.c: Registration from '"2006"
<sip:2006@192.168.1.253>' failed for '192.168.1.249:5060' - No matching peer
found
```

2.5.3.10 Download CDR

You can download the Call Detail Record file by clicking “Download” button.

IP-PBX – Download CDR



The CDR file is shown as below for your reference. The maximum number of CDR records is 1,000.

Example of CDR file

Caller ID	Callee ID	Source SIP ID	Destination SIP ID	Command		Start time	Answer time
2001 s-BUSY DialState	2001	SIP/2002-00000010	SIP/2002-00000011	Hangup		2/1/70 21:56	
2001 2002 r1	2001	SIP/2001-00000012	SIP/2002-00000013	Dial	SIP/2002,,rtTk	2/1/70 22:00	2/1/70 22:00
2001 s-BUSY DialState	2001	SIP/2002-00000014	SIP/2001-00000015	Hangup		2/1/70 22:00	
2001 2002 r1	2001	SIP/2001-00000016	SIP/2002-00000017	Dial	SIP/2002,,rtTk	2/1/70 22:01	2/1/70 22:01
2002 2001 r1	2002	SIP/2002-00000018	SIP/2001-00000019	Dial	SIP/2001,,rtTk	2/1/70 22:01	2/1/70 22:01
2002 2001 r1	2002	SIP/2002-0000001a	SIP/2001-0000001b	Dial	SIP/2001,,rtTk	2/1/70 22:09	2/1/70 22:09

Start time	Answer time	End time	Duration	Billsec	Status		
2/1/70 21:56		2/1/70 21:56	0	0	BUSY	DOCUMENTATION	2757373.16
2/1/70 22:00	2/1/70 22:00	2/1/70 22:00	10	7	ANSWERED	DOCUMENTATION	2757628.18
2/1/70 22:00		2/1/70 22:00	0	0	BUSY	DOCUMENTATION	2757646.2
2/1/70 22:01	2/1/70 22:01	2/1/70 22:01	6	3	ANSWERED	DOCUMENTATION	2757667.22
2/1/70 22:01	2/1/70 22:01	2/1/70 22:01	9	2	ANSWERED	DOCUMENTATION	2757690.24
2/1/70 22:09	2/1/70 22:09	2/1/70 22:09	24	15	ANSWERED	DOCUMENTATION	2758146.26

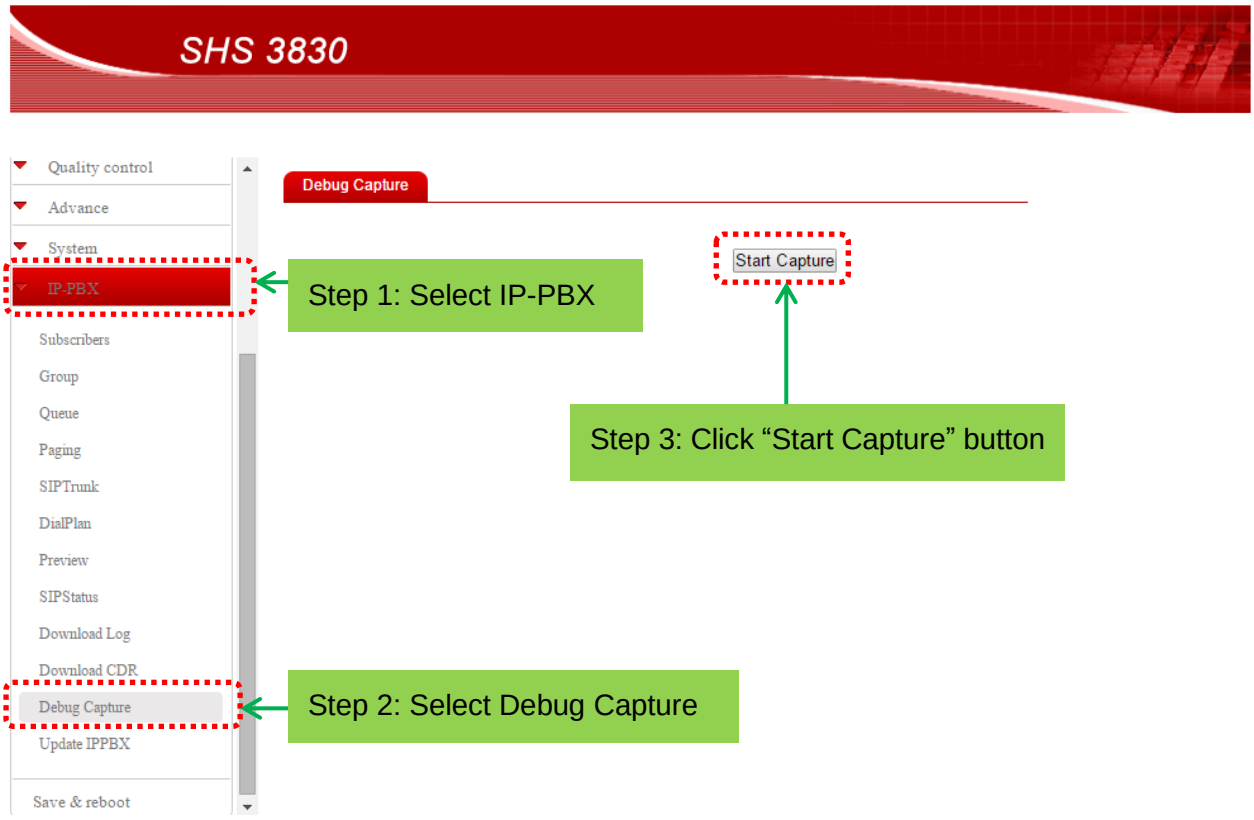
2.5.3.11 Debug Capture

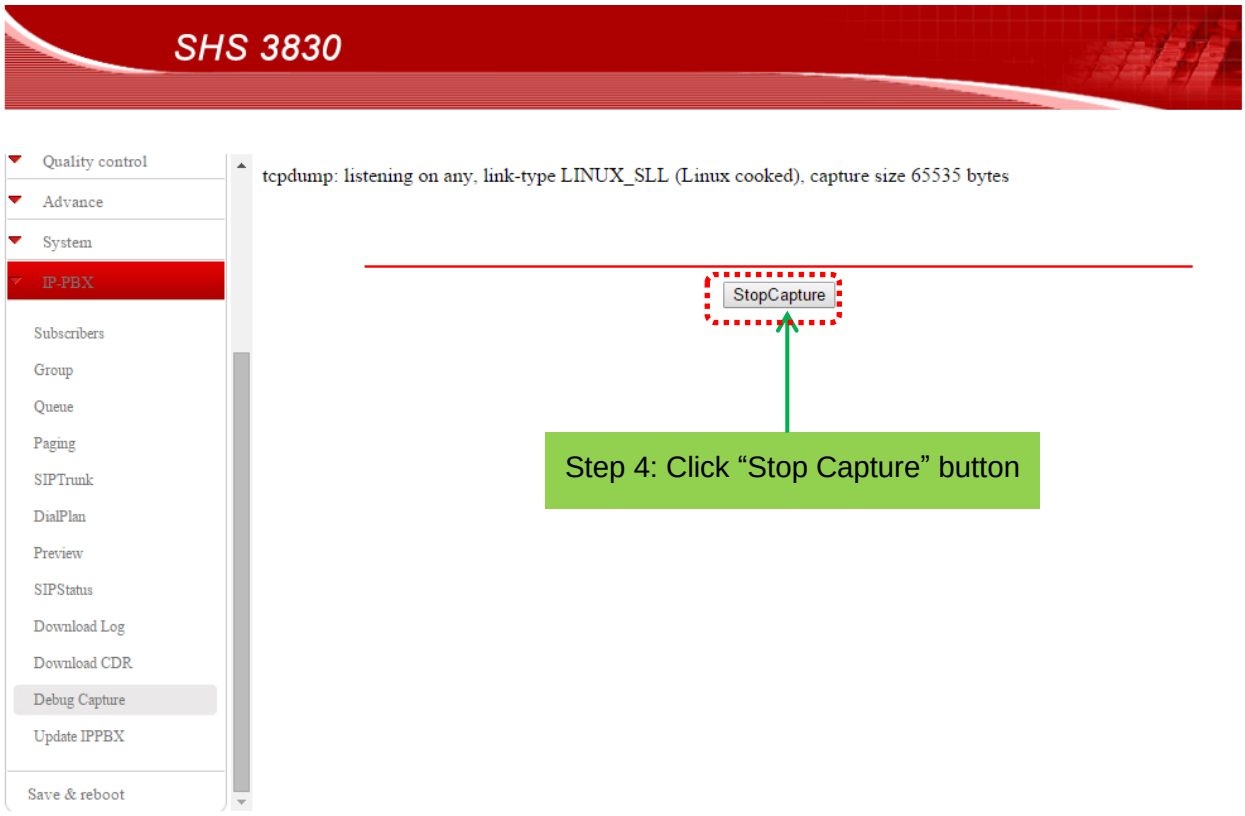
When you have finished the configuration of SHS 3830 but the IP-PBX can NOT work smoothly or you get trouble in the usage of SHS 3830. Please select the function of Debug Capture to download the capture file for the network packet analysis and troubleshooting.

The capture file will be open and read by **Wireshark** software package. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting and analysis. You can free download from website www.wireshark.org.

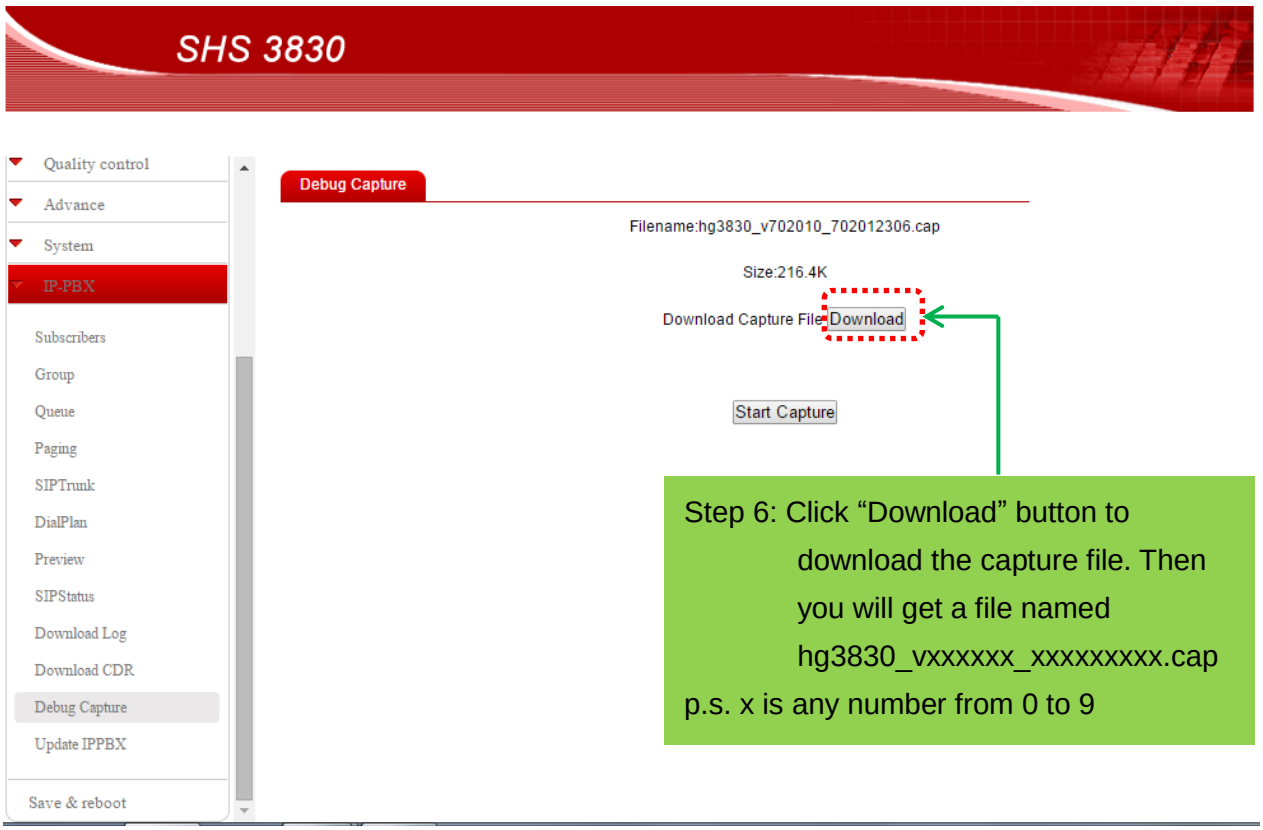
Following diagrams will tell you how to download the capture file step by step.

IP-PBX – Debug Capture





Step 5: Click “Yes” button to confirm the capture file is complete.



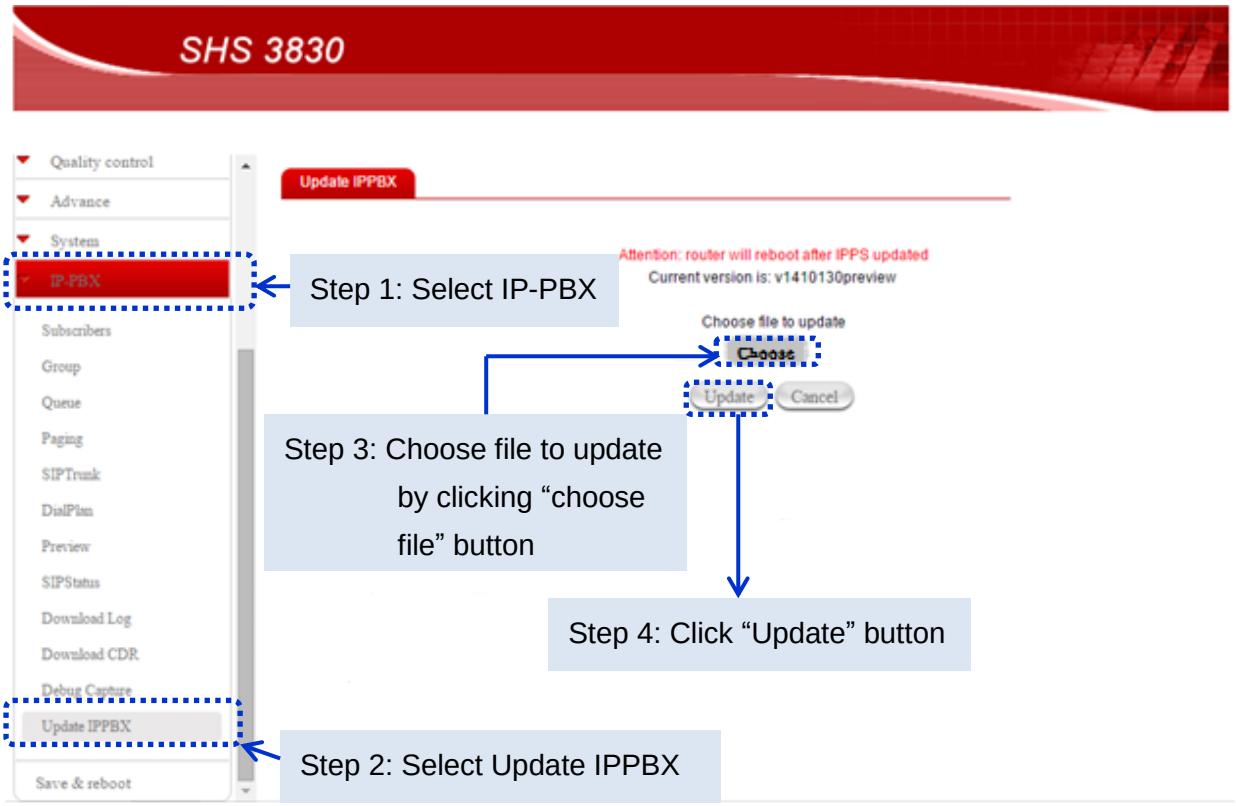
Step 6: Click “Download” button to download the capture file. Then you will get a file named hg3830_vxxxxxx_xxxxxxxxx.cap

p.s. x is any number from 0 to 9

2.5.3.12 Update IPPBX

You can update your SHS 3830 IP-PBX by clicking “Update IPPBX” in the main menu of IP-PBX as described below.

IP-PBX – Update IPPBX



Chapter 3 Web configuration for Router functions

3.1 System status

3.1.1 Link status

You can get the following information in **Link status** window

- LAN Status,
- WAN Status,
- Firmware Version

LAN Status: Shows the information of MAC Address, IP Address, Subnet Mask and DHCP Status (Enable/Disable).

WAN Status: Shows the information of MAC Address, IP Address, and Subnet Mask on each or all WAN ports

Firmware version: version of software and its released date.

System status - Link status

3.1.2 Data monitor

Differ from “Link status”, “Data monitor” indicates detailed packets transmitted and received status and system status at the moment.

System status

CPU usage / Memory usage / Live time

Packet transfer status

Current Session / TCP Session / UDP Session / Accumulative Session

Bandwidth

Current Bandwidth / Download Speed / Upload Speed

Load Balance

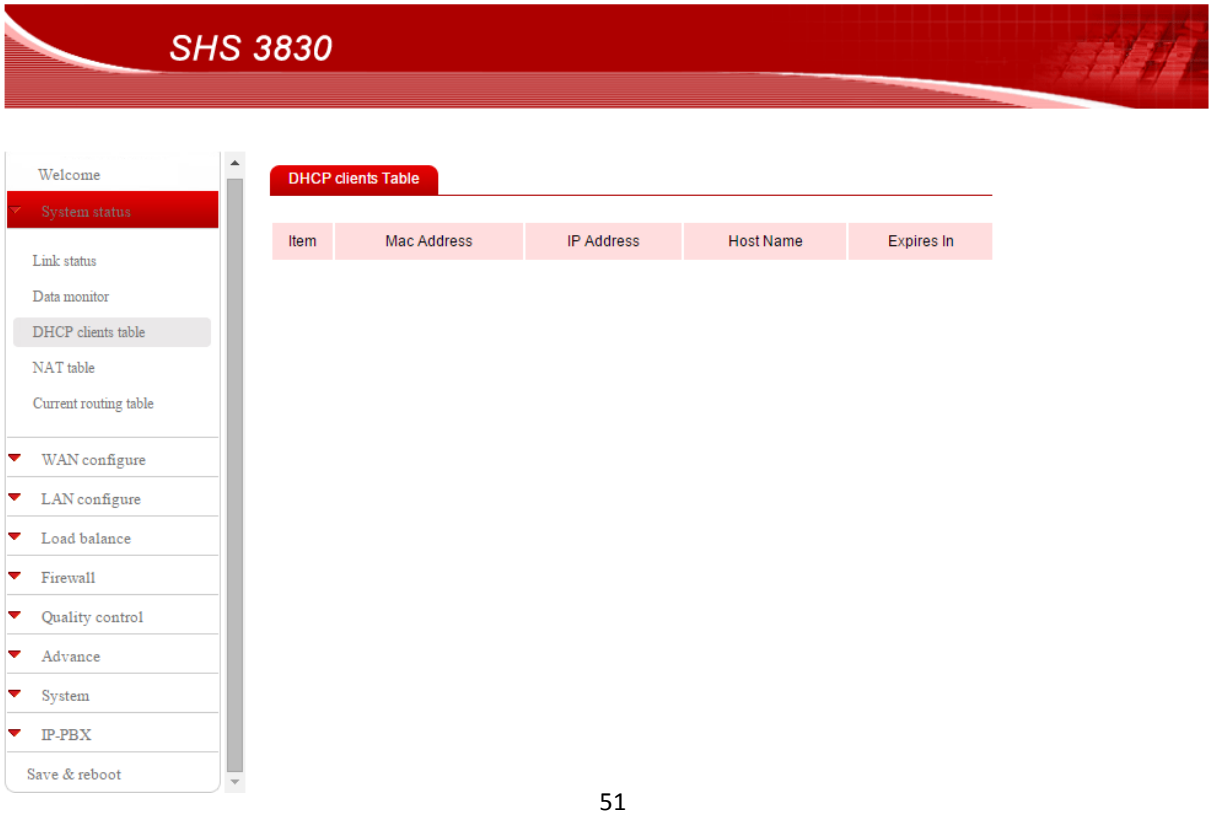
Load balance / Byte Received / Byte Transmitted / Total Bytes

System status - Data monitor

3.1.3 DHCP Clients table

You can get the detail information of DHCP clients in following window.

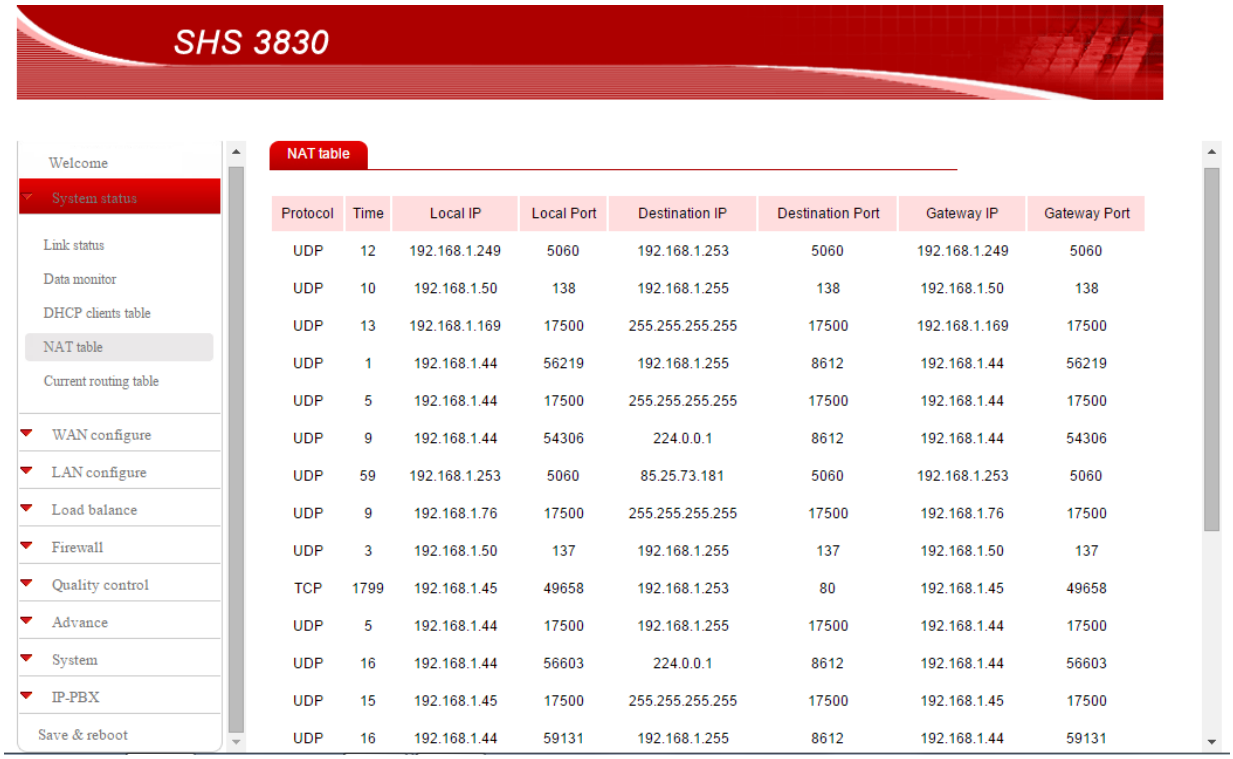
System status – DHCP Clients table



3.1.4 NAT table

Display NAT (Network Address Translation) sessions occurred at the moment in router. NAT is widely implemented in router in order to resolve not sufficient IPs in IPv4, and functions as IP translation between public IP and private IP. Time means life time for each session type while session active.

System status – NAT table

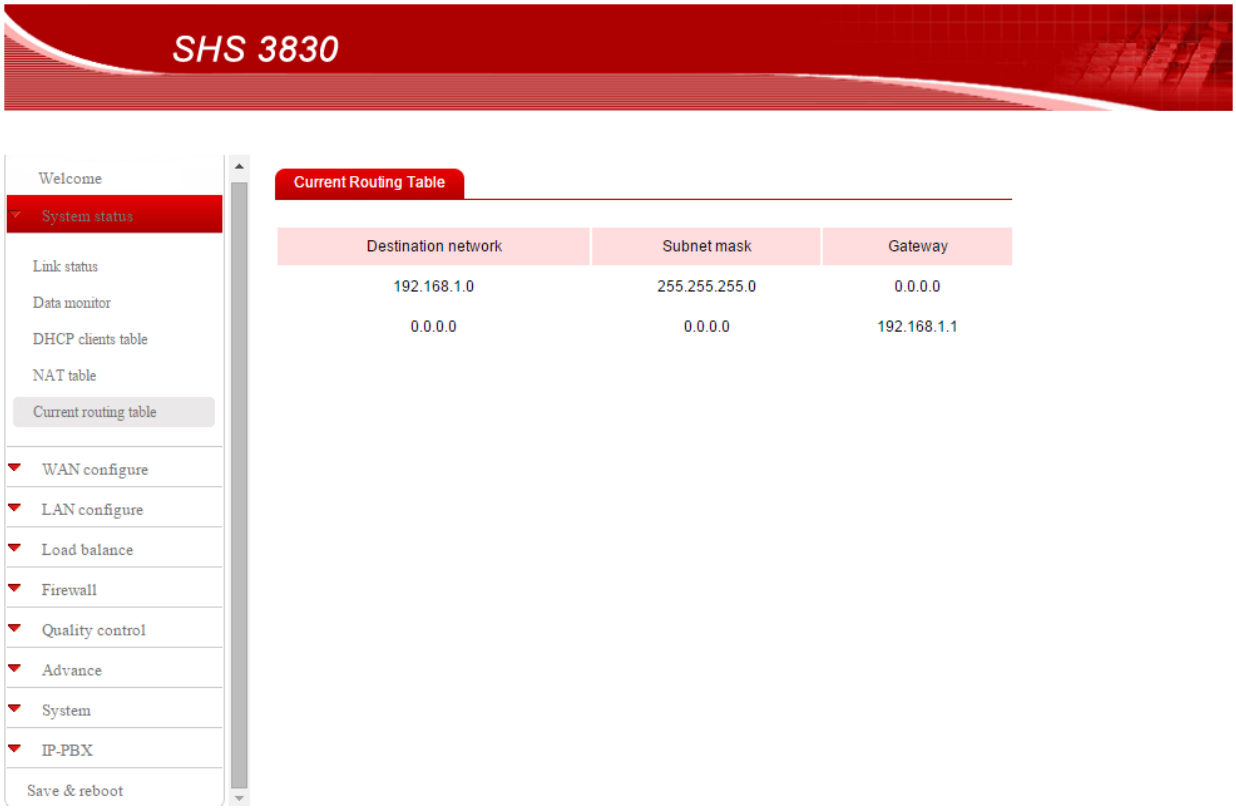


Protocol	Time	Local IP	Local Port	Destination IP	Destination Port	Gateway IP	Gateway Port
UDP	12	192.168.1.249	5060	192.168.1.253	5060	192.168.1.249	5060
UDP	10	192.168.1.50	138	192.168.1.255	138	192.168.1.50	138
UDP	13	192.168.1.169	17500	255.255.255.255	17500	192.168.1.169	17500
UDP	1	192.168.1.44	56219	192.168.1.255	8612	192.168.1.44	56219
UDP	5	192.168.1.44	17500	255.255.255.255	17500	192.168.1.44	17500
UDP	9	192.168.1.44	54306	224.0.0.1	8612	192.168.1.44	54306
UDP	59	192.168.1.253	5060	85.25.73.181	5060	192.168.1.253	5060
UDP	9	192.168.1.76	17500	255.255.255.255	17500	192.168.1.76	17500
UDP	3	192.168.1.50	137	192.168.1.255	137	192.168.1.50	137
TCP	1799	192.168.1.45	49658	192.168.1.253	80	192.168.1.45	49658
UDP	5	192.168.1.44	17500	192.168.1.255	17500	192.168.1.44	17500
UDP	16	192.168.1.44	56603	224.0.0.1	8612	192.168.1.44	56603
UDP	15	192.168.1.45	17500	255.255.255.255	17500	192.168.1.45	17500
UDP	16	192.168.1.44	59131	192.168.1.255	8612	192.168.1.44	59131

3.1.5 Current routing table

This display shows the valid routing paths in router. Users can view the information about current routing paths.

System status – Current touting table



3.2 Load balance

3.2.1 Outbound

Load Balance Router provides two load balance work modes:

Session	All the enabled WAN ports have the same (1:1) bandwidth rate.
Weight round robin	Configure the WAN ports bandwidth rate manually.

Session mode:

When choose this mode, the router will assign each coming session to each WAN port one by one, no matter how traffic loading on each WAN port.

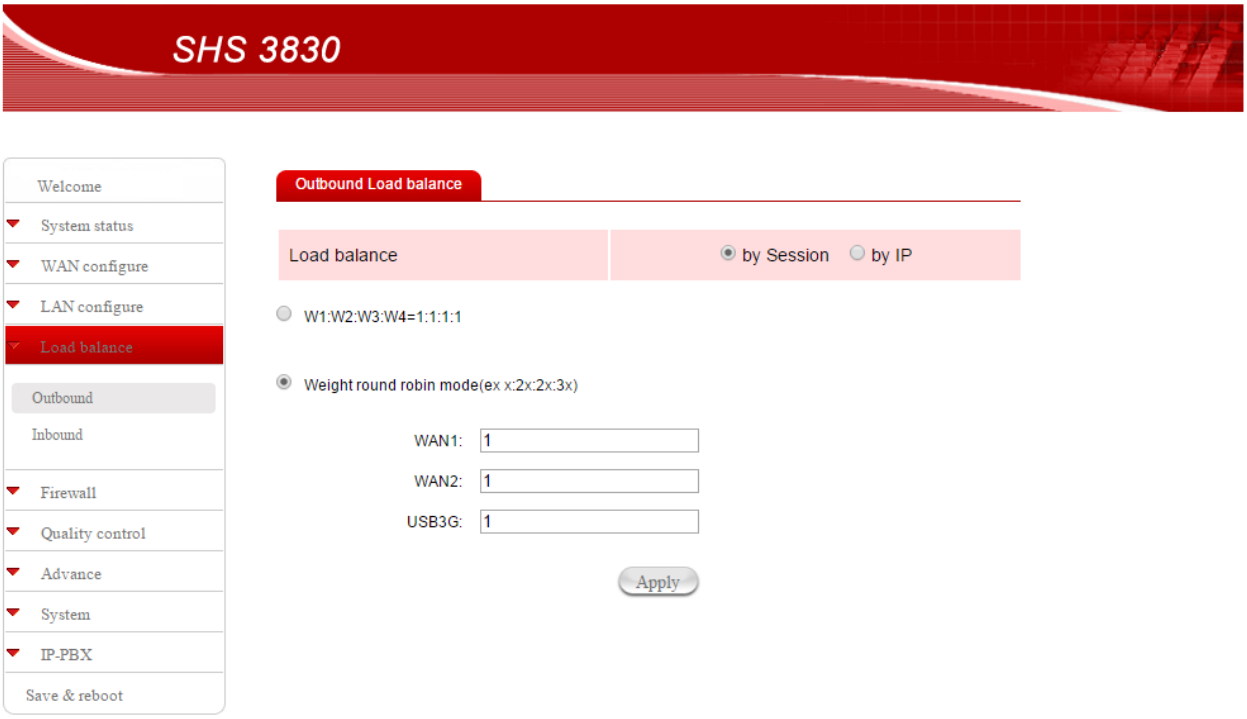
LOAD BALANCE – Outbound (1)

Weight Round Robin mode:

Configure the WAN ports bandwidth rate manually, means you can distribute each coming session from users to each WAN port, following the rate that you assign in each WAN port.

The session number in each WAN can be numbered from **1 to 100**, the suggest number is under 1 ~10. If rate is 1:1 for each WAN port, the router function will act like Session mode

LOAD BALANCE – Outbound (2)



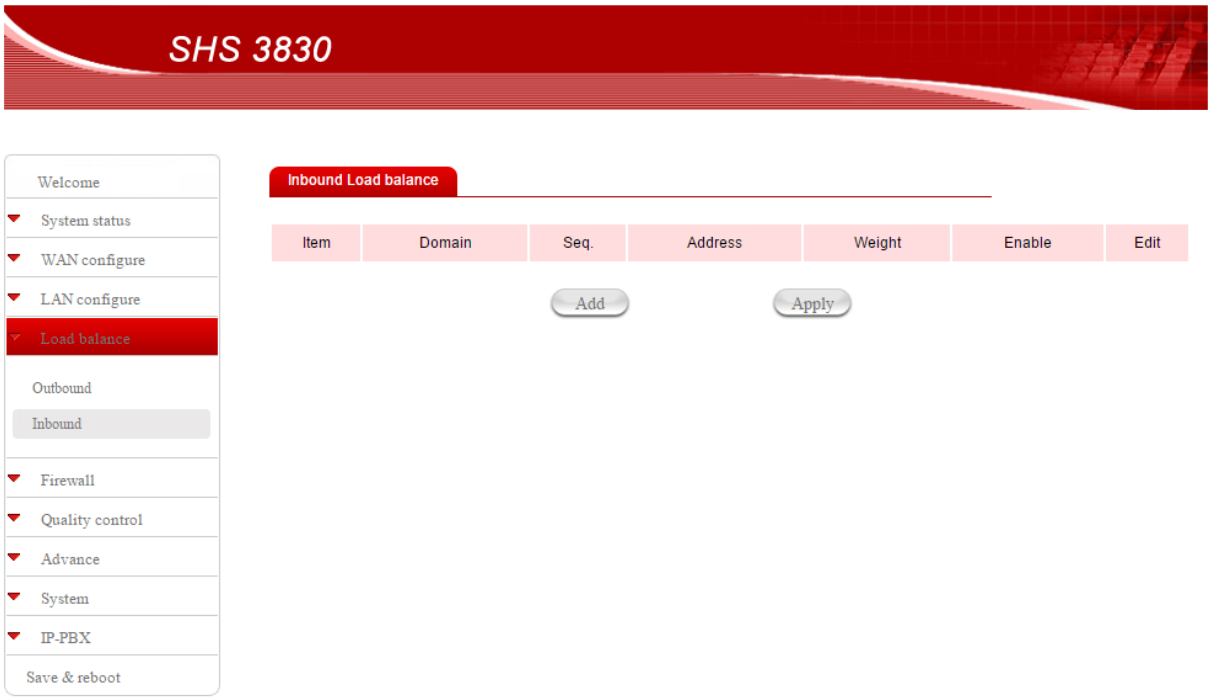
3.2.2 Inbound

Inbound function allows incoming traffic to be allocated by inbound load balance policy so that increasingly all broadband bandwidth usage and balancing load among connected lines. Refer to Chapter 4 for more information.

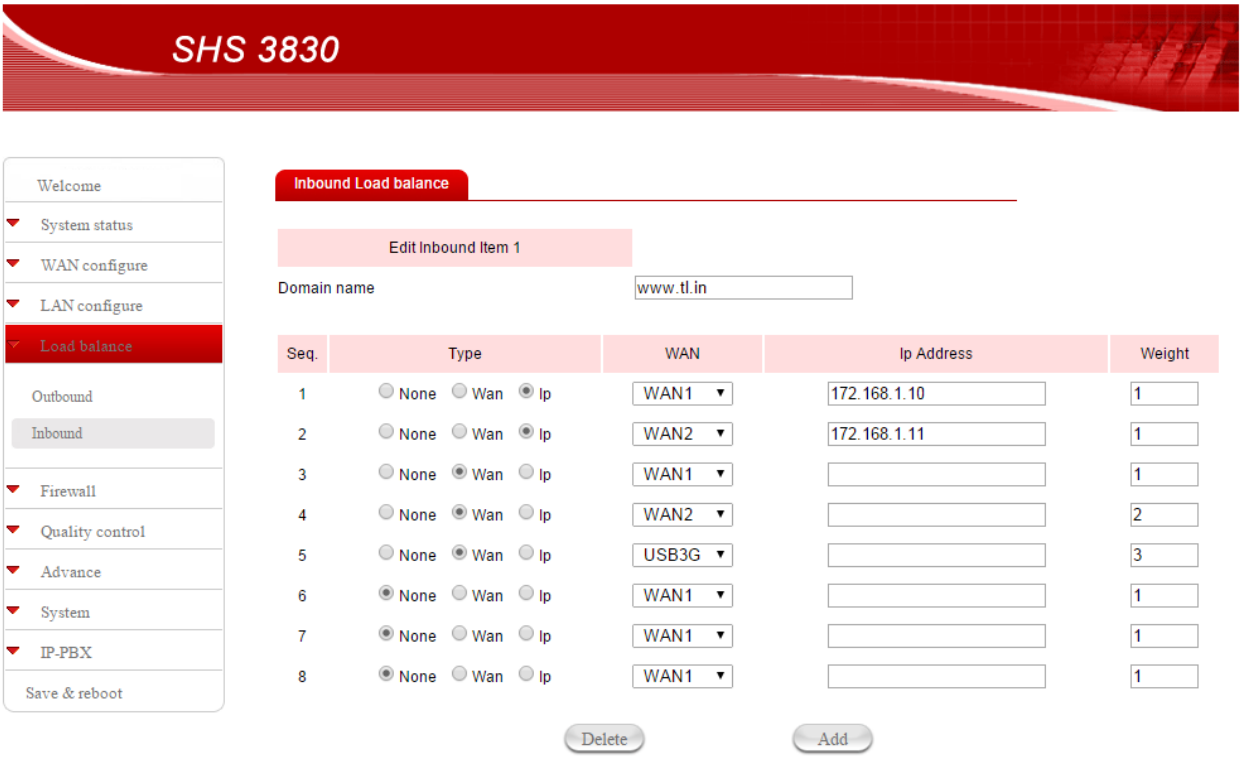
For example, please follow these steps as below for adding an item.

Step 1: Enter **inbound** web page. Then click “Add” to enter the added page.

LOAD BALANCE – Inbound



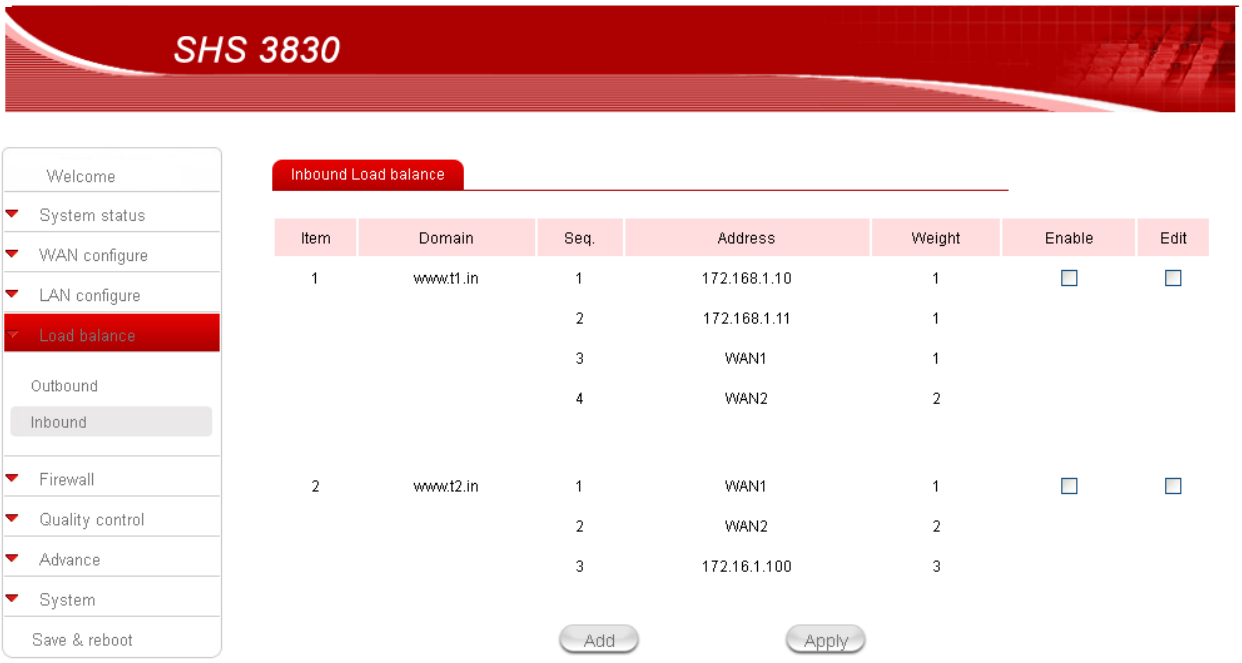
Step 2: Fill data to Domain name. If Type is IP, user must fill an IP for selected WAN port. If Type is WAN, User does NOT fill IP address. Then Click “Add” then router go back to **Inbound** list table.



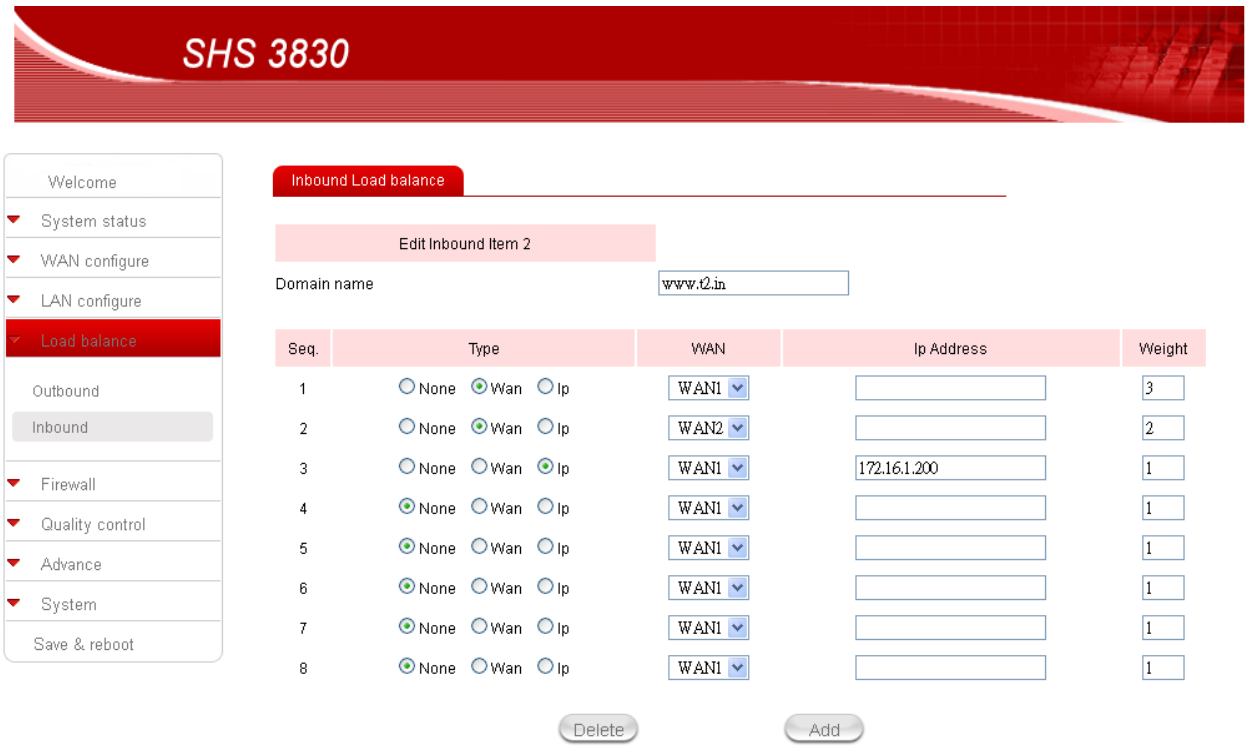
Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

Option: Edit or Delete

Step 1: Enter **Inbound** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router go back to **Inbound** list table. If users want to edit, click “add” when user finish editing job. Then router go back to **Inbound** list table.



Step 3: Go back to **Inbound** list table

3.3 Firewall

Firewall indeed is a big issue in networking, not only protect router from attack, but also complex inspection cause not so friendly usage experience while configured. Therefore how to make it easily and highly workable by user is an important issue for designer. Below supported functions by router are the most useful for deployment in real networking environment.

- Super Users

- DoS defense
- ARP protection
- Local IP filtering
- Remote IP filtering
- Intrusion security
- Messenger blocking
- IP session limit

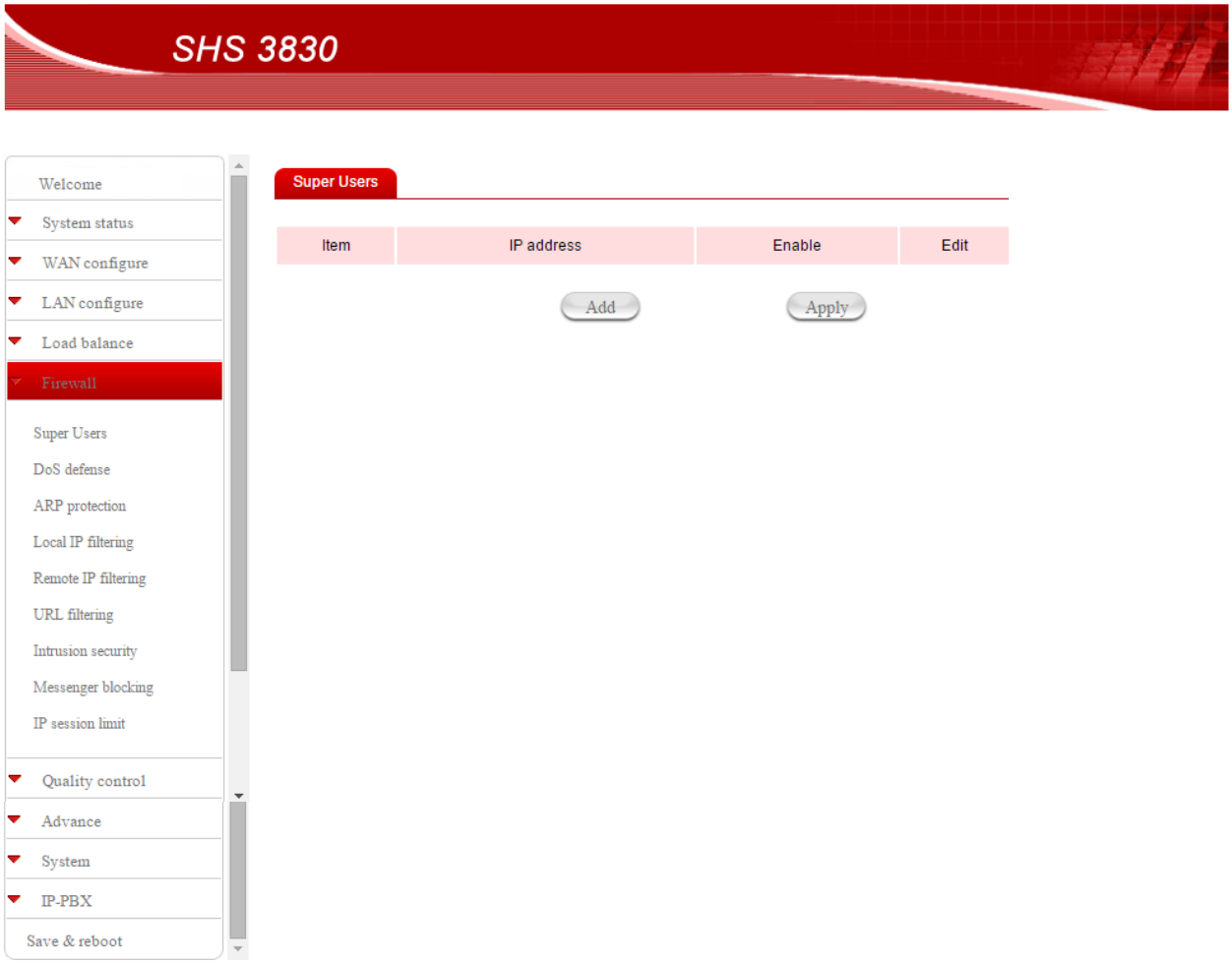
3.3.1 Super Users

The SHS 3830 allows super users IP can access Internet without limitation when enable block function.

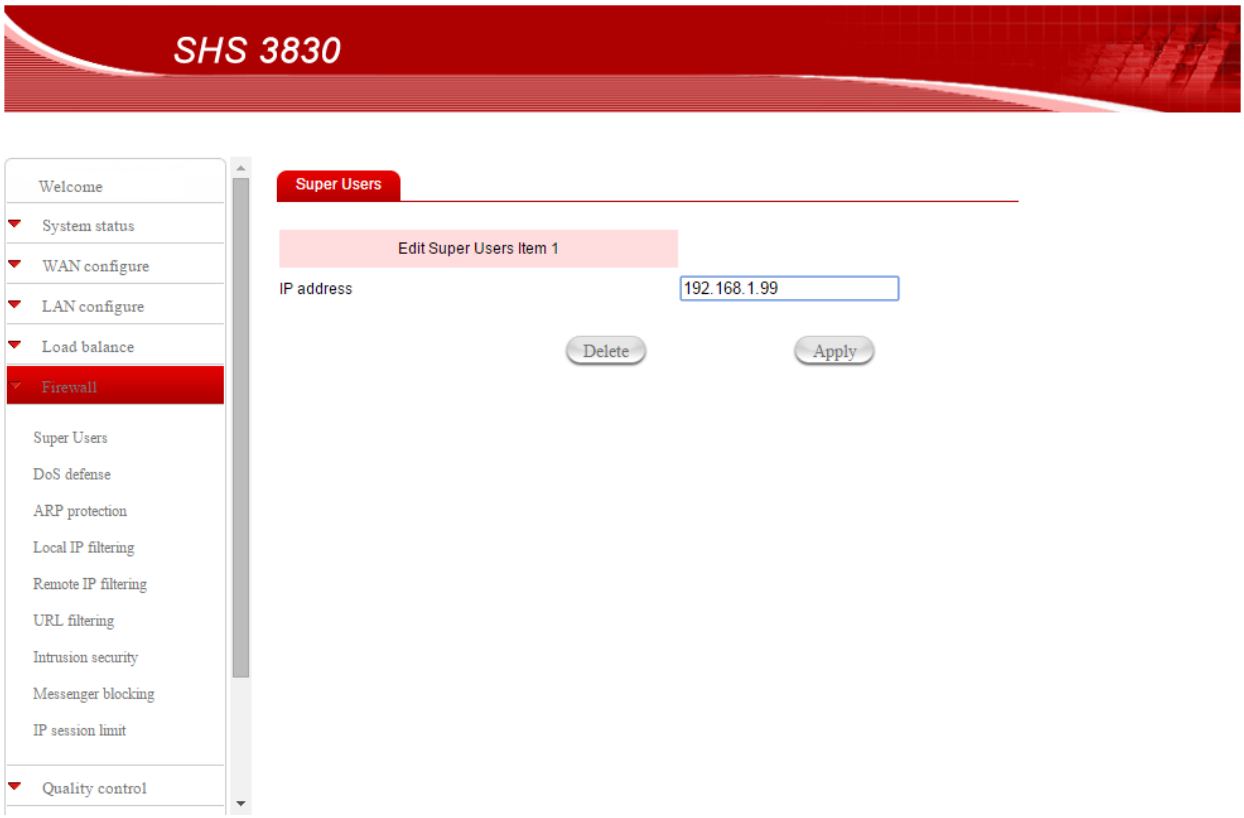
Option: Add a new item.

Step 1: Enter **Super Users** web page. Then click “Add” to enter the added page.

Firewall – Super users



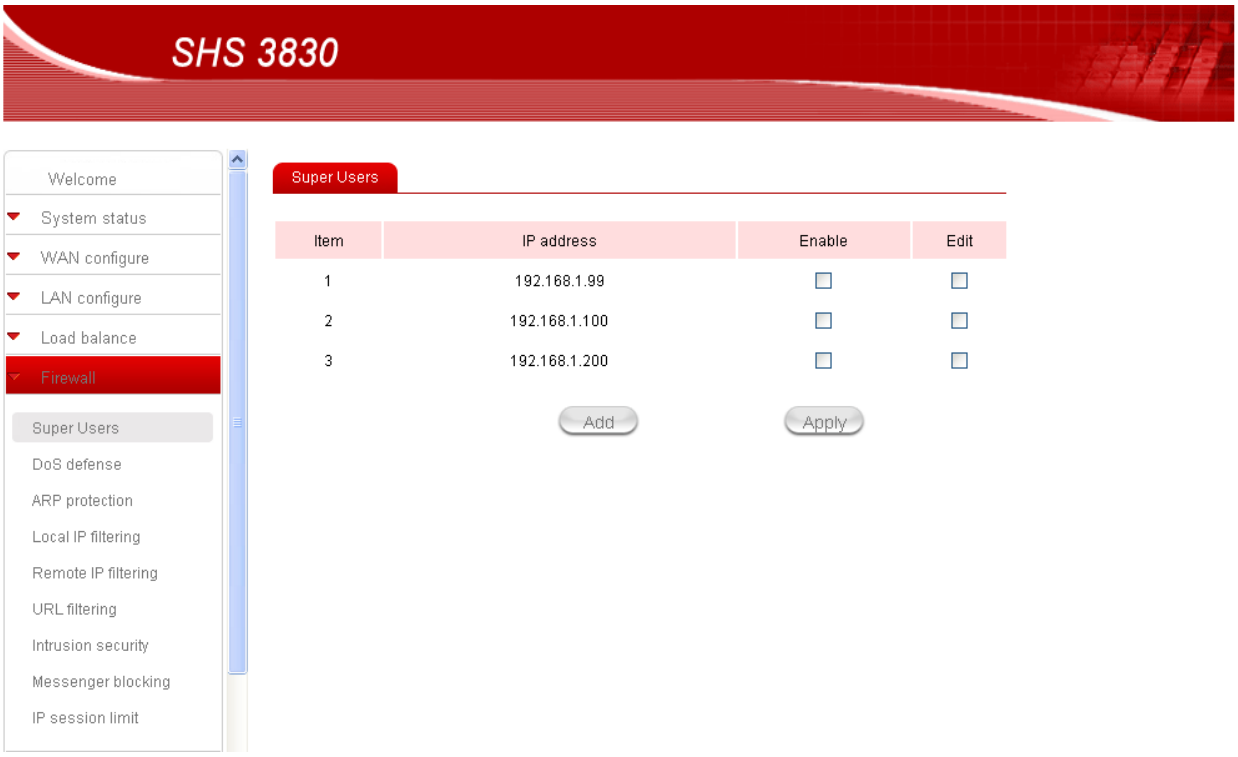
Step 2: Fill data to IP address. Then Click “Add” then router goes back to **Super Users** list table.



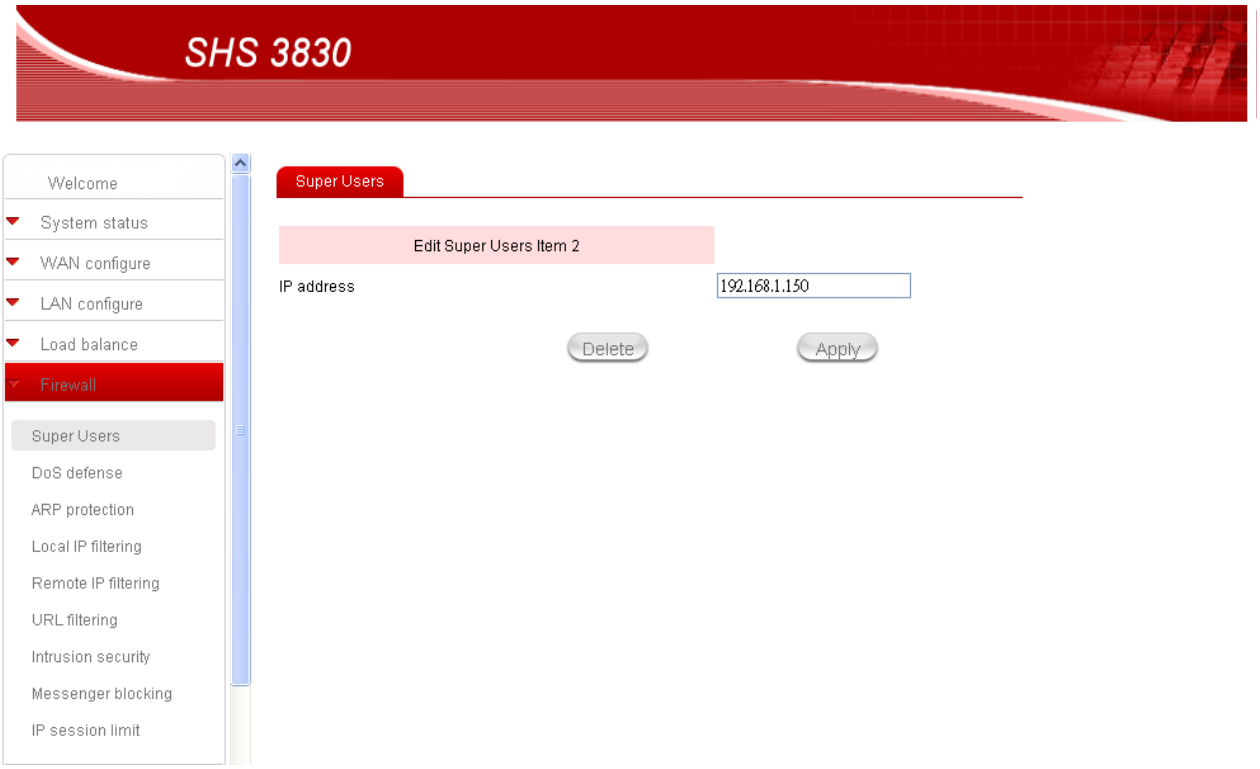
Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

Option: Edit or Delete

Step 1: Enter **Super Users** web page. Then click “Enable” check square of item 2 to enter the edited page.



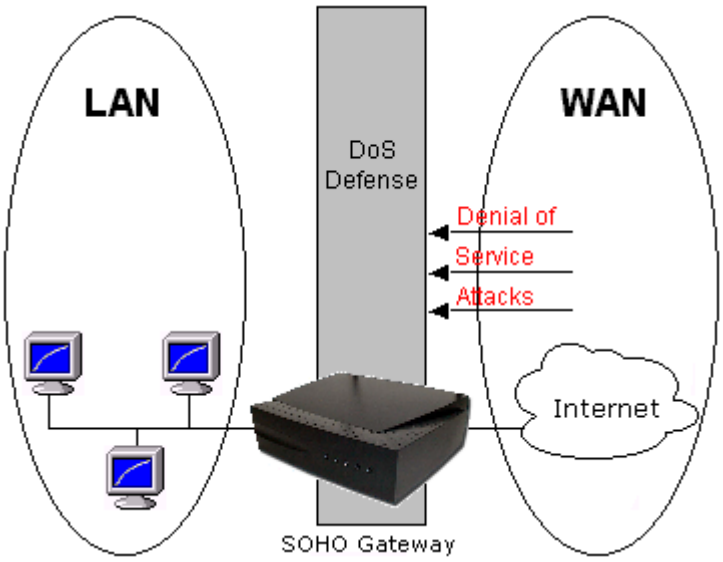
Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Super Users** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Super Users** list table.



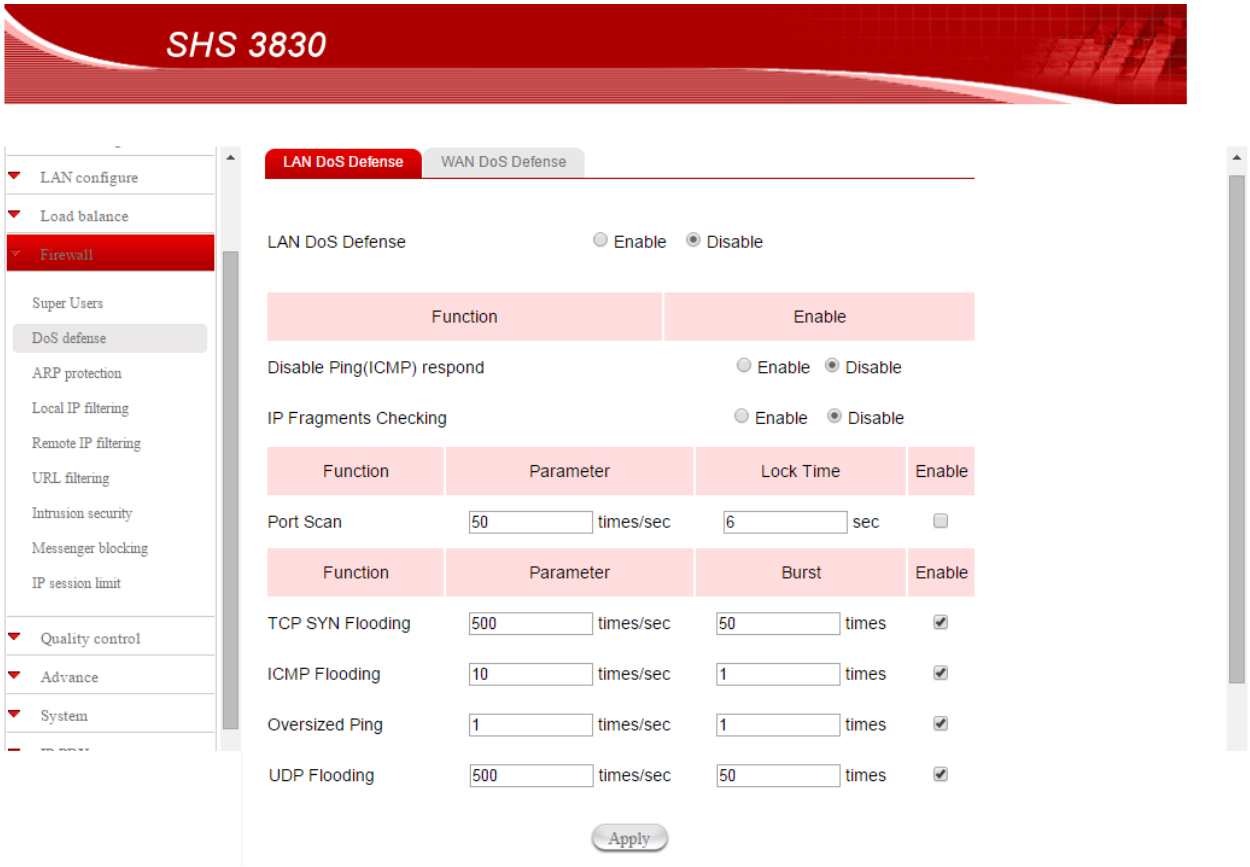
Step 3: Router go back to **Super Users** list table.

3.3.2 DoS defense

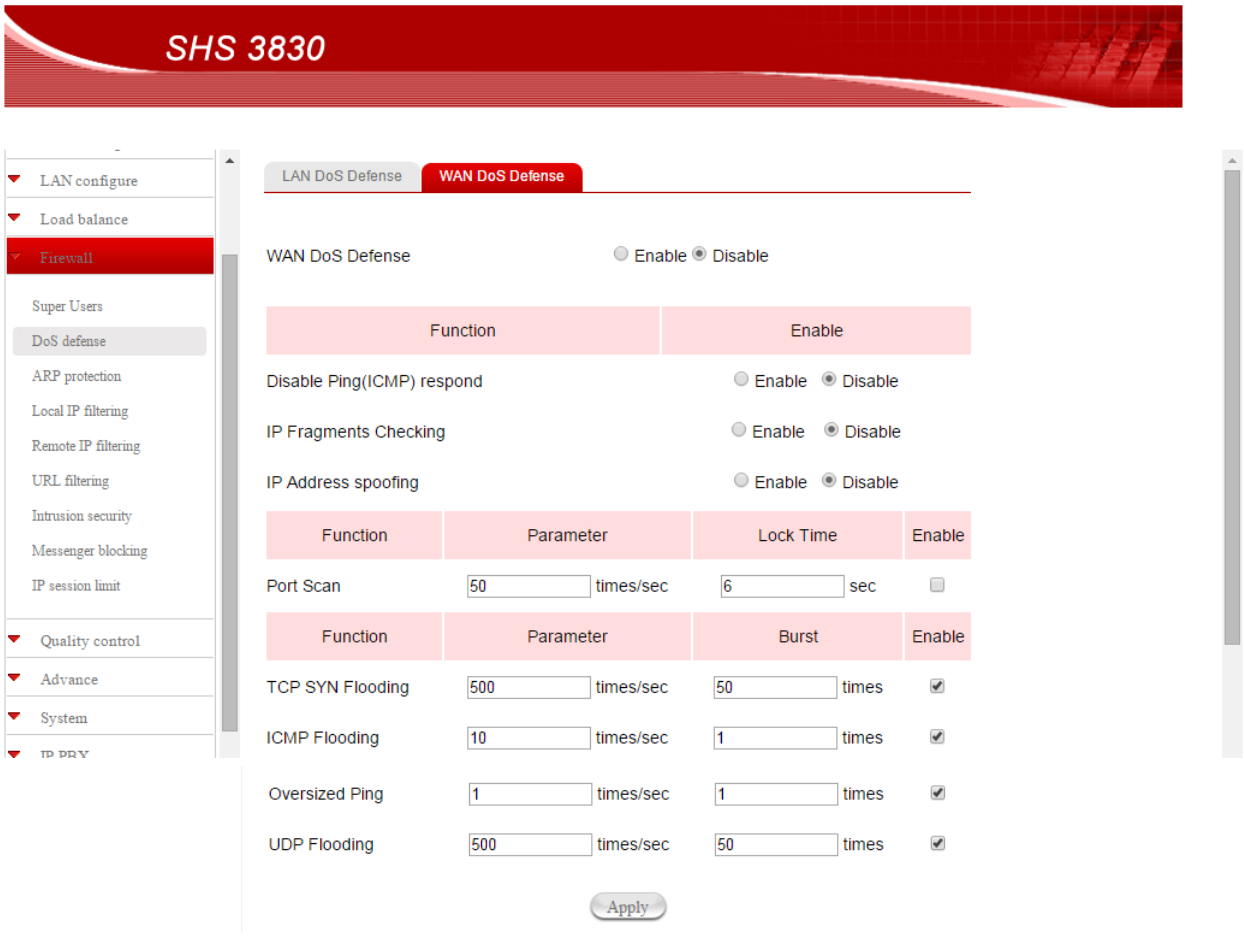
The SHS 3830 also provides with DoS (Denial of Service Defense) function to protect your network servers, hosts, routers and other devices from the attacking of villain using mass data transmission. The default value in the display is the optimize parameter for Router.



Firewall – DoS defense – LAN DoS Defense



Firewall – DoS defense – WAN DoS Defense



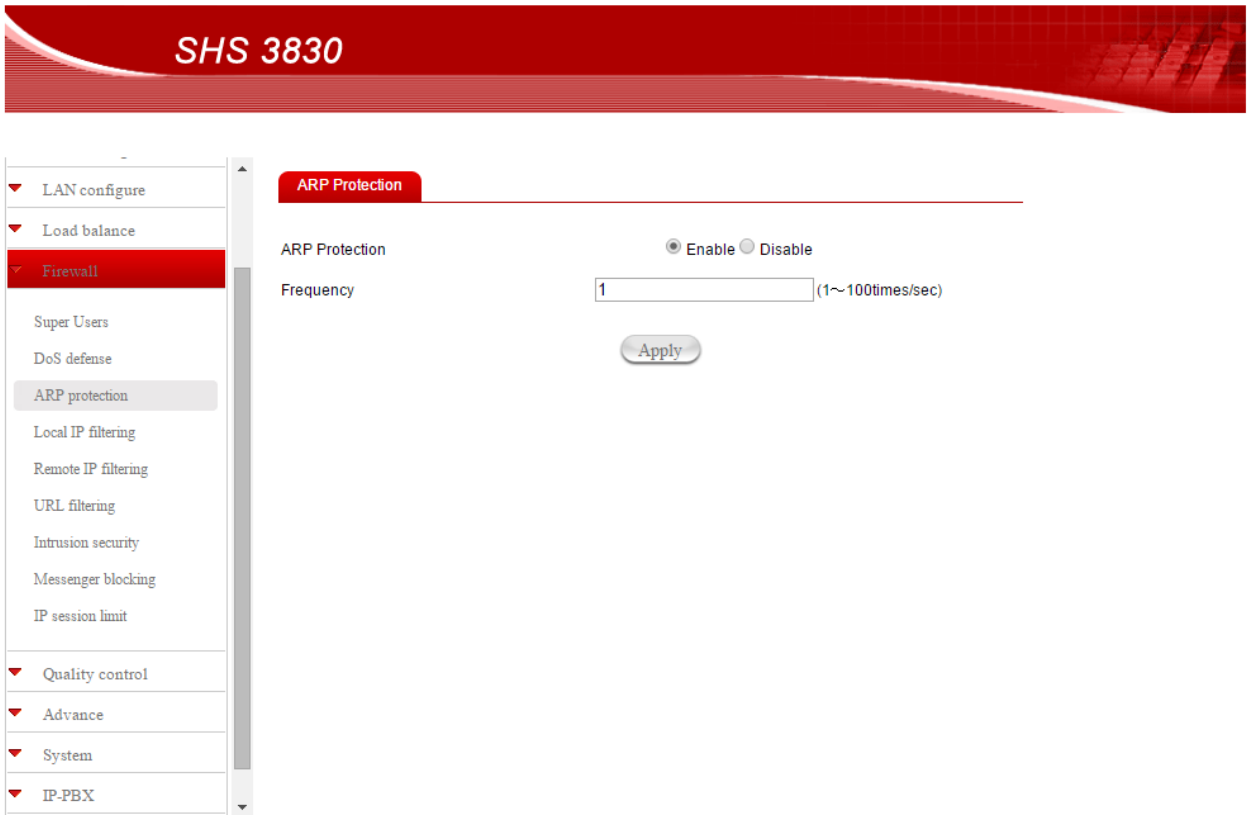
* Some virus are using “PING” command to attack network, this Router can be defined as accept or reject “PING” command from WAN or LAN.

Function	Description
IP Fragments Checking	Checking the IP fragments. When it finds someone from WAN side tries to attack your network using overlap IP fragments in a bad attention, this function will check over these packets and drop them.
IP Address spoofing	Finding out whether the source address(s) and destination address(s) are legal IP’s or not. If they are illegal IP’s or multicast addresses, this function will cast these packets away.
Port Scan	When an IP from Internet tries to scan the IP of Load Balance Router up to 10000ports/sec (default value), this function will drop all the packets from this IP within 5 minutes (default value).
TCP SYN Flooding (WAN)	When a destination address and destination port of Load Balance Router receives TCP SYN packet from WAN over 10000 times (default value) in one second, Load Balance Router will close this address and port for 5 minutes (default value) temporarily.
TCP SYN Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send TCP SYN packet over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.
ICMP Flooding (WAN)	When a destination address of Load Balance Router receives ICMP from WAN over 10000 times (default value) in one second, Load Balance Router will close this address for 5 minutes (default value) temporarily.
ICMP Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send ICMP over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.
UDP Flooding (WAN)	When a destination address of Load Balance Router receives UDP from WAN over 10000 times (default value) in one second, Load Balance Router will close this address for 5 minutes (default value) temporarily.
UDP Flooding (LAN)	When an IP in LAN of Load Balance Router tries to send UDP over 10000 times (default value) in one second, Load Balance Router will close this source address for 5 minutes (default value) temporarily.

3.3.3 ARP protection

It prevents network hosts from ARP spoofing attack so that enable the function to immune any ARP spoofing. So router updates ARP message for hosts to keep accurate ARP table restoring in hosts due to attacker sending spoofed ARP while attacking.

Firewall – ARP protection



3.3.4 Local IP filtering

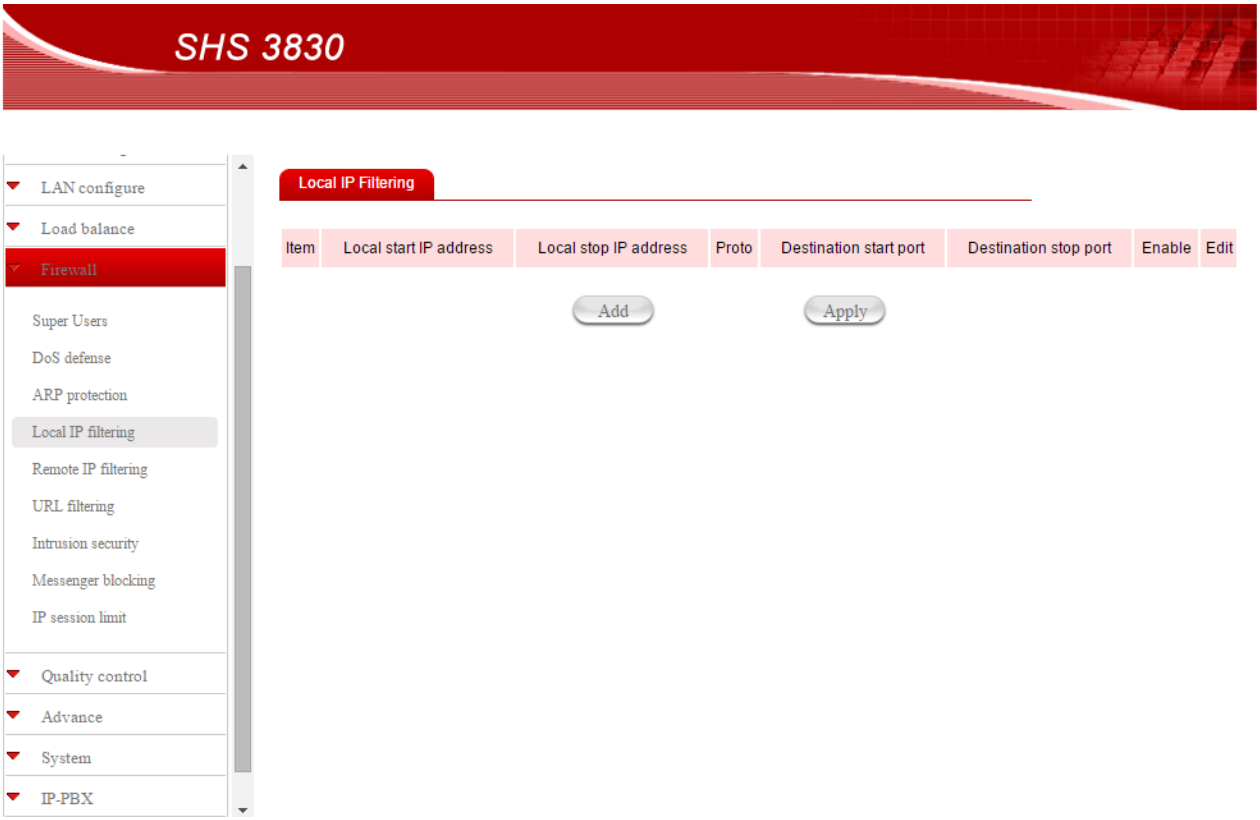
SHS 3830 allows you to do accessed restriction of block/allow outgoing IP packets by protocol (port number).

You may restrict some IP's only to perform limited protocols or allow them to execute partial protocols. And the first thing you have to know is the port numbers and their usages.

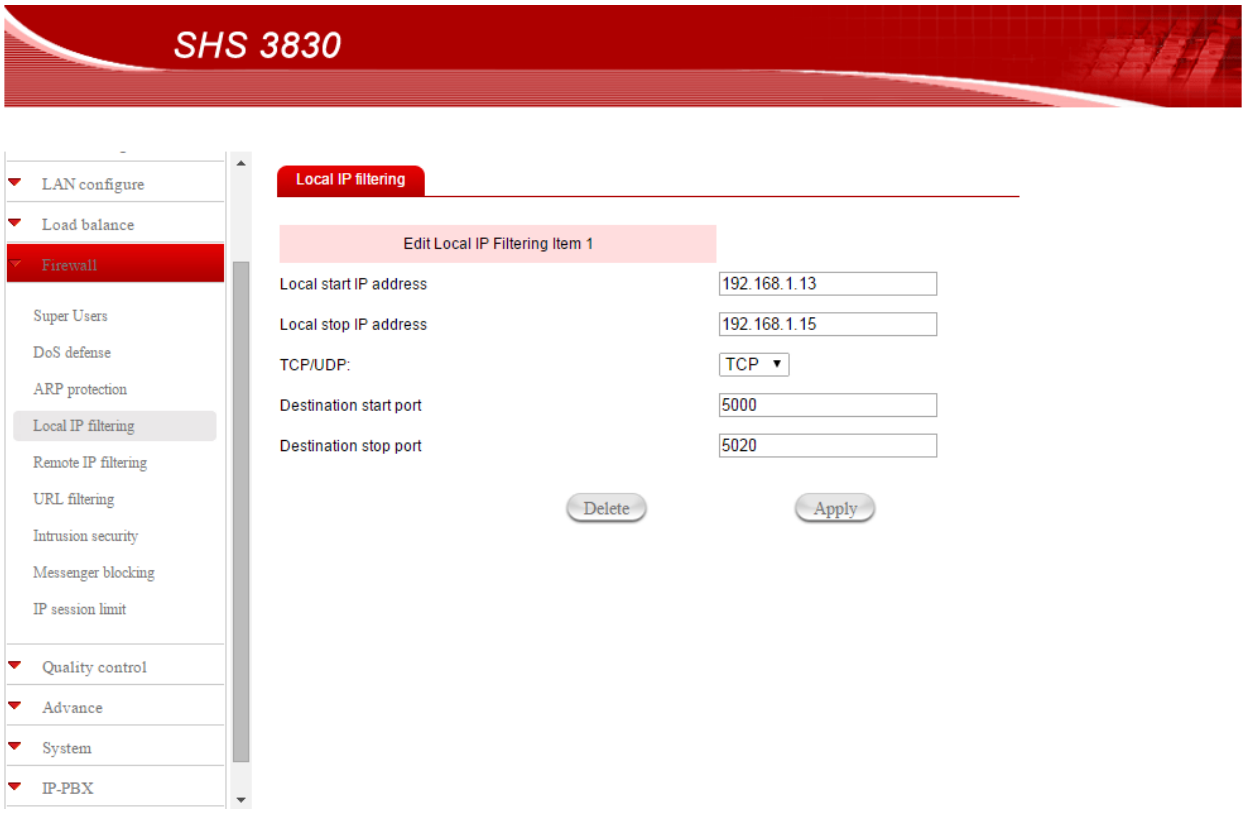
Option: Add a new item.

Step 1: Enter **Local IP filtering** web page. Then click "Add" to enter the added page.

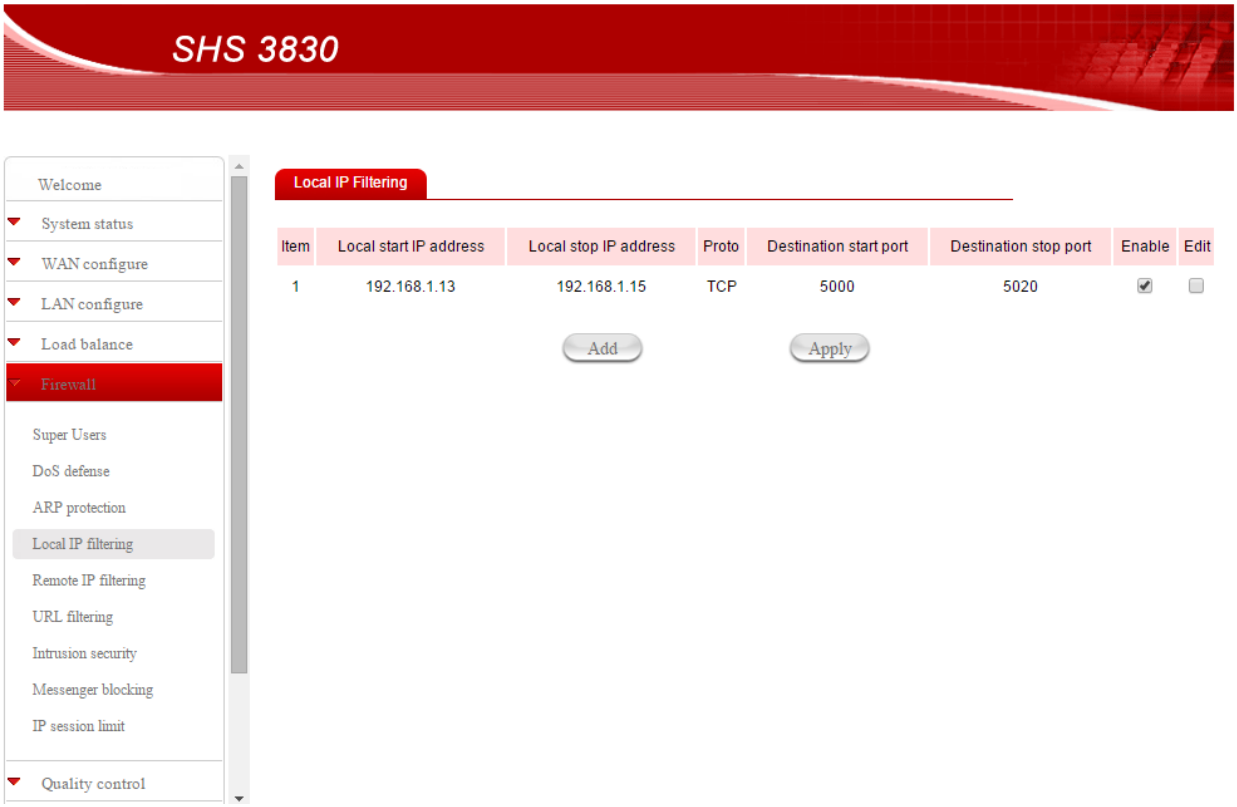
Firewall – Local IP filtering



Step 2: Fill data to Local Start IP, Local Stop IP, Protocol, Local Port and Local Stop Port. Then click “Add” then router goes back to **Local IP filtering** list table.

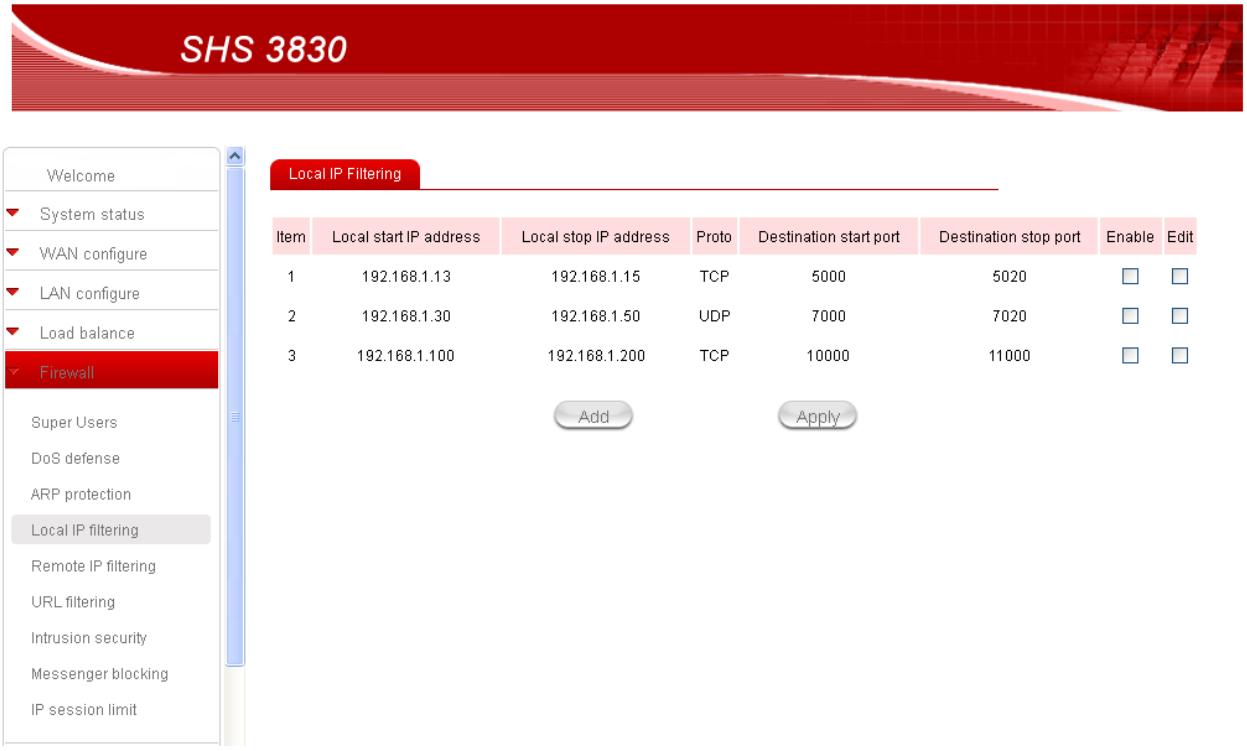


Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

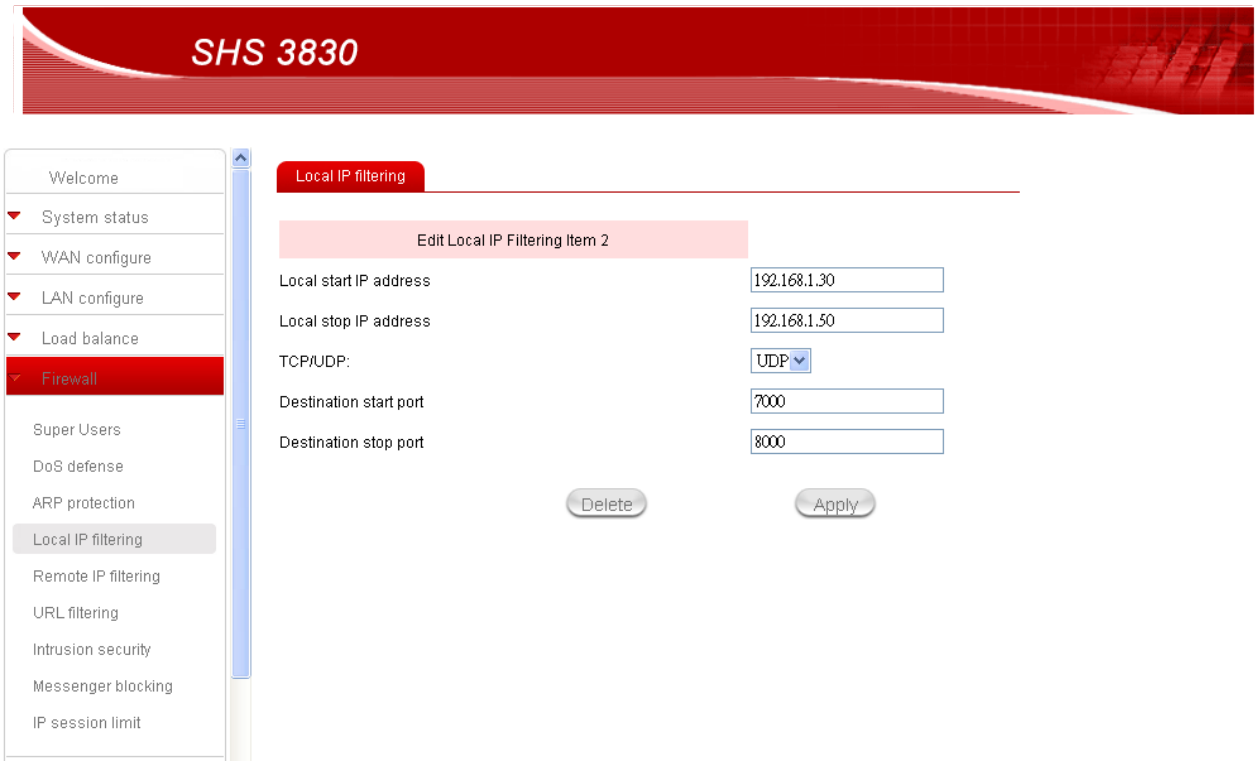


Option: Edit or Delete

Step 1: Enter **Local IP filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Local IP filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Local IP filtering** list table.



Step 3: Router go back to **Local IP filtering** list table.

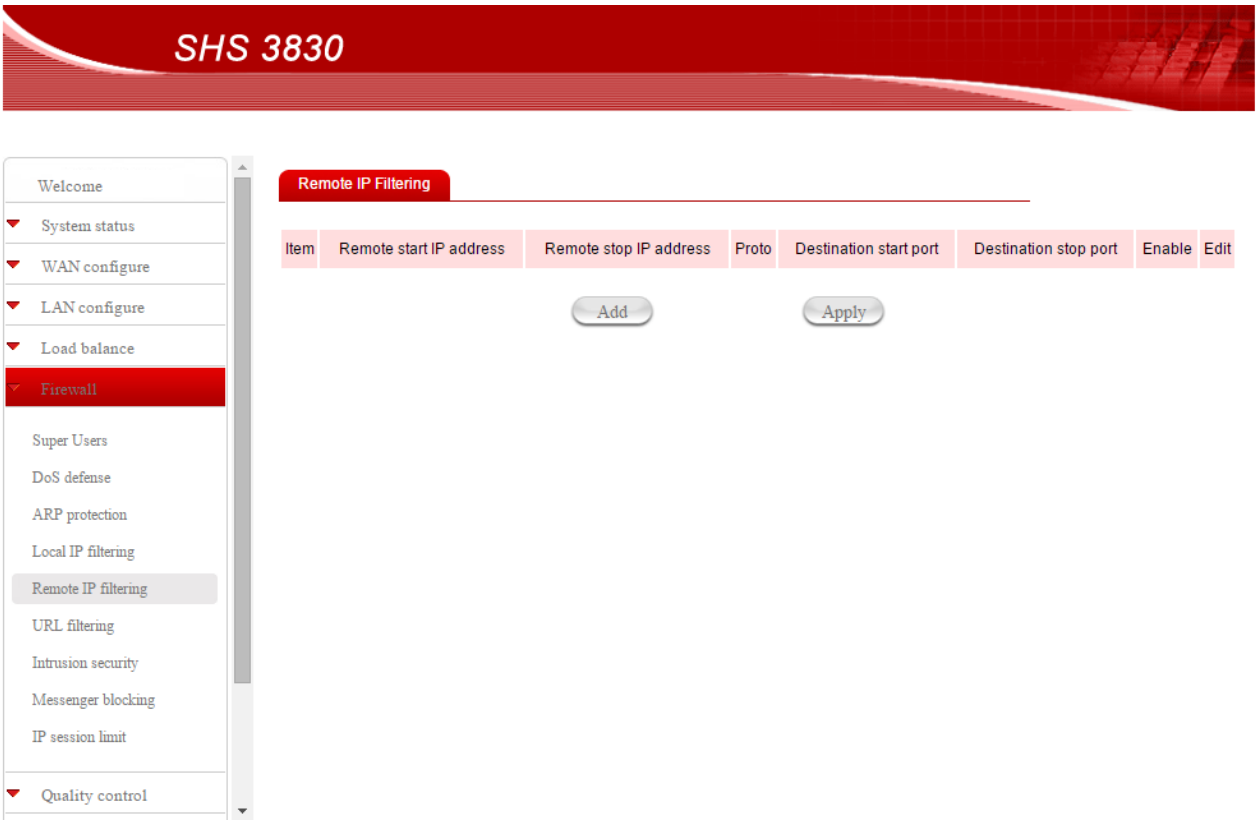
3.3.5 Remote IP filtering

As name implied, router filters remote IP user desire to and set below.

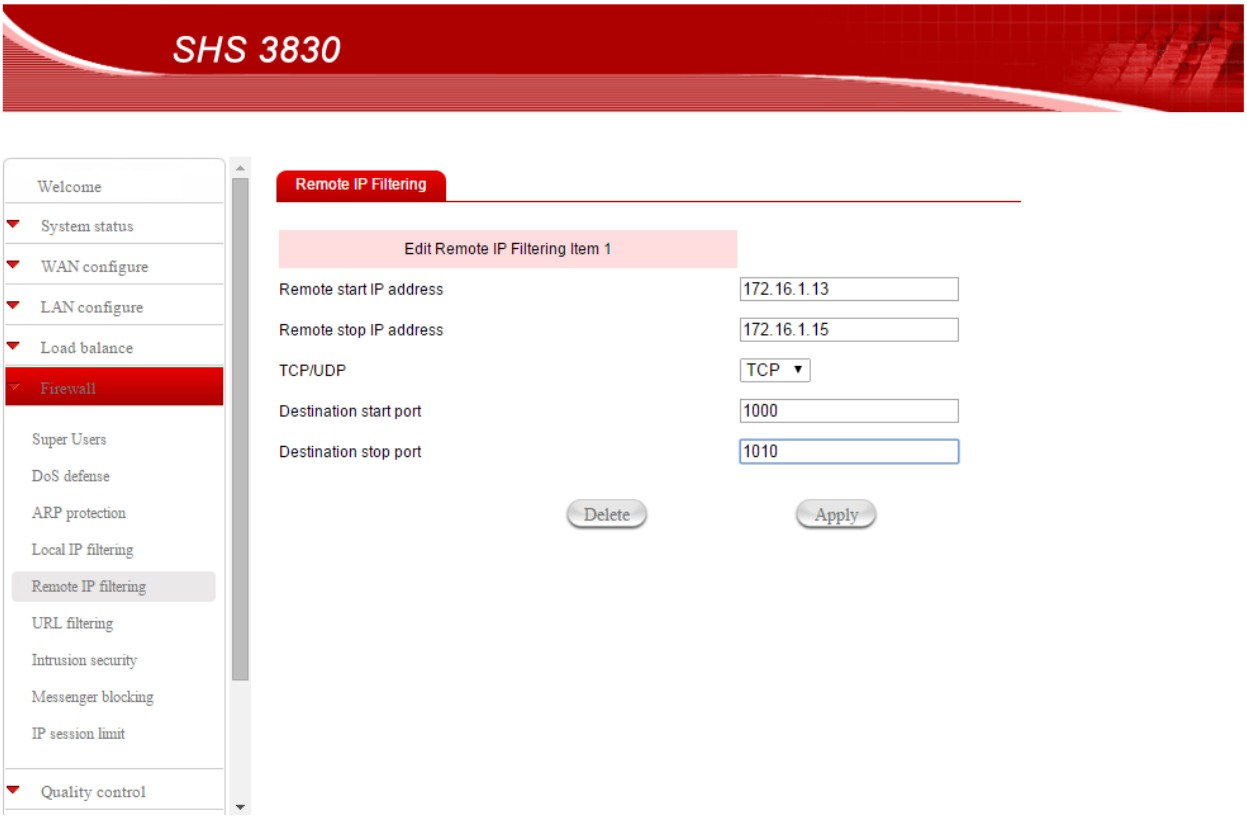
Option: Add a new item.

Step 1: Enter **Remote IP filtering** web page. Then click “Add” to enter the added page.

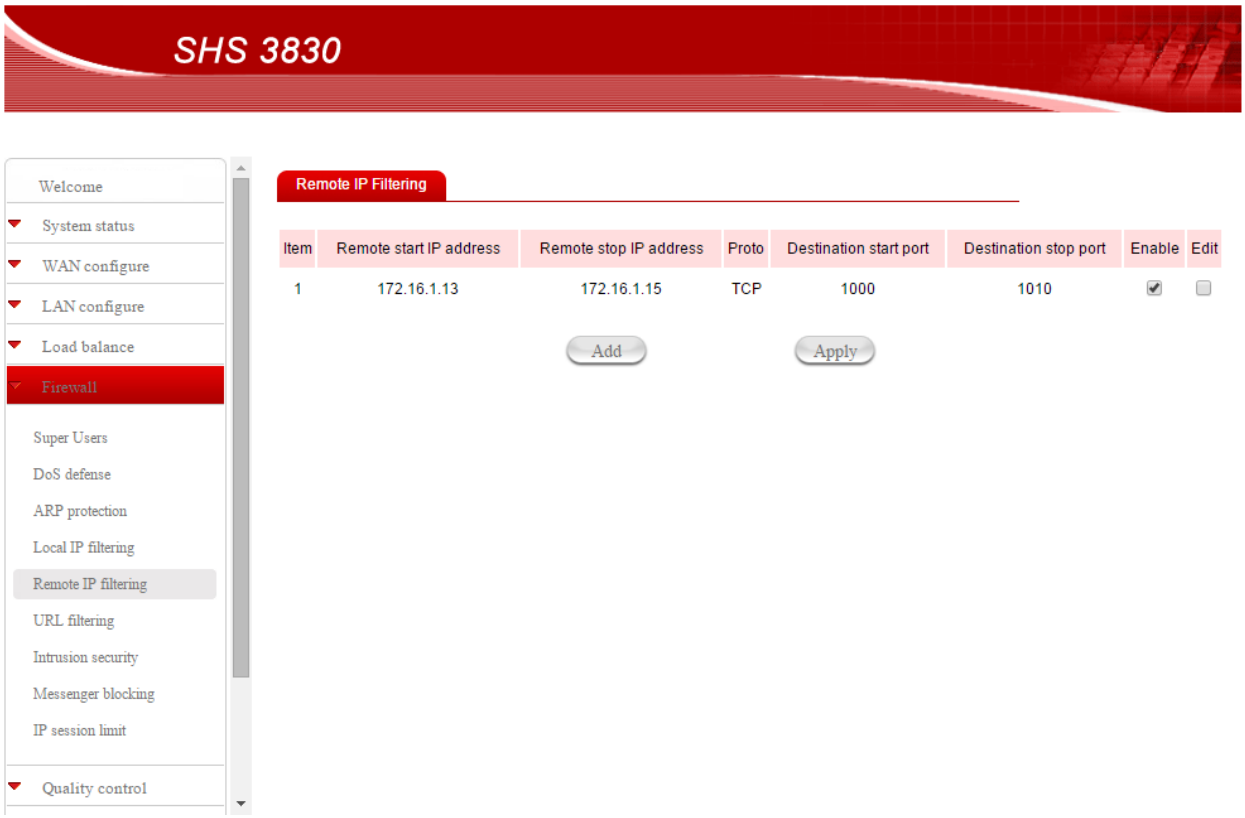
Firewall – Remote IP filtering



Step 2: Fill data to Remote Start IP, Remote Stop IP, Protocol, Remote Port and Remote Stop Port. Then Click “Add” then router goes back to **Remote IP filtering** list table.

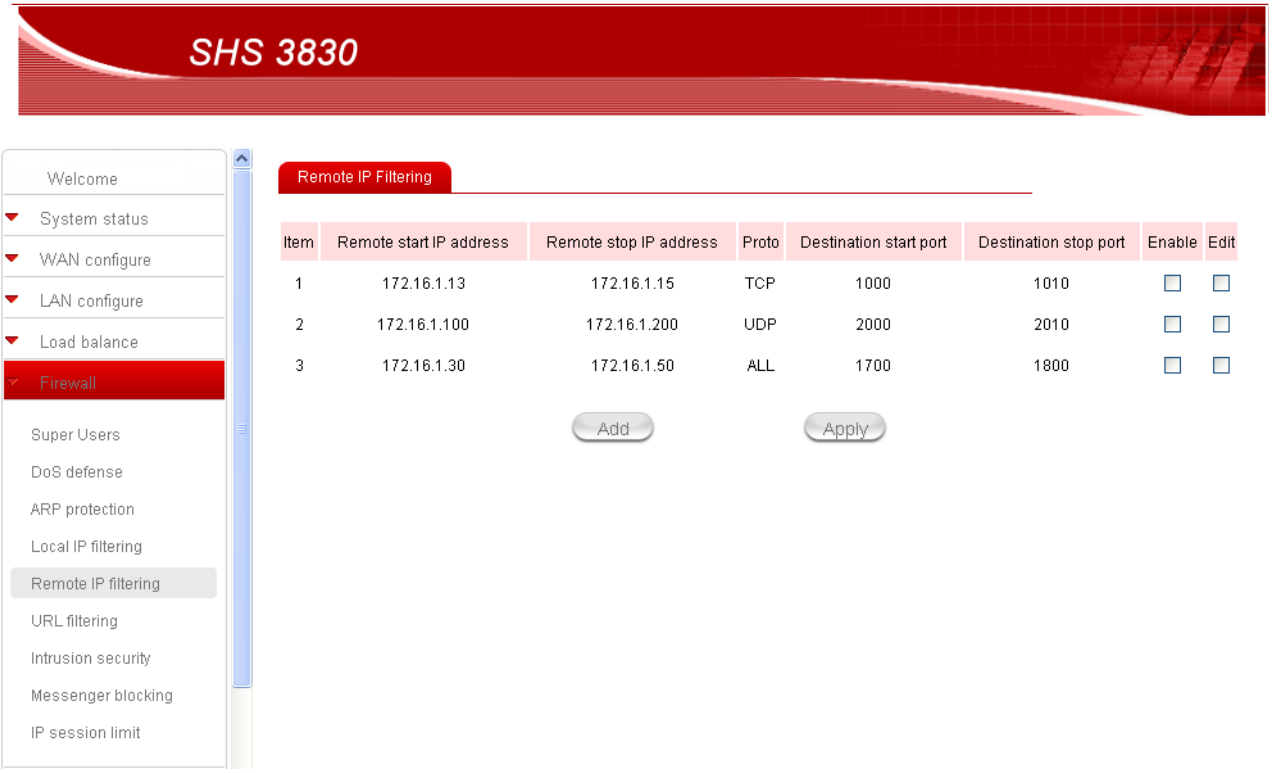


Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Option: Edit or Delete

Step 1: Enter **Remote IP filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Remote IP filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Remote IP filtering** list table.

Step 3: Router go back to **Remote IP filtering** list table.

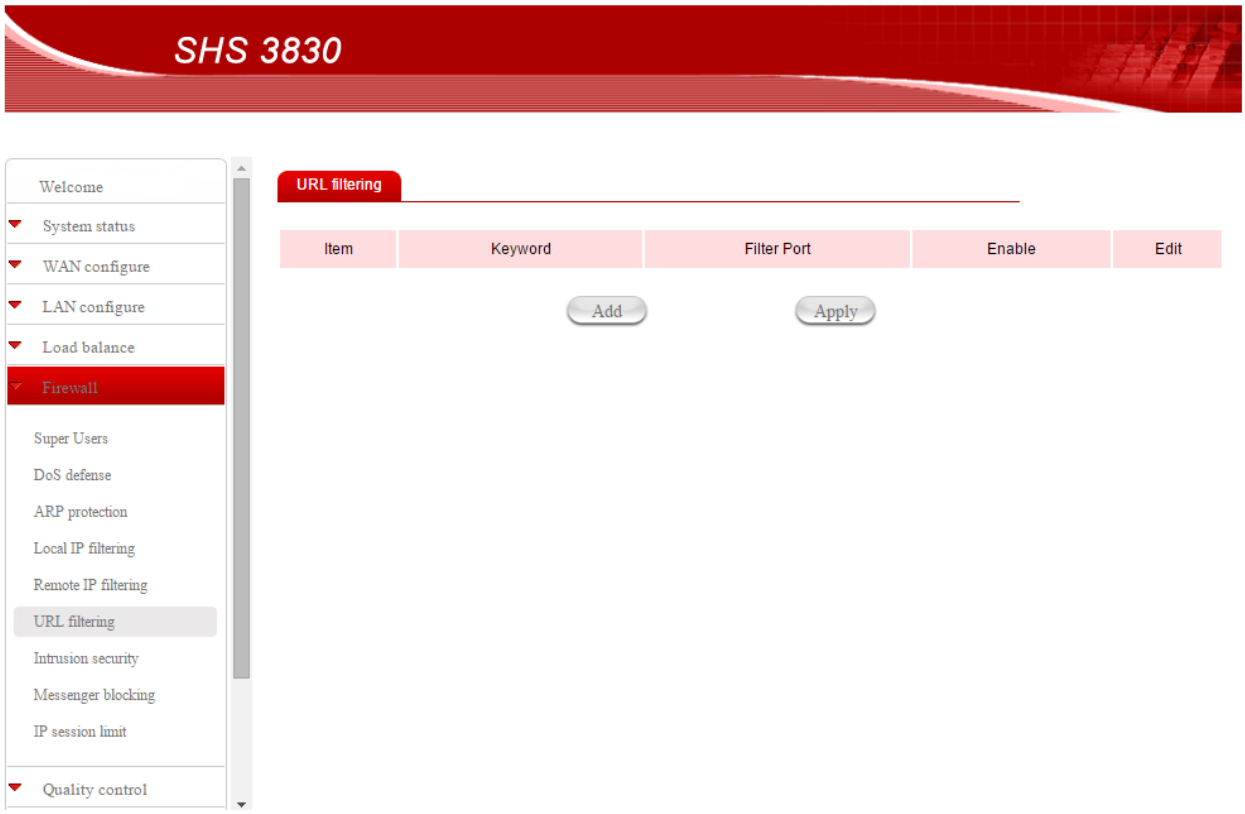
3.3.6 URL filtering

Besides restrict users by local/destination IP, the SHS 3830 provides you to do accessed restriction for user by URL as well. You may restrict some URL address that are not allow to reach

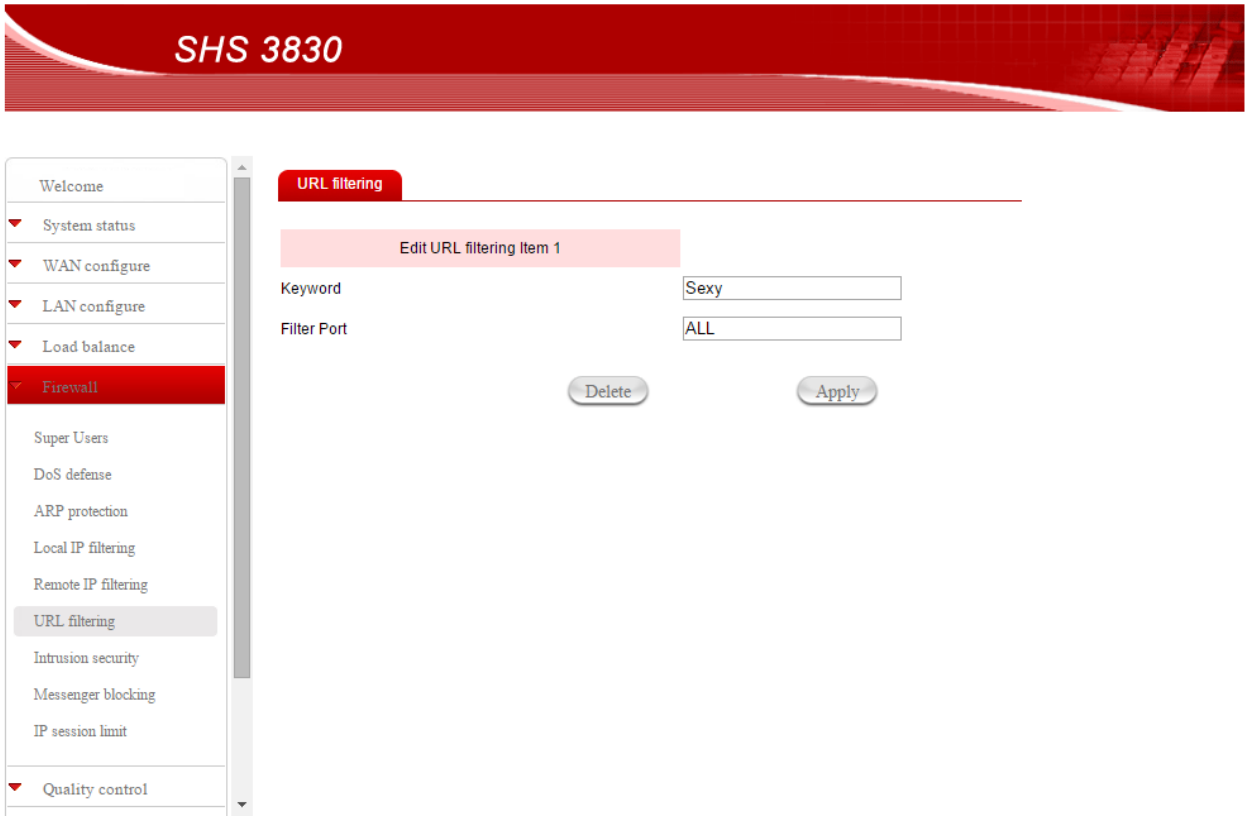
Option: Add a new item.

Step 1: Enter **URL filtering** web page. Then click “Add” to enter the added page.

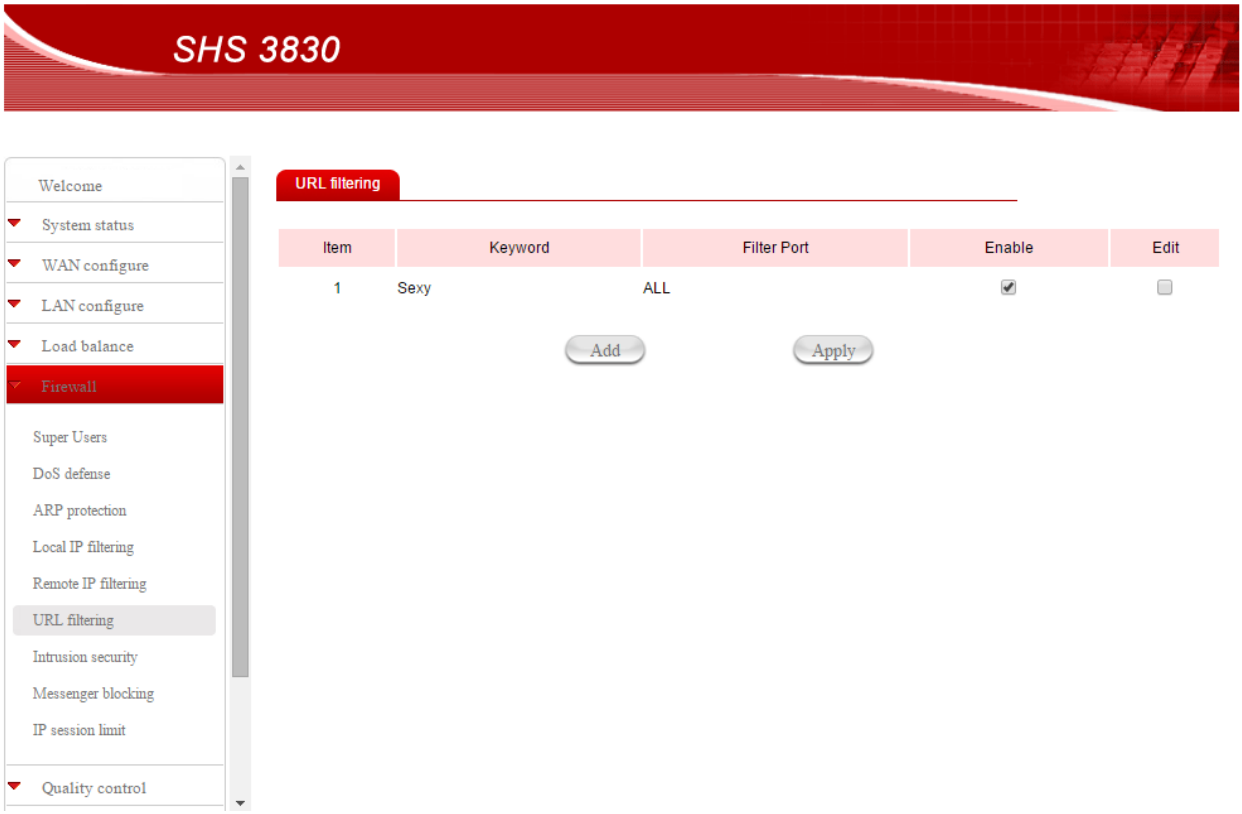
Firewall – URL filtering



Step 2: Fill data to Keyword and Filter Port. You can write a number or ALL to Filter Port. Then Click “Add” then router goes back to **URL filtering** list table.



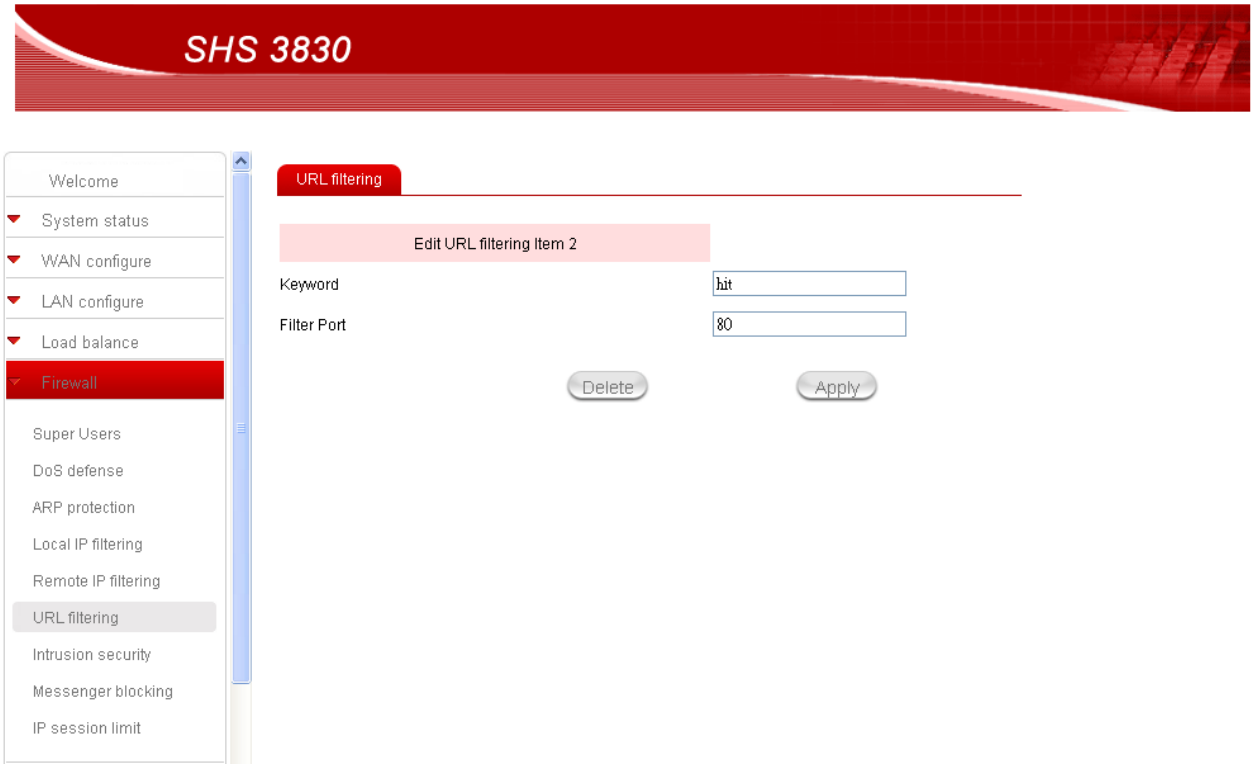
Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



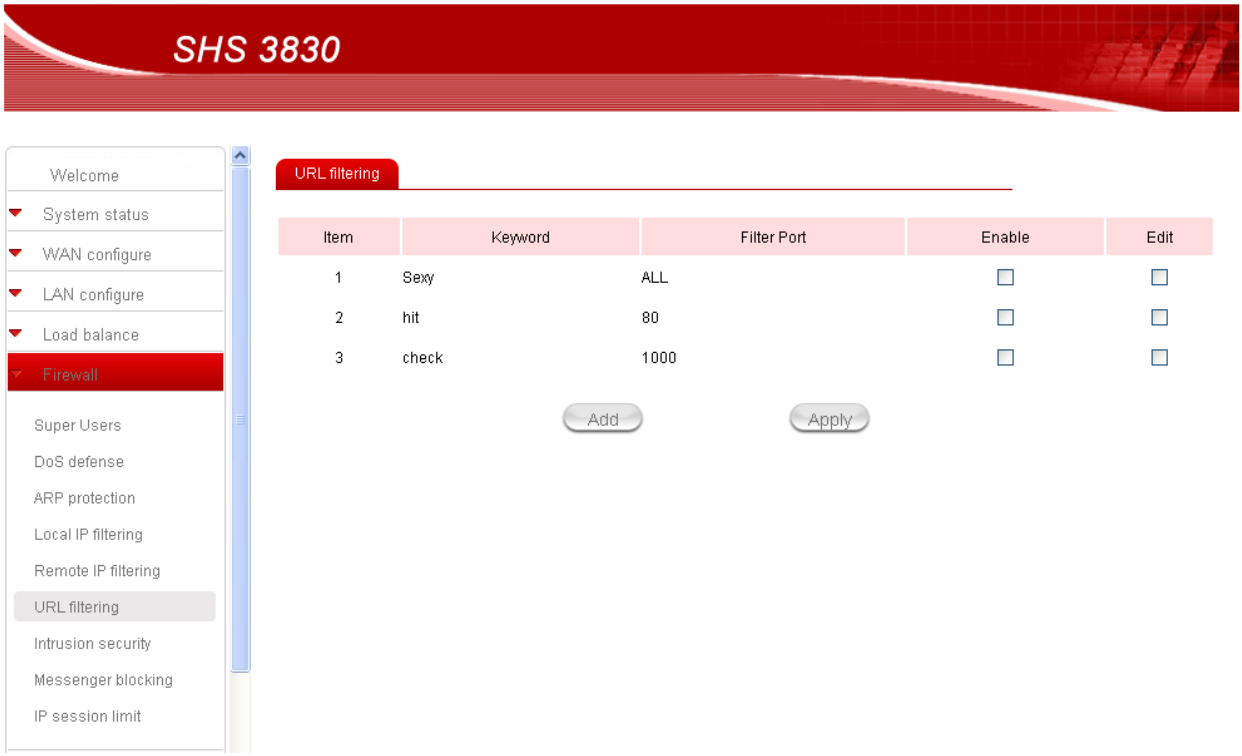
Option: Edit or Delete

Step 1: Enter **URL filtering** web page. Then click “Enable” check square of item 2 to enter the edited page.

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **URL filtering** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **URL filtering** list table.



Step 3: Router go back to **URL filtering** list table.



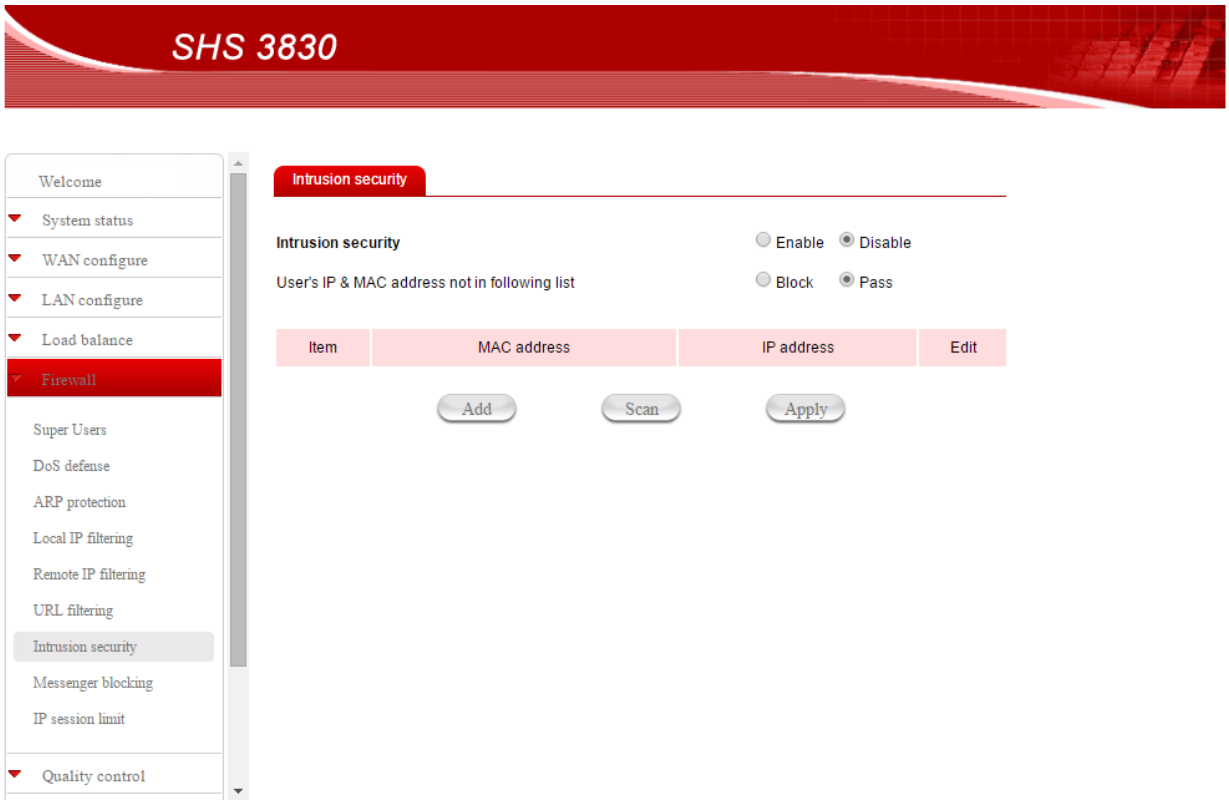
3.3.7 Intrusion security

Pre-setting IP & MAC mapping to prevent from not anticipate association for security consideration. By setting up this table router will perform “BLOCK” or “PASS” function according to the option.

Option: Add a new item.

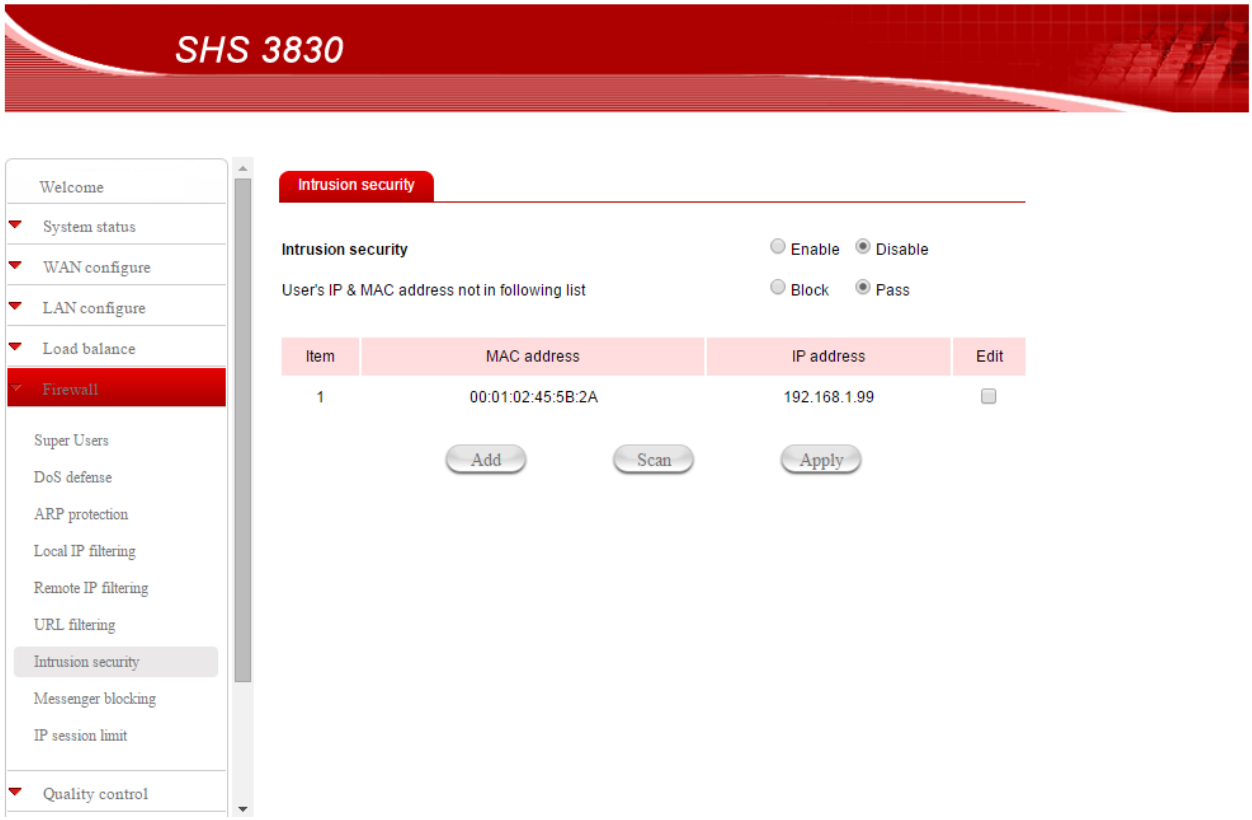
Step 1: Enter **Intrusion security** web page. Then click “Add” to enter the added page.

Firewall – Intrusion security



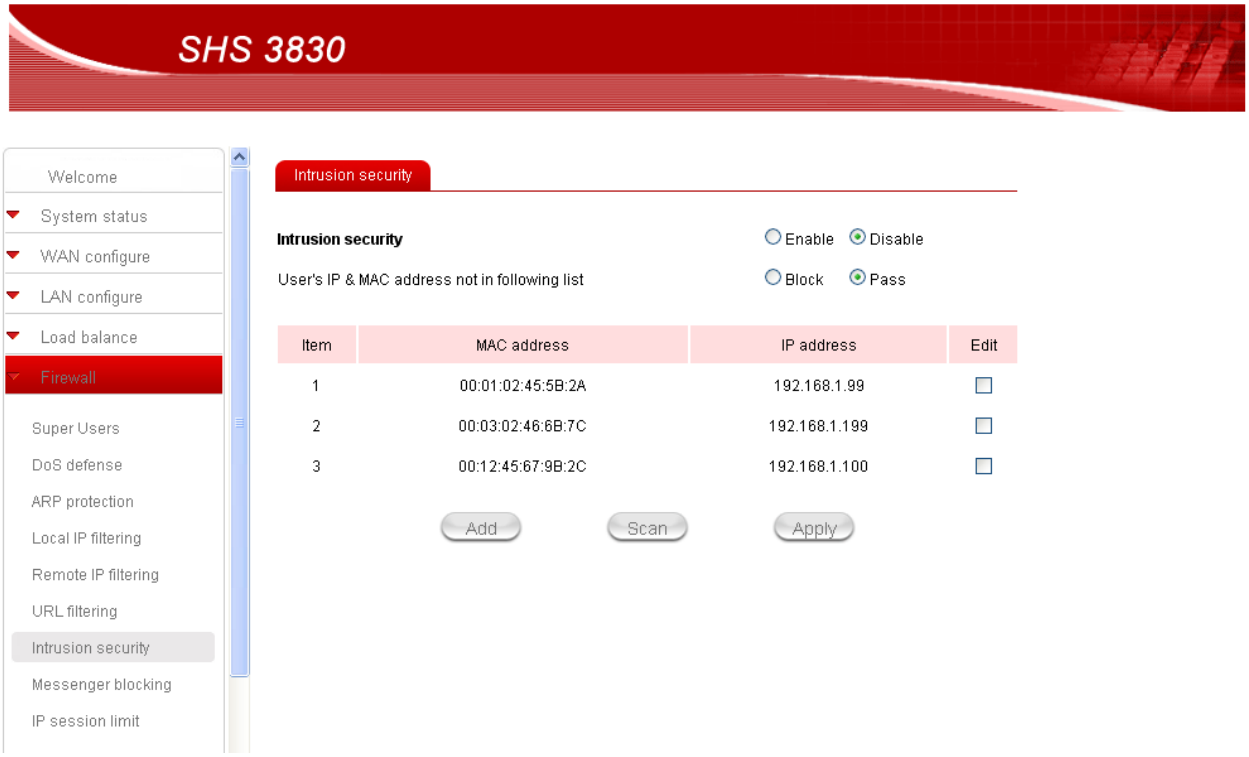
Step 2: Fill data to MAC address and IP. Then Click “Add” then router go back to **Intrusion security** list table.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



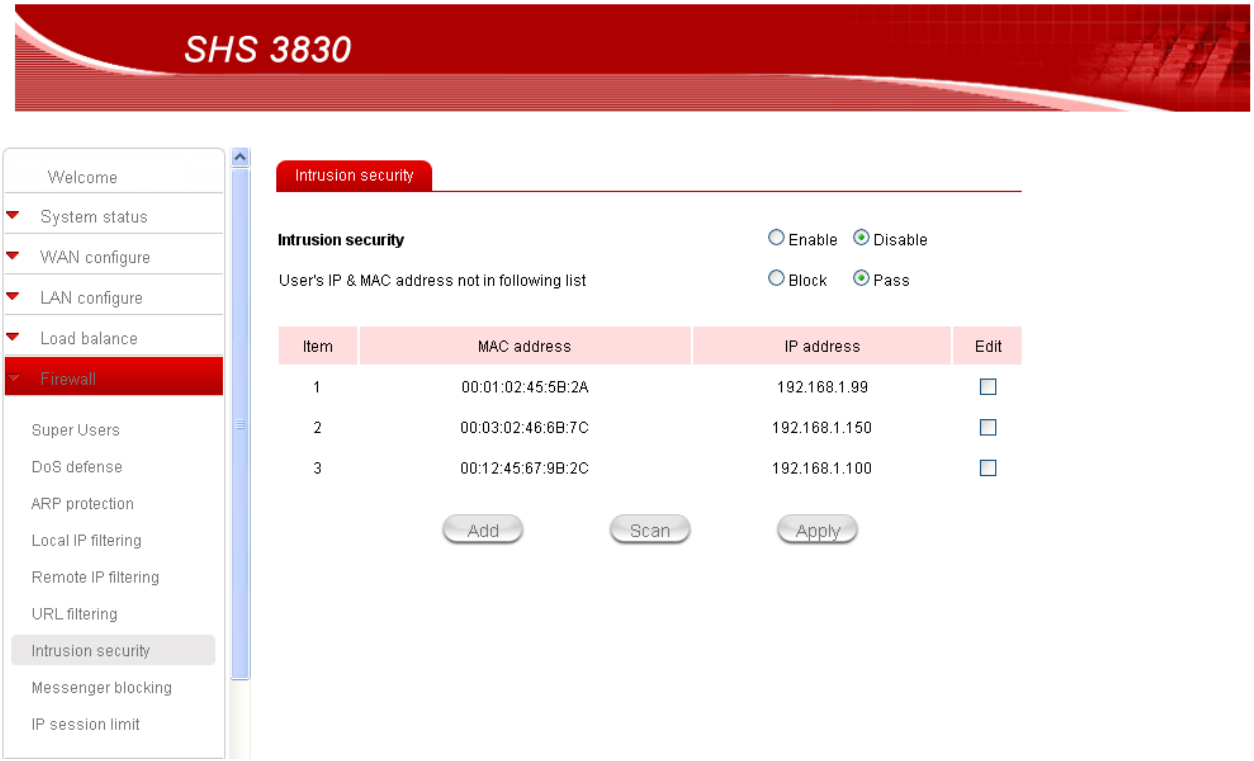
Option: Edit or Delete

Step 1: Enter **Intrusion security** web page. Then click “Enable” check square of item 2 to enter the edited page.

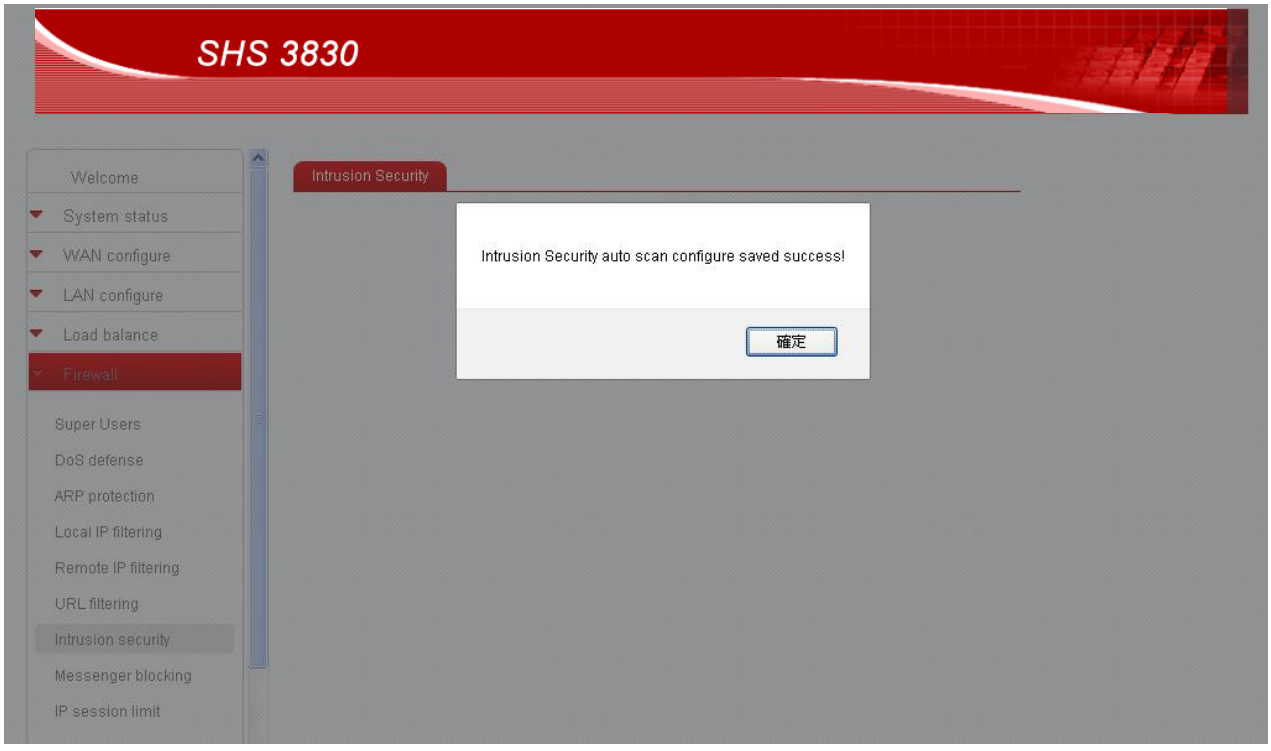


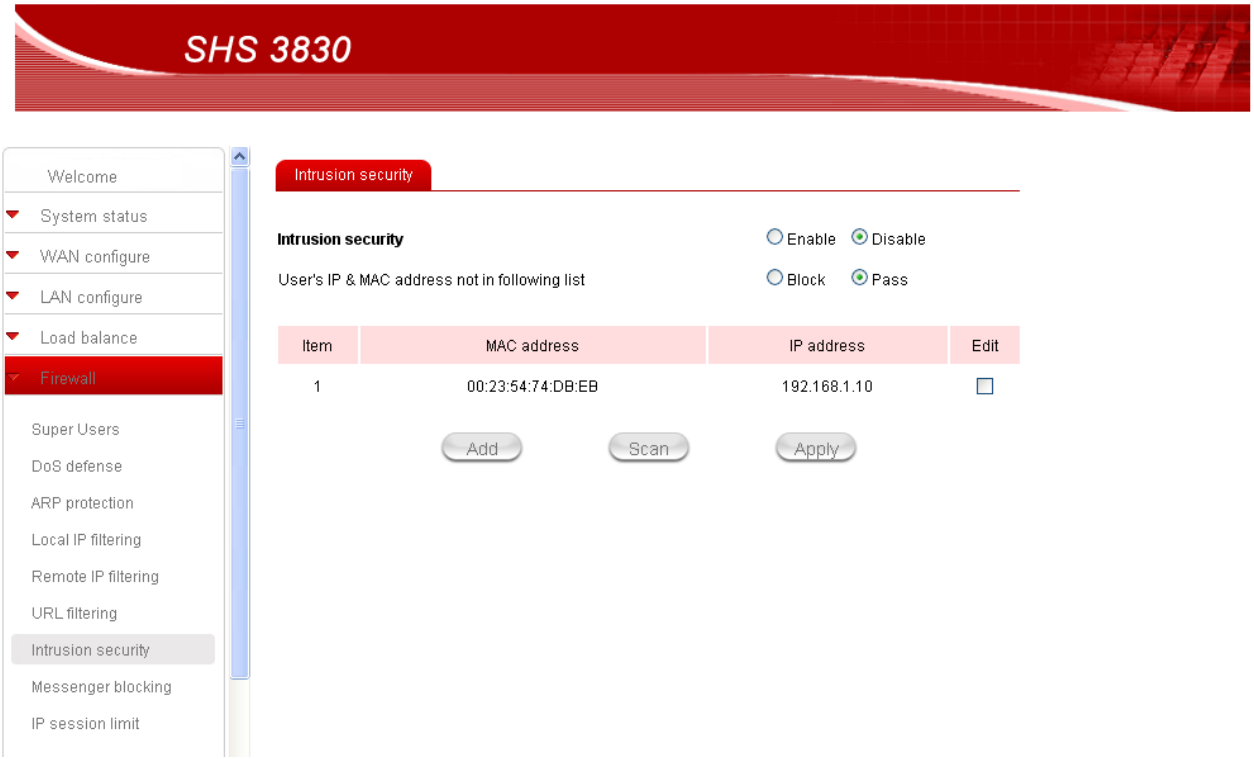
Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Intrusion security** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Intrusion security** list table.

Step 3: Router go back to **Intrusion security** list table.



Example: Scan all PC connect with Router. Directly click scan. It will clear all old data. Replace it with scanned data. But it need some time to scan all PC. The delay time depend on PC quantity.

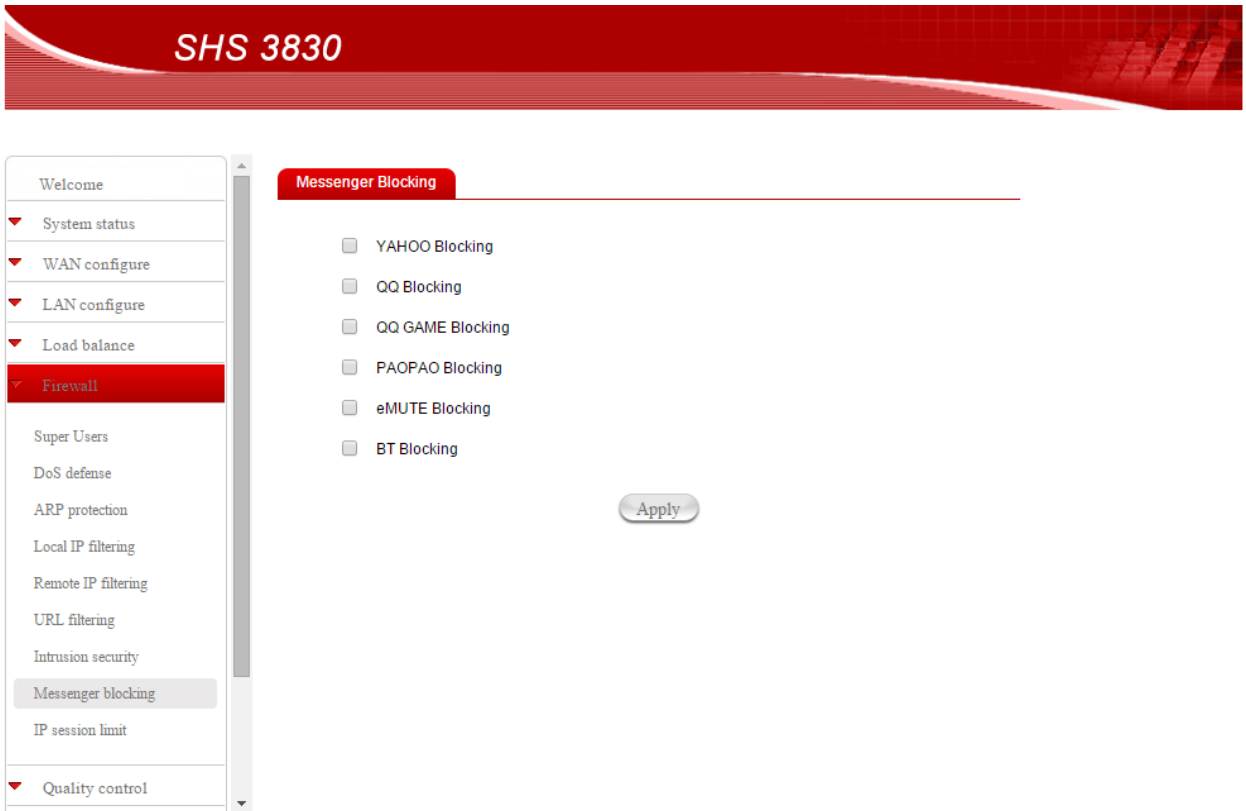




3.3.8 Messenger Blocking

Router can block below traffic packet from LAN to WAN. For some exception Router allow **Super users** IP can access Internet without limitation when enable block function Instant Message Blocking/ P2P BT Blocking

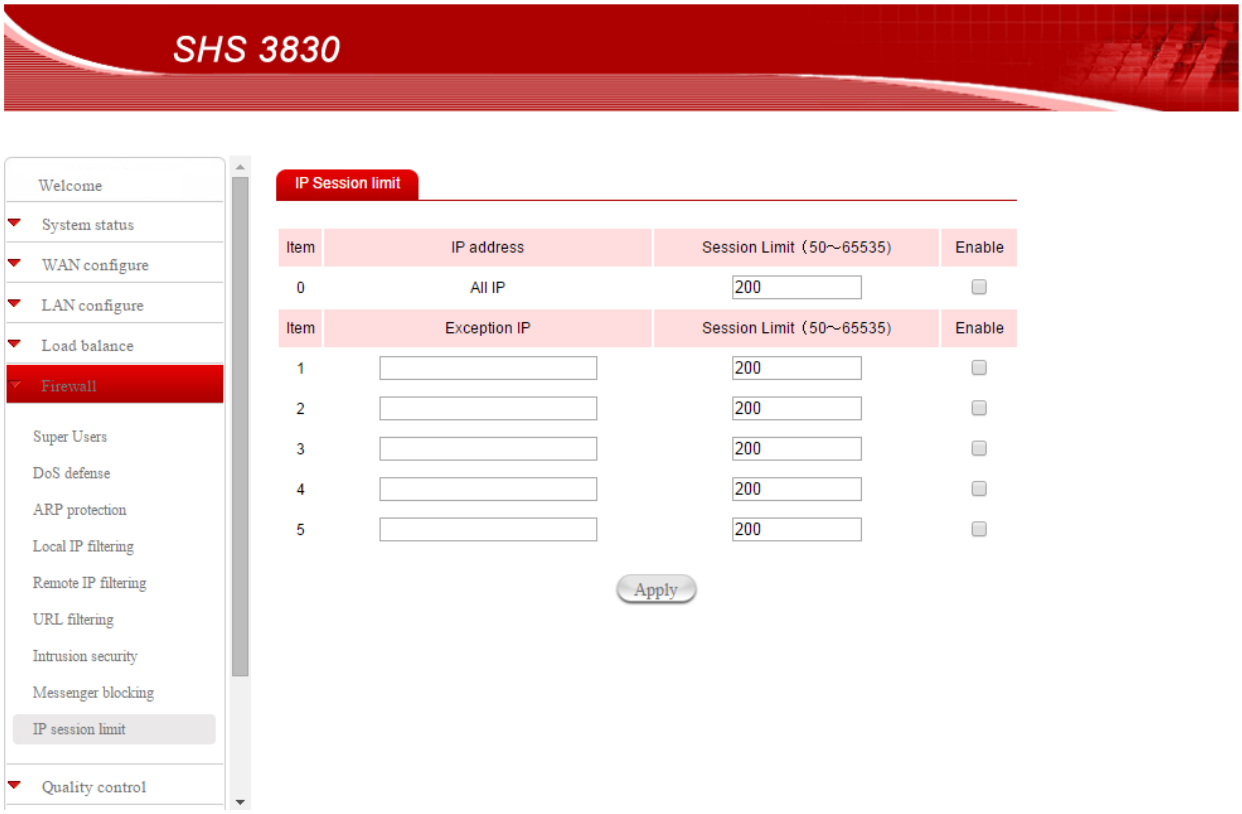
Firewall – Messenger blocking



3.3.9 IP session limit

For each user IP default session limit is 200. Session amounts per each IP can be change from 200 to 65,000.

Firewall – IP session limit



3.4 Quality control

- QoS
- Bandwidth control
- Outgoing route
- LAN IP speed limit

3.4.1 QoS

With this function, you can set up **USER BANDWIDTH** with Maximum & Minimum bandwidth value.

Configure WAN Speed

The WAN speeds must be configured for the QoS configuration to take effect.

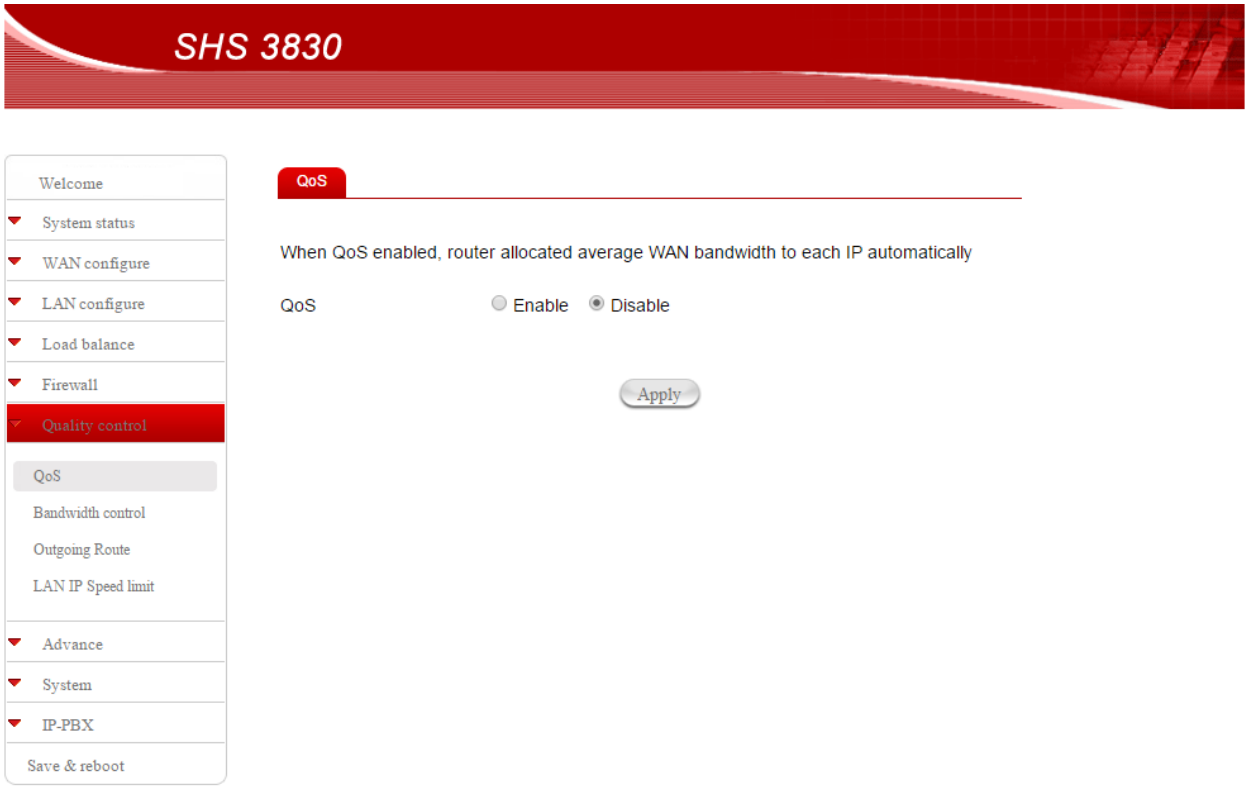
IP MAX/MIN Limit

Allocate bandwidths to users.

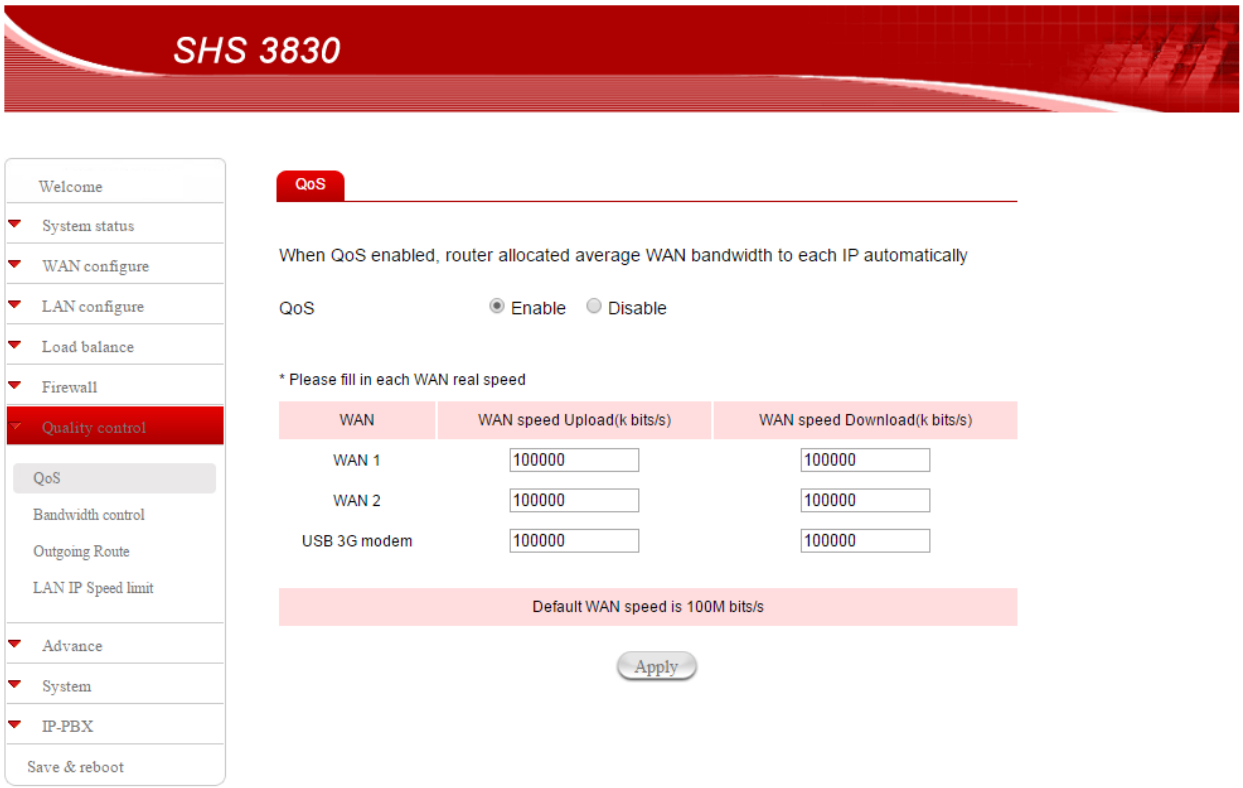
- IP: IP address of specified user.
- MAX: Bandwidth limitation to this user.
- MIN: Minimal Bandwidth kept for this user before allocating any bandwidth from this user to others.
- Down Rate: Download speed.

- Up Rate: Upload speed.
- WAN Apply: Which WAN you want the allocation to take effect. (Do not use this option to specify which WAN to use for this user.)

Quality Control – QoS



Quality control – QoS Enable



3.4.2 Bandwidth Control

This is a very useful function, it can let you to control WAN port bandwidth usage by each protocol. Like FTP

When someone uses FTP to transfer file, it will occupied heavy bandwidth, by using this function, you can limit allocated bandwidth.

Dedicated application bandwidth

For example:

In following display, FTP, HTTP & Mail bandwidth will be limit in certain percentage. This router provide 3 most often use protocol in the table, Just fill in port number and % usage for each application.

Protocol … name of protocol data packet will be limit.

Port … protocol port number

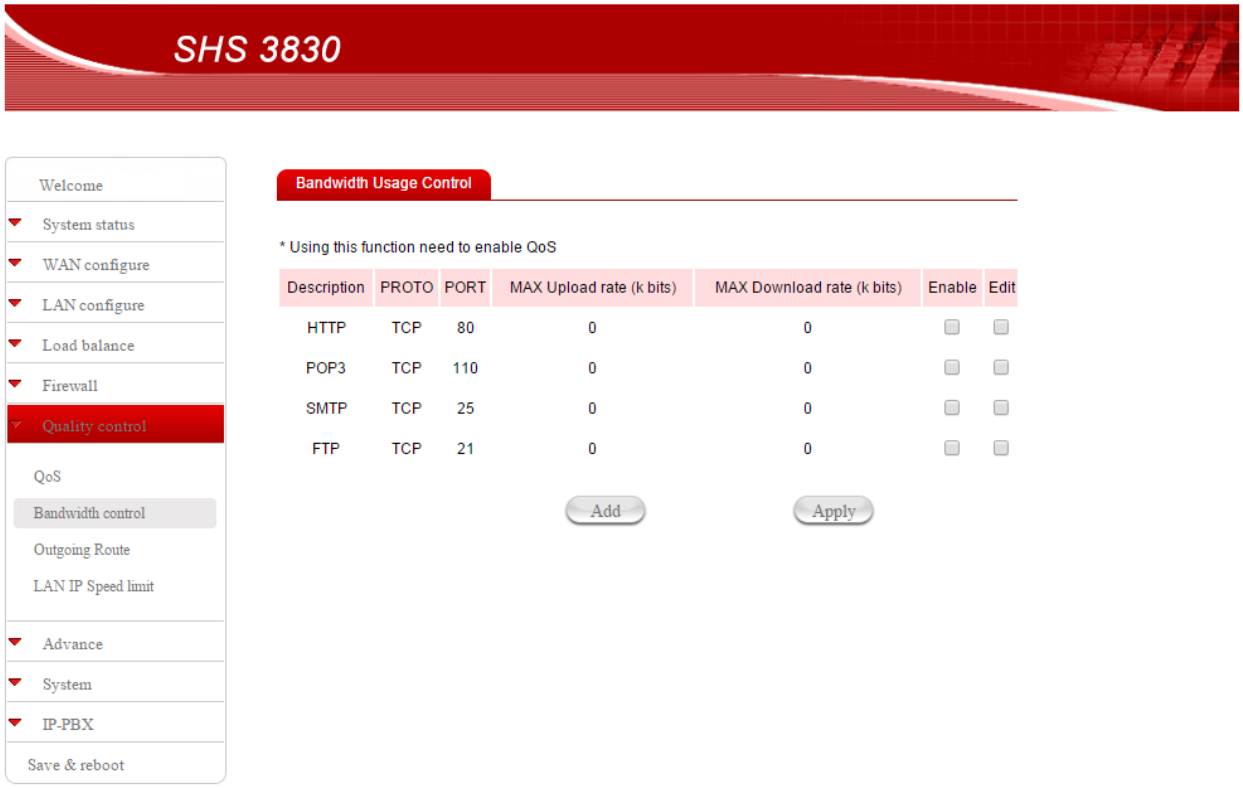
Usage: % of WAN speed can be used.

Protocol % usage cannot exceed 100% for each WAN port.

Router provides another 4-user self-define port number for easy use, just fill in port number for each protocol.

Step 1: Enter **Quality Control** web page.

Quality Control – Bandwidth usage control



Step 2: Clink the “Edit” check square of FTP. Then enter its edit page

Step 3: There are 5 fields in the page.

Description: It will be display in bandwidth table.

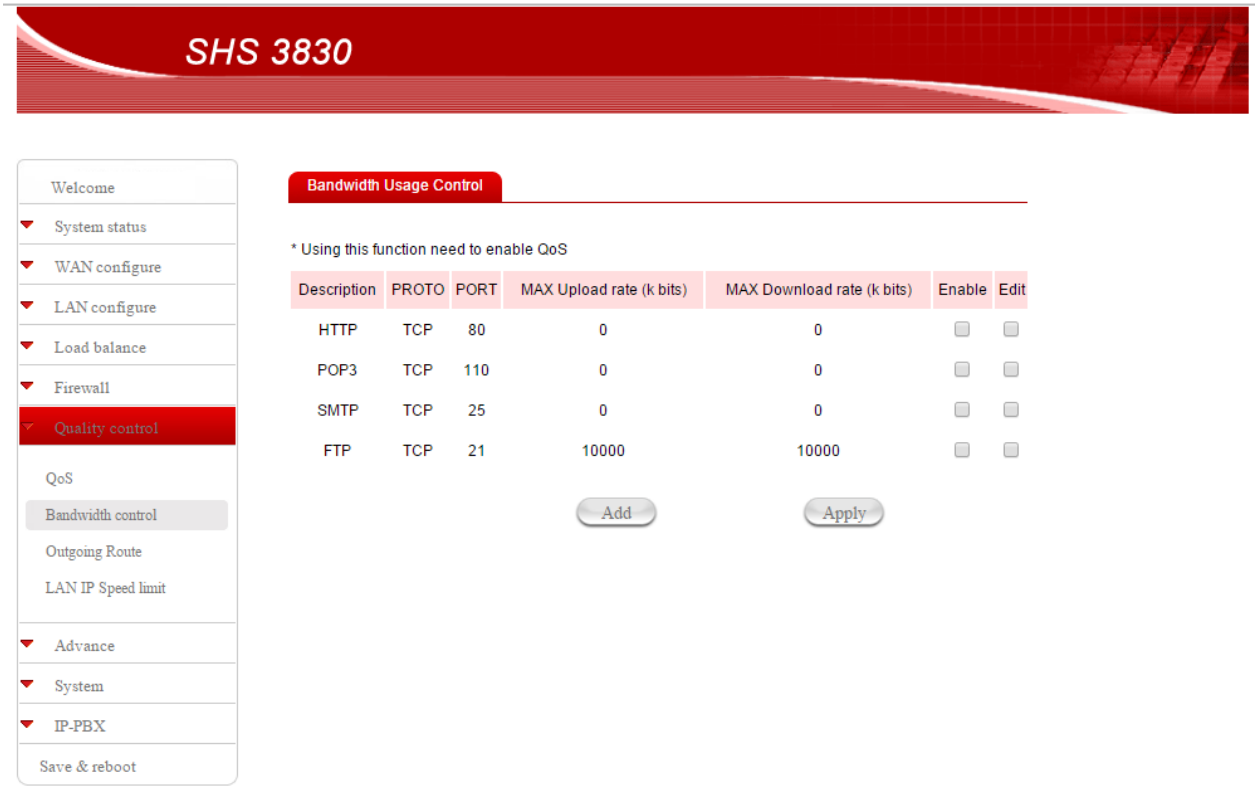
TCP/UDP: The AP use protocol. Example: FTP use TCP.

Port: The AP use port.

MAX Upload speed: The AP's maximum upload speed. Its unit is kbit.

MAX Download speed: The AP's maximum download speed. Its unit is kbit.

Finish the job then click "Apply" to save parameter and go back Bandwidth control table.

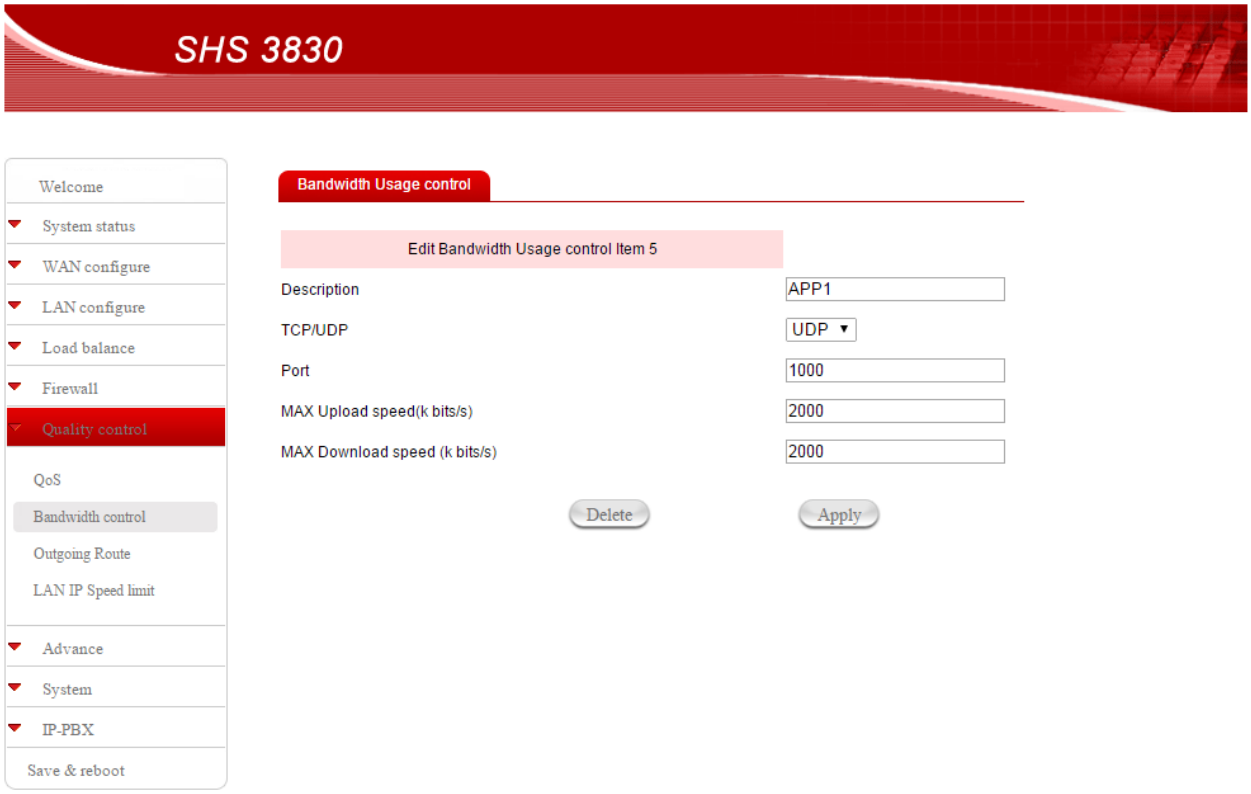


Step 4: Clink the “Enable” check square of FTP. Then Click “Apply”.

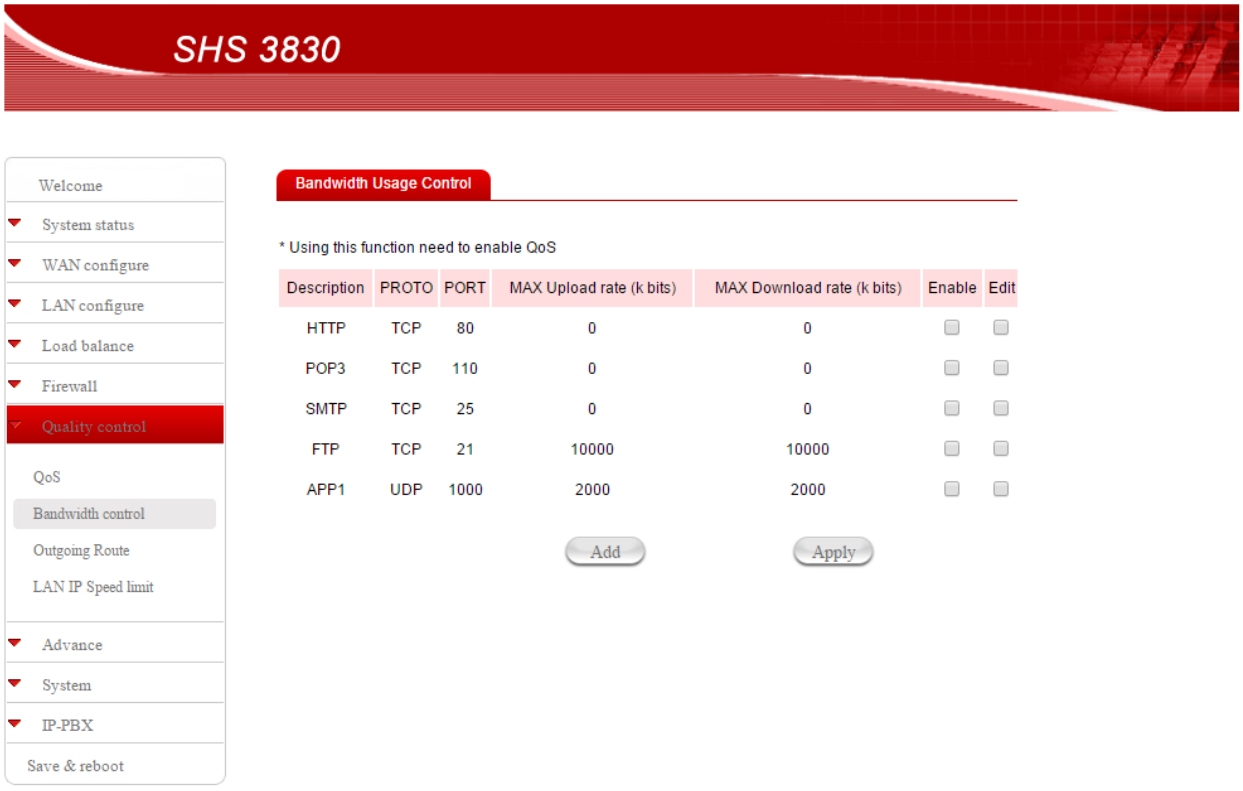
If user would like to create a new protocol, please follow below steps:

Step 1: Enter Bandwidth control web page.

Step 2: Clink the “Add” then enter its added page. Set parameters in below page. Then click “Apply”.



Step 3: Clink the “Enable” check square of APP1. Then Click “Apply”.



3.4.3 Outgoing route

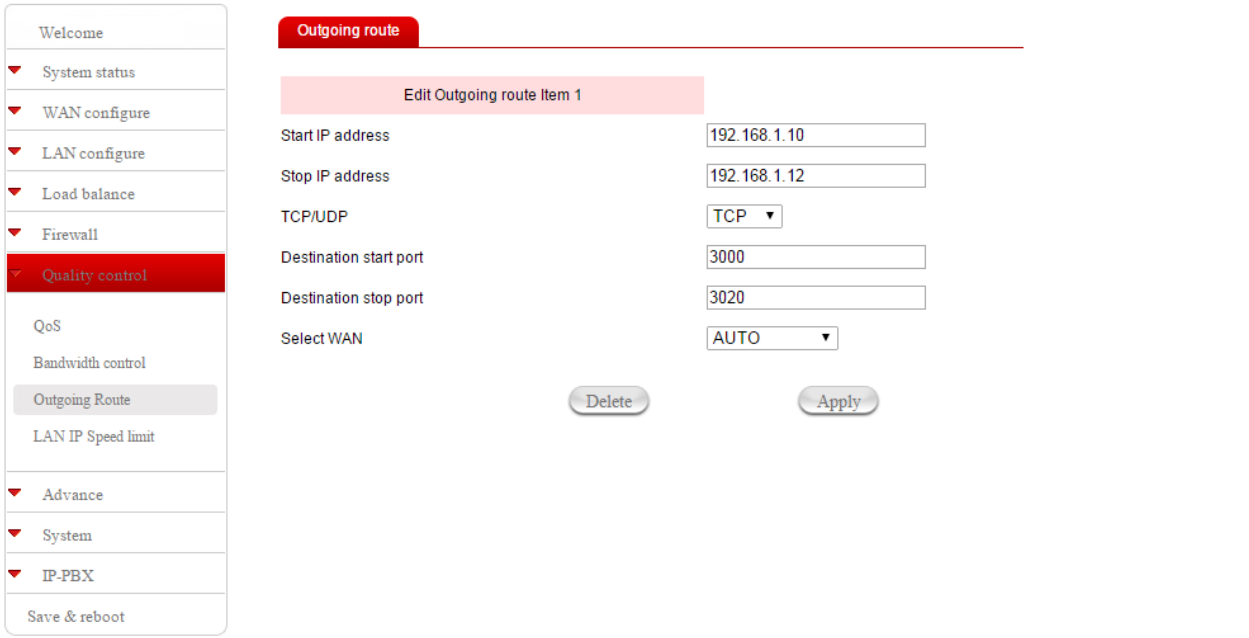
This function can let you arrange data packet from specific IP address to access Internet by designated WAN port. With this function, you can easily let VOIP packet or other special applications with high bandwidth in designated WAN port in order to have best performance.

Example: Add a new item.

Step 1: Enter **Outgoing route** web page. Then click “Add” to enter the added page.

Quality Control – Outgoing route

Step 2: Fill data to Destination network, Netmask and Gateway IP. Then Click “Add” then router goes back to **Outgoing route** list table.

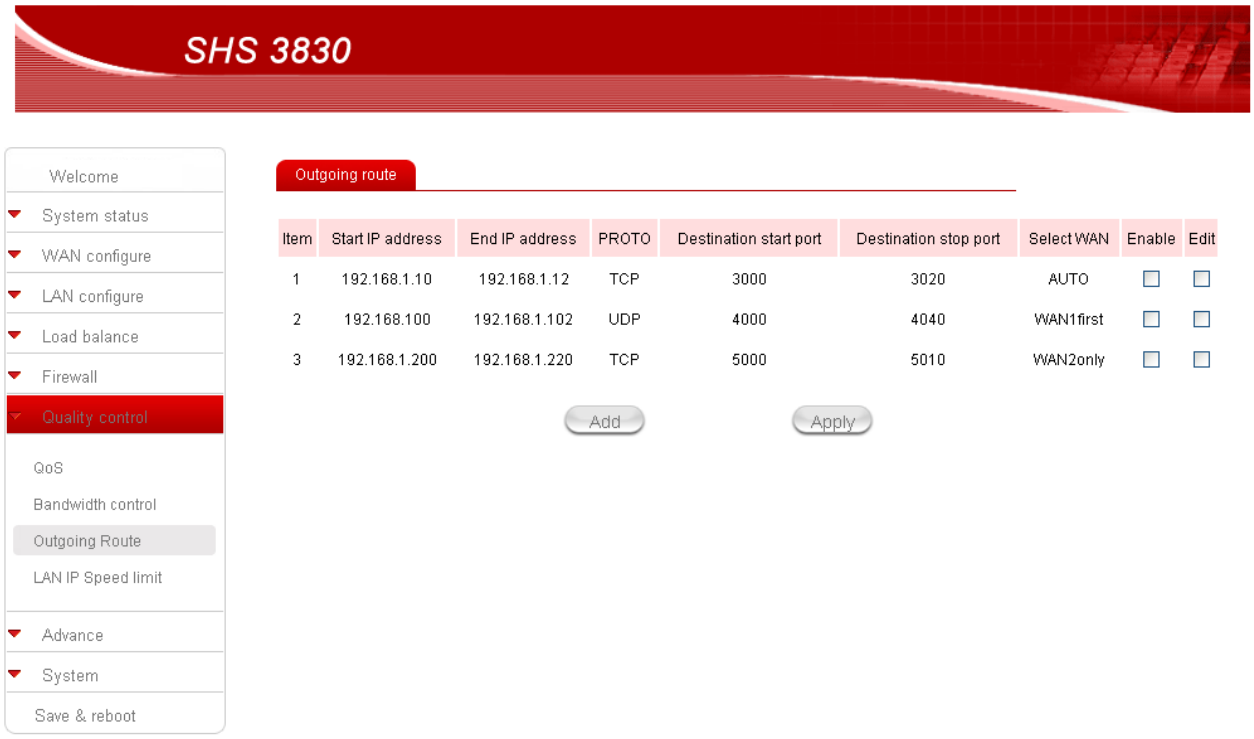


Note: Select WAN has 7 items. They are AUTO, WAN1 first, WAN2 first, USB3G first, WAN1 only, WAN2 only and USB3G only.

Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

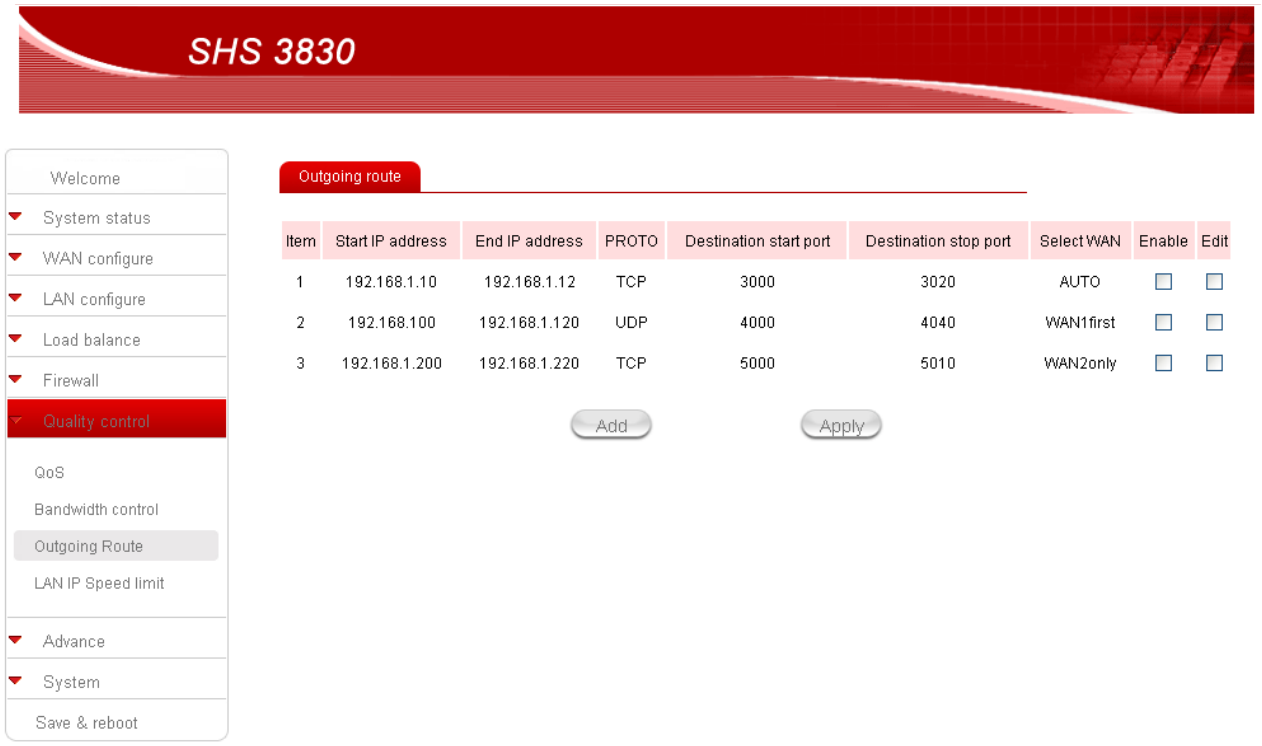
Example: Edit or Delete

Step 1: Enter **Outgoing route** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Outgoing route** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Outgoing route** list table.

Step 3: Router go back to **Outgoing route** list table.



3.4.4 LAN IP Speed limit

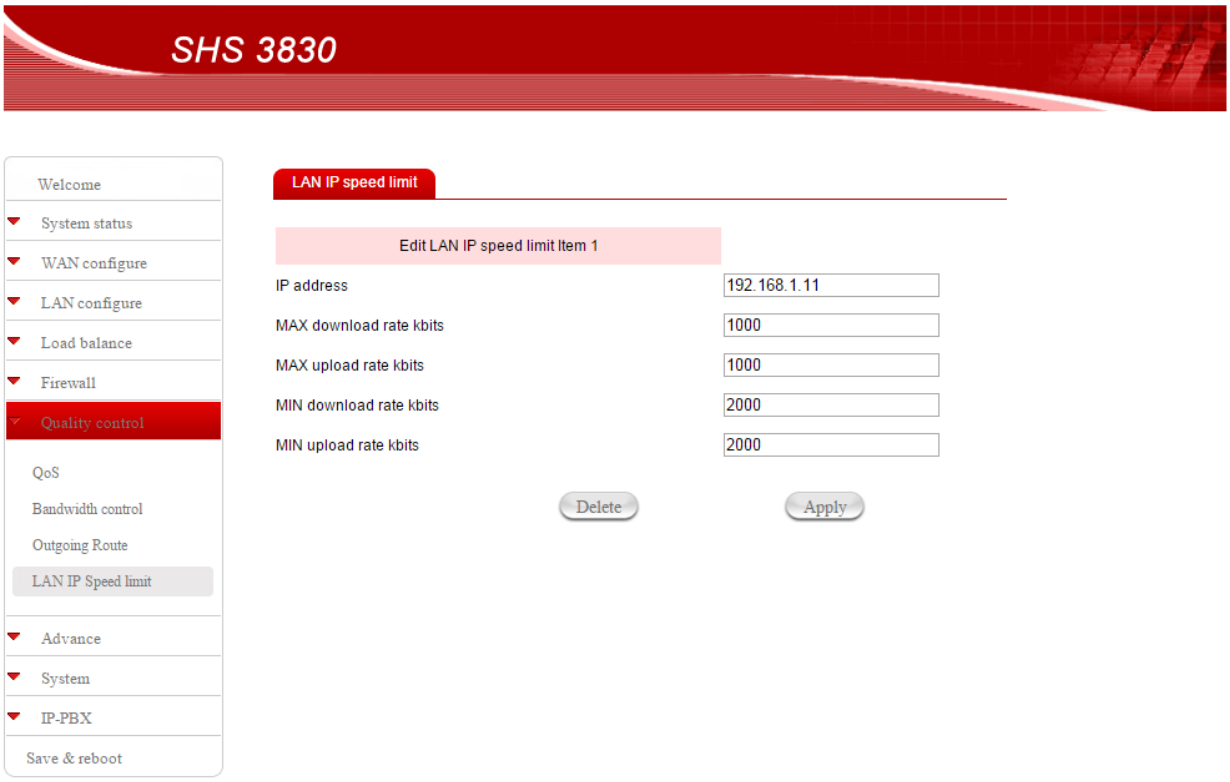
To limit each IP bandwidth allocation in LAN so that an IP may need high data rates for specific application can be satisfied to fulfill all demands. Before the feature is effective then user need to enable QoS first.

Example: Add a new item.

Step 1: Enter **LAN IP Speed limit** web page. Then click “Add” to enter the added page.

Quality Control – LAN IP Speed limit

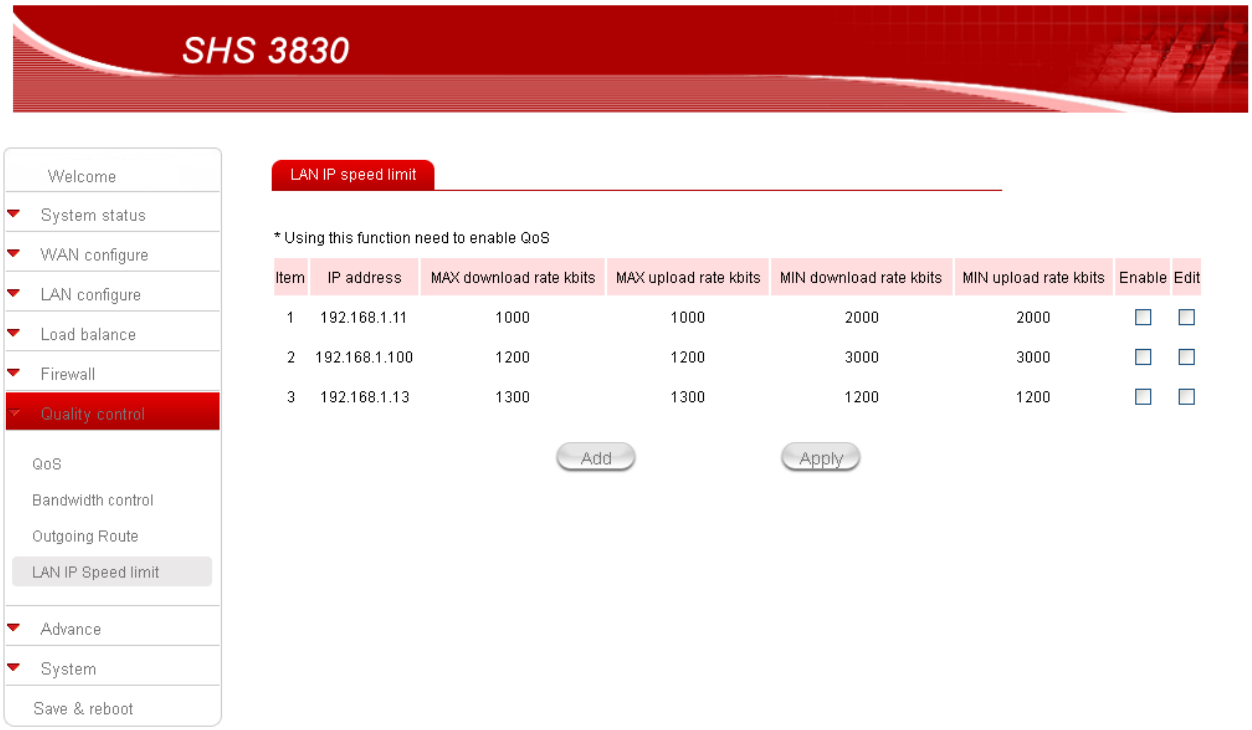
Step 2: Fill data to IP address, upload speed and Download speed. Then Click “Add” then router goes back to **LAN IP Speed limit** list table.



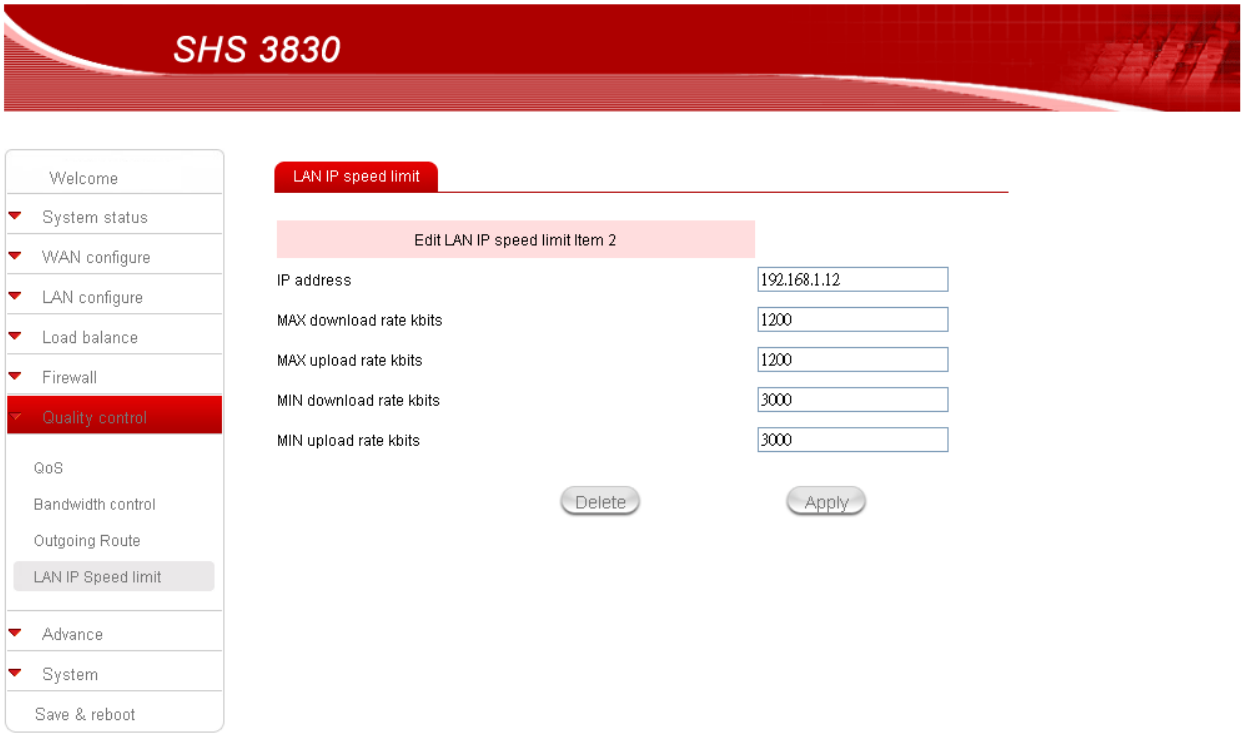
Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable

Example: Edit or Delete

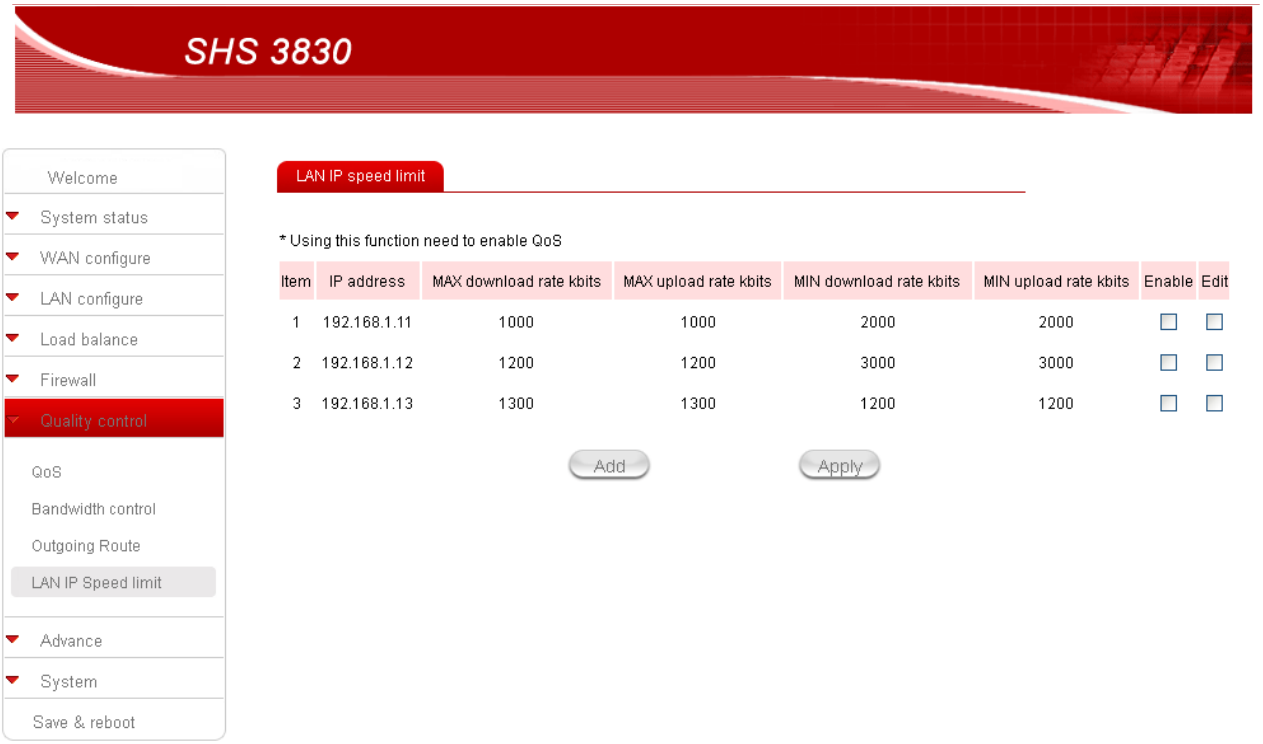
Step 1: Enter **LAN IP Speed limit** web page. Then click “Enable” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **LAN IP Speed limit** list table. If user wants to edit, click “add” when user finish editing job. Then router goes back to **LAN IP Speed limit** list table.



Step 3: Router go back to **LAN IP Speed limit** list table.



3.5 Advance

- VPN pass through
- DMZ
- Virtual server
- DDNS
- MAC clone
- Multi-NAT
- Inner DNS
- Routing configure

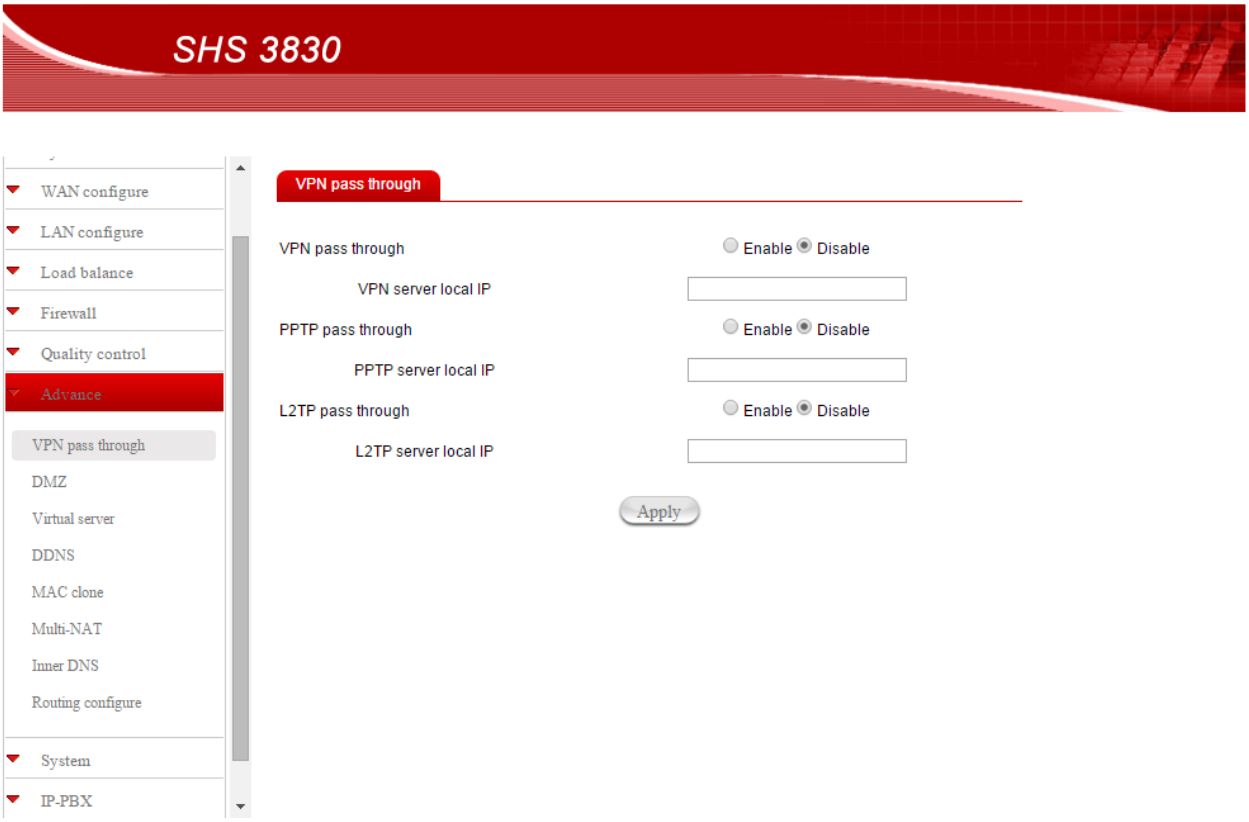
3.5.1 VPN pass through

VPN is the abbreviation for Virtual Private Network, which provide a secured link through public network by encrypting data between local and remote sides.

In order to pass through VPN traffic, router needs to recognize VPN packets and pass them in transparent way. VPN packets like IP Sec., PPTP and L2TP will not be affected and passed to the destination for appropriate process as desired.

Example: Select Pass through protocol and fill its local IP.

Advance – VPN pass through



3.5.2 DMZ

The Demilitarized Zone (DMZ) function provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers configured in DMZ Host list but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you keep all sensitive information off of the public servers. Please store sensitive information in computers on LAN.

If you would like to grant remote users the right to access one of your computers on LAN to perform some actions such as Internet games, you must enable the function of DMZ. When remote users access your legal IP(s), Load Balance Router will transmit these packets to the corresponding virtual IP(s).

Share-IP-DMZ

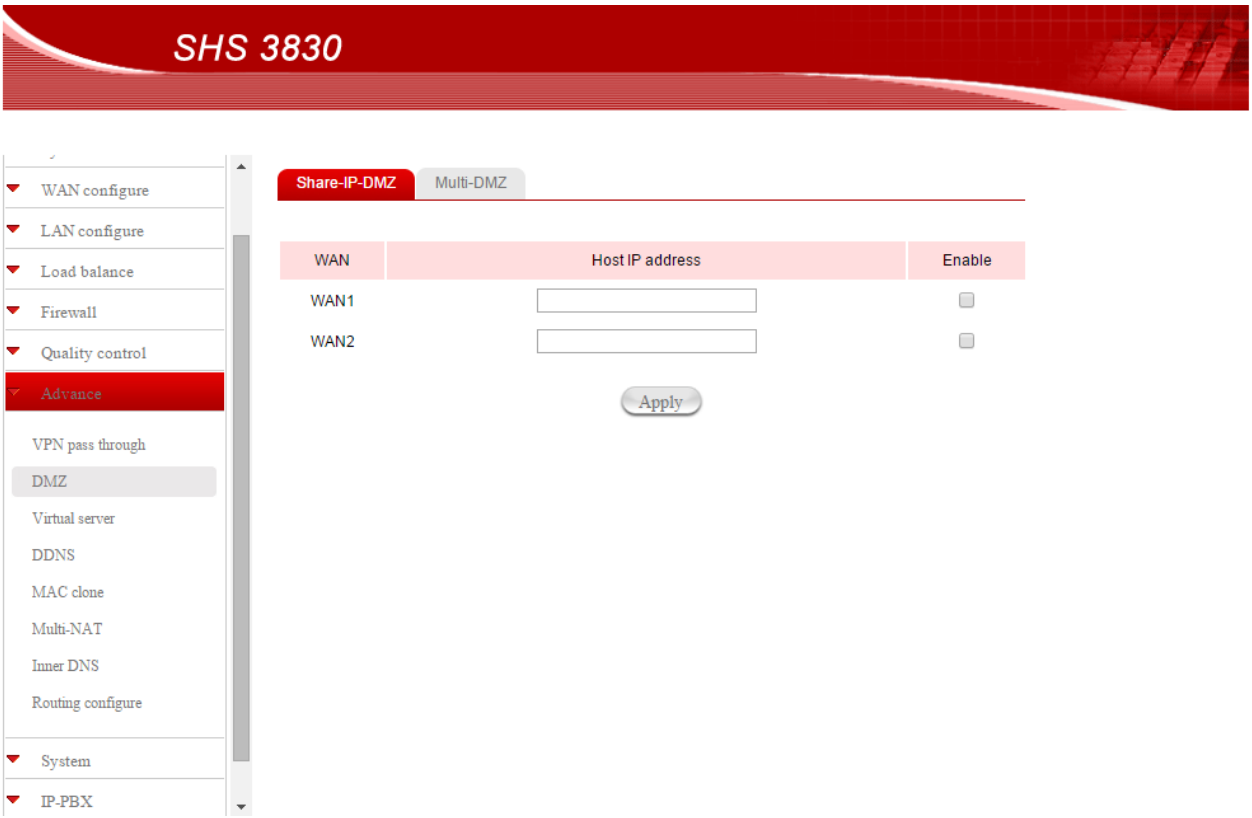
WAN: Host IP Address (PPPoe Mode)

When WAN port IP assigned by ISP obtained by PPPoE (**Dynamic IP**), you can fill

in DMZ host that inside the network, the router will mapping WAN IP to internal DMZ host automatically.

Example: Set the IP of WAN1 or WAN2. Click the “Enable” check square then click “Apply”

Advance – Share IP-DMZ



Multi-DMZ

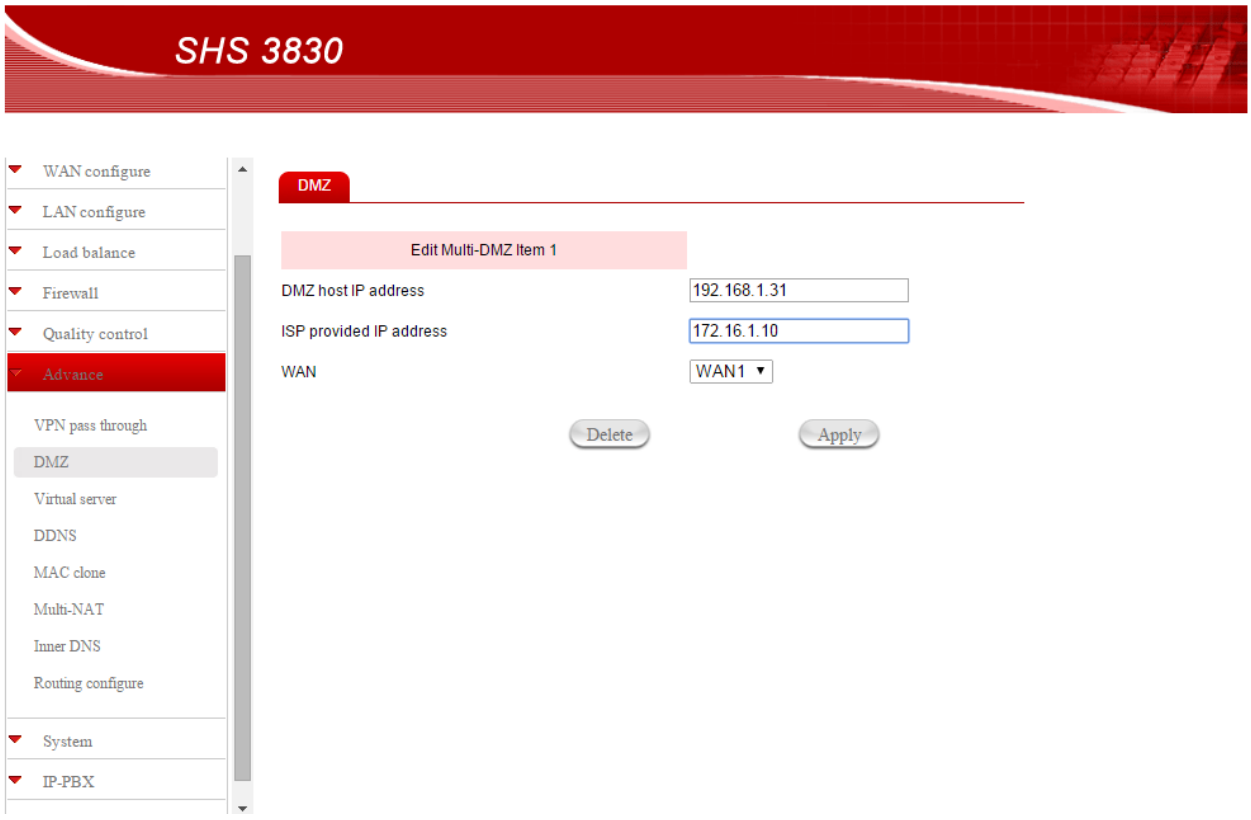
When using this function, the WAN port IP need to be **FIX IP** assigned by ISP.

Example: Add a new item.

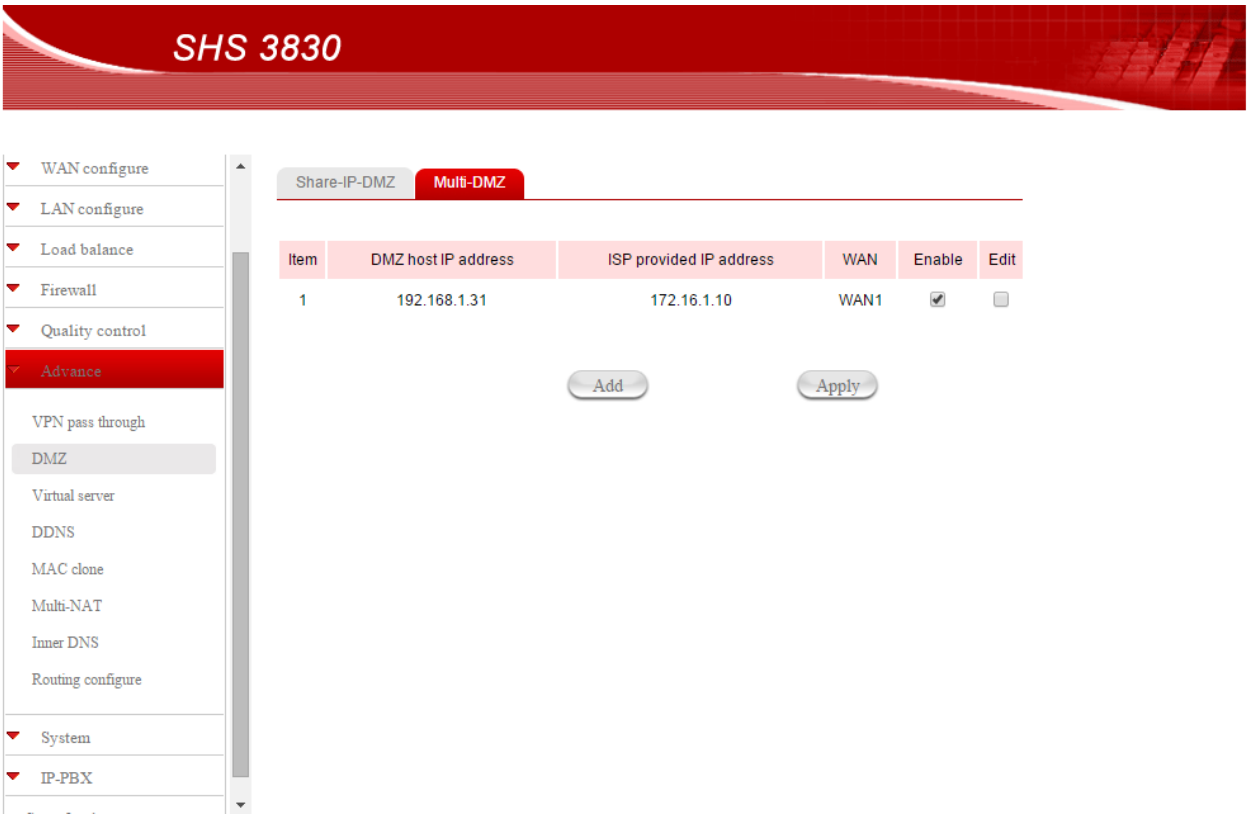
Step 1: Enter **Multi-DMZ** web page. Then click “Add” to enter the added page.

Advance – Multi-DMZ

Step 2: Fill data to DMZ host IP address, ISP provided IP address and WAN. Then Click “Add” then router goes back to **Multi-DMZ** list table.



Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



Example: Edit or Delete

Step 1: Enter **Multi-DMZ** web page. Then click “Enable” check square of item 2 to enter the edited page.

Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Multi-DMZ** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Multi-DMZ** list table.

Step 3: Router go back to **Multi-DMZ** list table.

3.5.3 Virtual server

You may have FTP, MAIL, VPN or other server on your LAN. If you would like to allow the global users access some servers providing special services on your LAN. This function can help you to do this.

Provide with global port & local port mapping function, let you easily configure internal server with same port number mapping to WAN IP different port number.

Global port: WAN virtual protocol number
Local port: used by internal server port number
Local IP: local server IP address

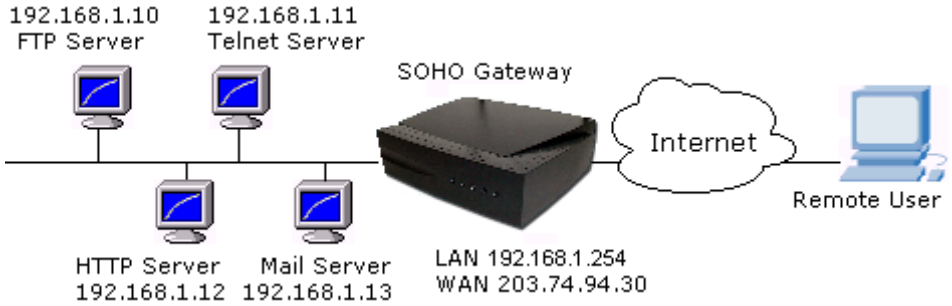
For multi-wan port router, no matter data packet coming in from which WAN port (WAN IP address), router will check incoming data port number only.

For example:

Global port number 1021 map into local server IP 192.168.1.10 port 21
Global port number 8080 map into local server IP 192.168.1.10 port 80
Global port number 2323 map into local server IP 192.168.1.25 port 23
Global port number 1100 map into local server IP 192.168.1.13 port 21

You also can configure
Global port number 1022 map into local server IP 192.168.1.20 port 21
same port number in local server with different global port number

Virtual server



For example,

Supposing you want to have four servers providing FTP, HTTP, Mail and Telnet services, you must enter four virtual servers and enable them.

If users key in ftp://203.74.94.30, Load Balance Router will send the data of FTP protocol to the server of 192.168.1.10.

If users use telnet software to connect to203.74.94.30, they will connect to the server of 192.168.1.11.

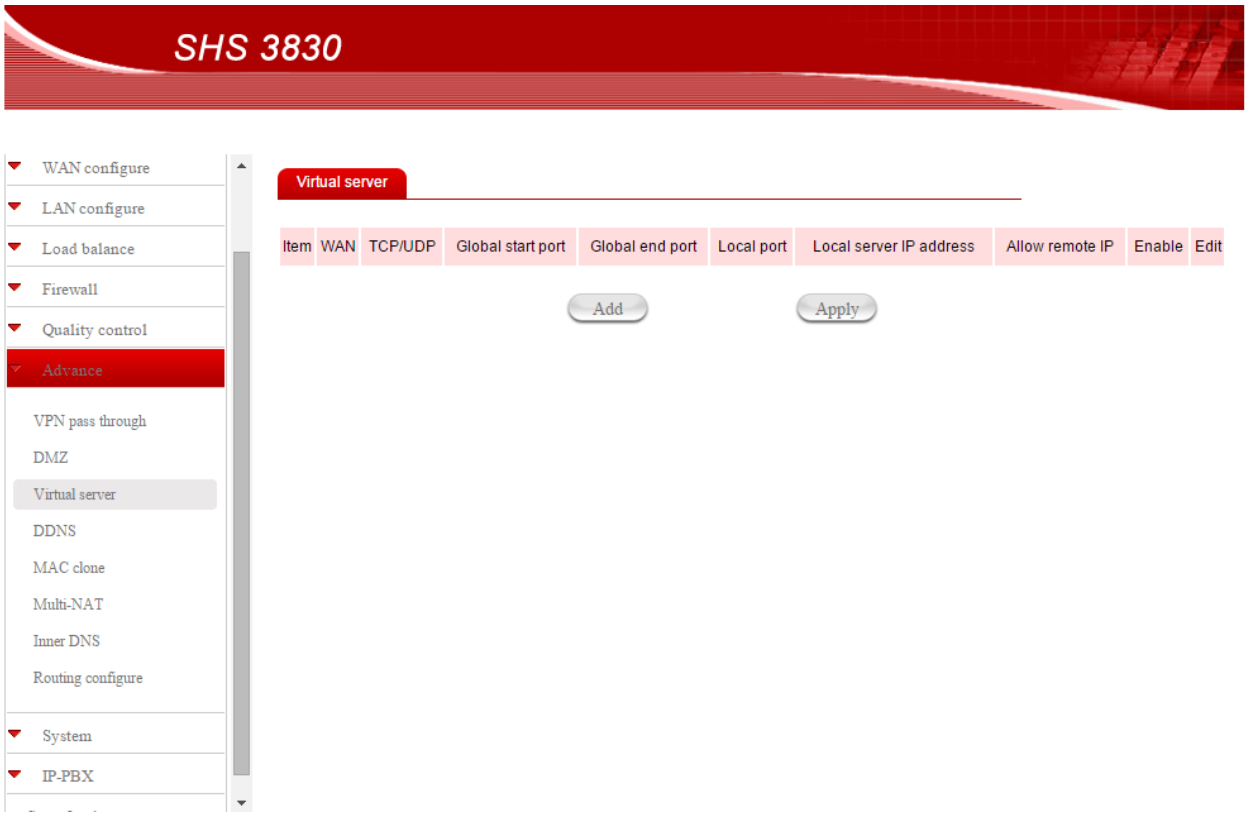
If users key in http://203.74.94.30, Load Balance Router will send the data of HTTP protocol to the server of 192.168.1.12.

If users use the email to connect to 203.74.94.30, they can receive the mails in Mail server of 192.168.1.13.
Group Virtual server eases user to configure a range of ports for some applications.

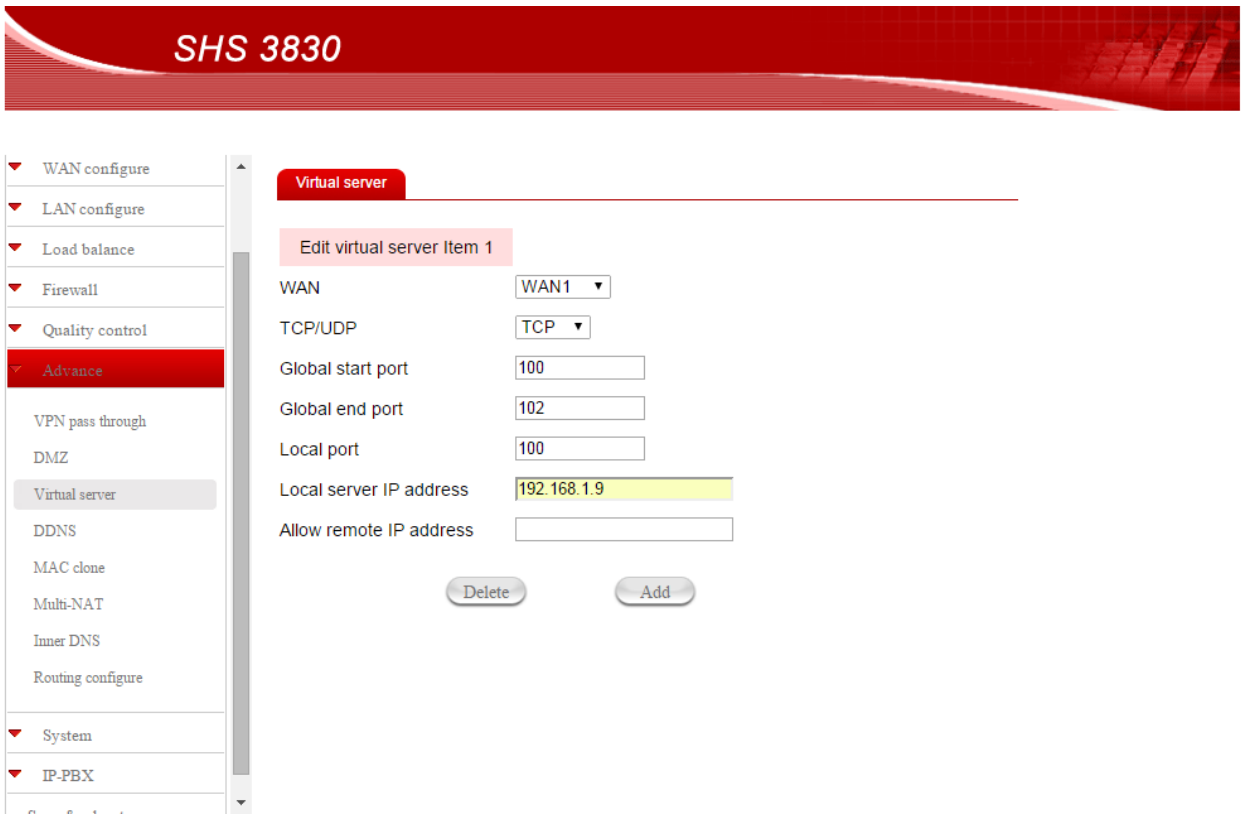
Example: Add a new item.

Step 1: Enter **Virtual server** web page. Then click “Add” to enter the added page.

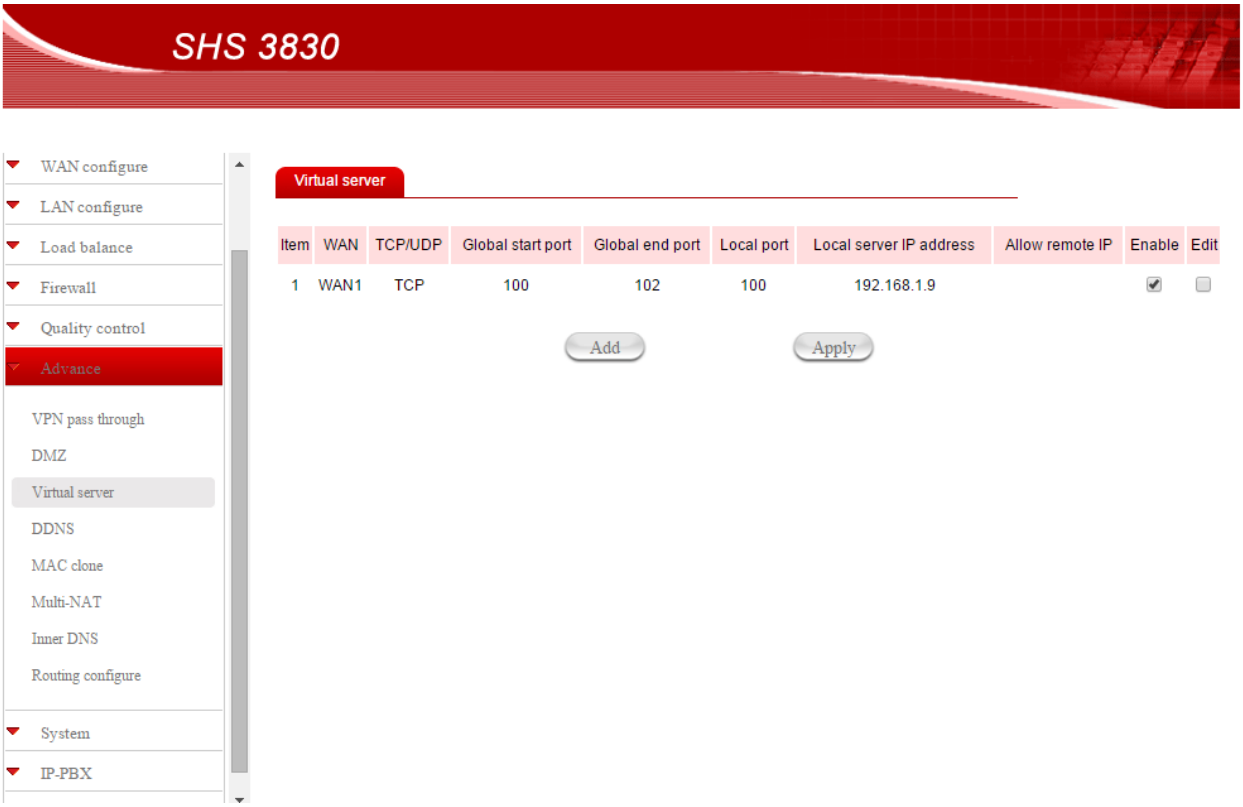
Advance – Virtual server



Step 2: Fill data to WAN, TCP/UDP, Global port, local port and local server address IP. Then Click “Add” then router goes back to **Virtual server** list table.

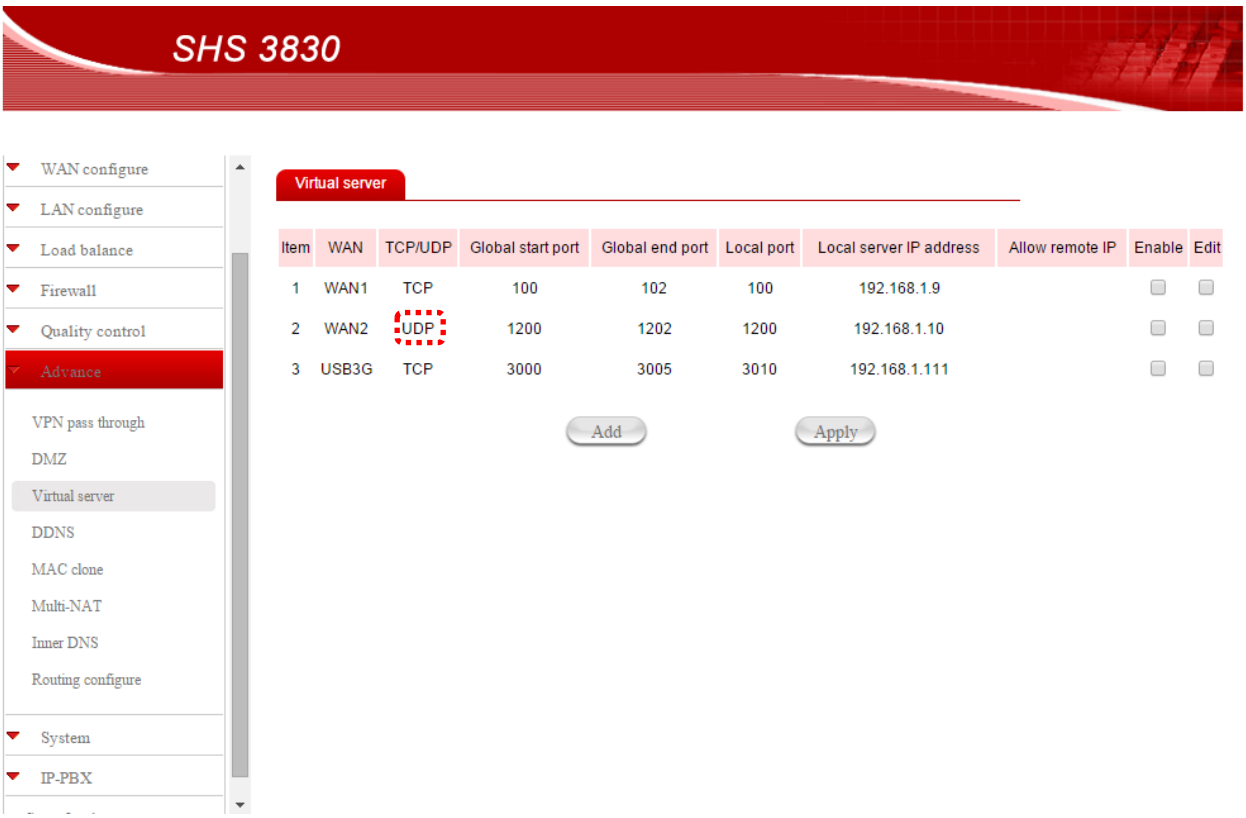


Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.



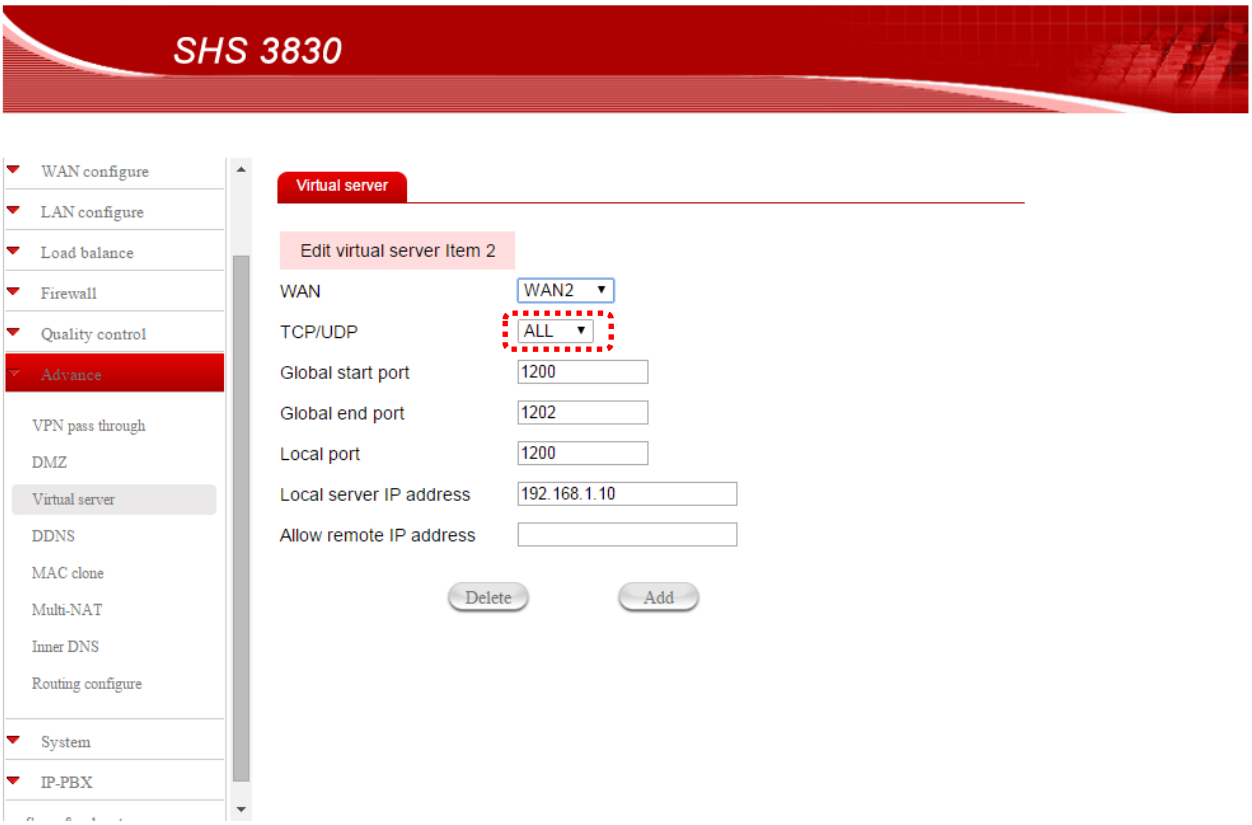
Example: Edit or Delete

Step 1: Enter **Virtual server** web page. Then click “Edit” check square of item 2 to enter the edited page.

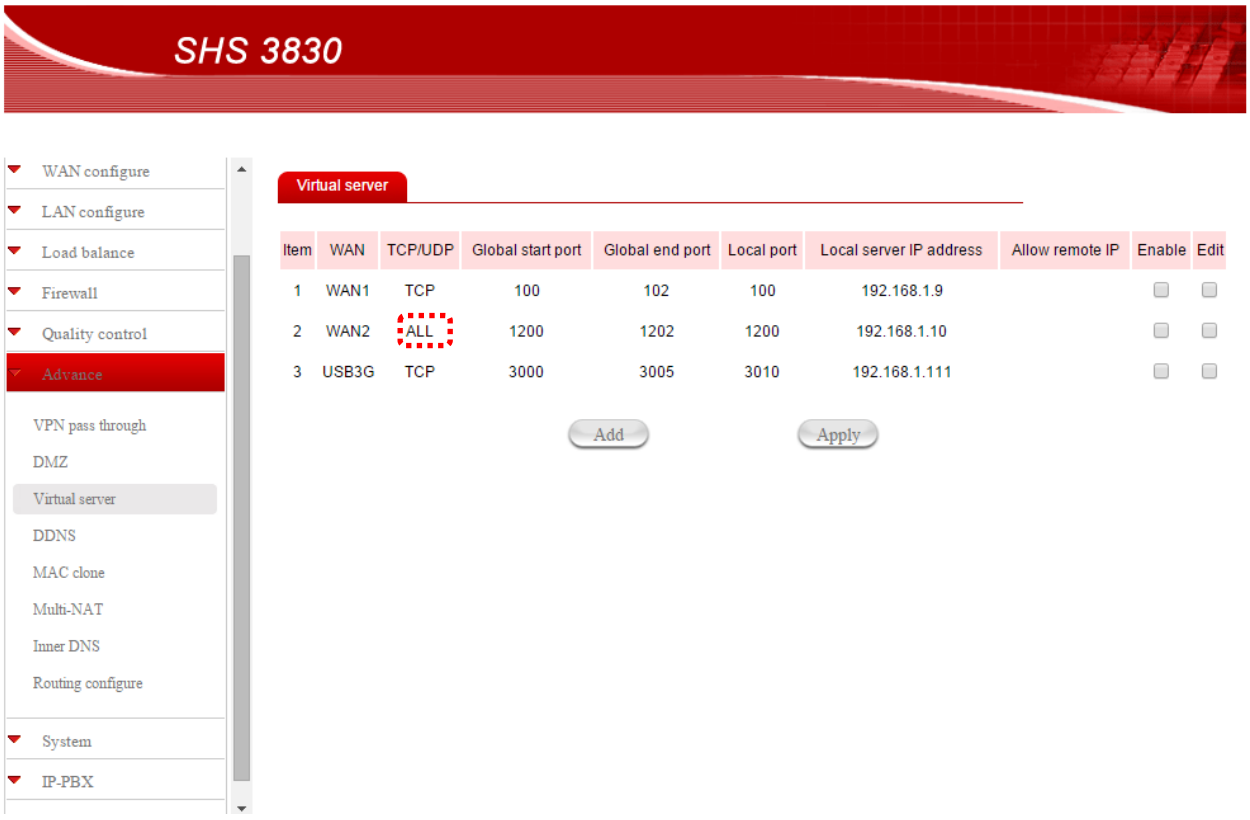


Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Virtual server** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Virtual server** list

table.



Step 3: Router go back to **Virtual server** list table.



3.5.4 DDNS

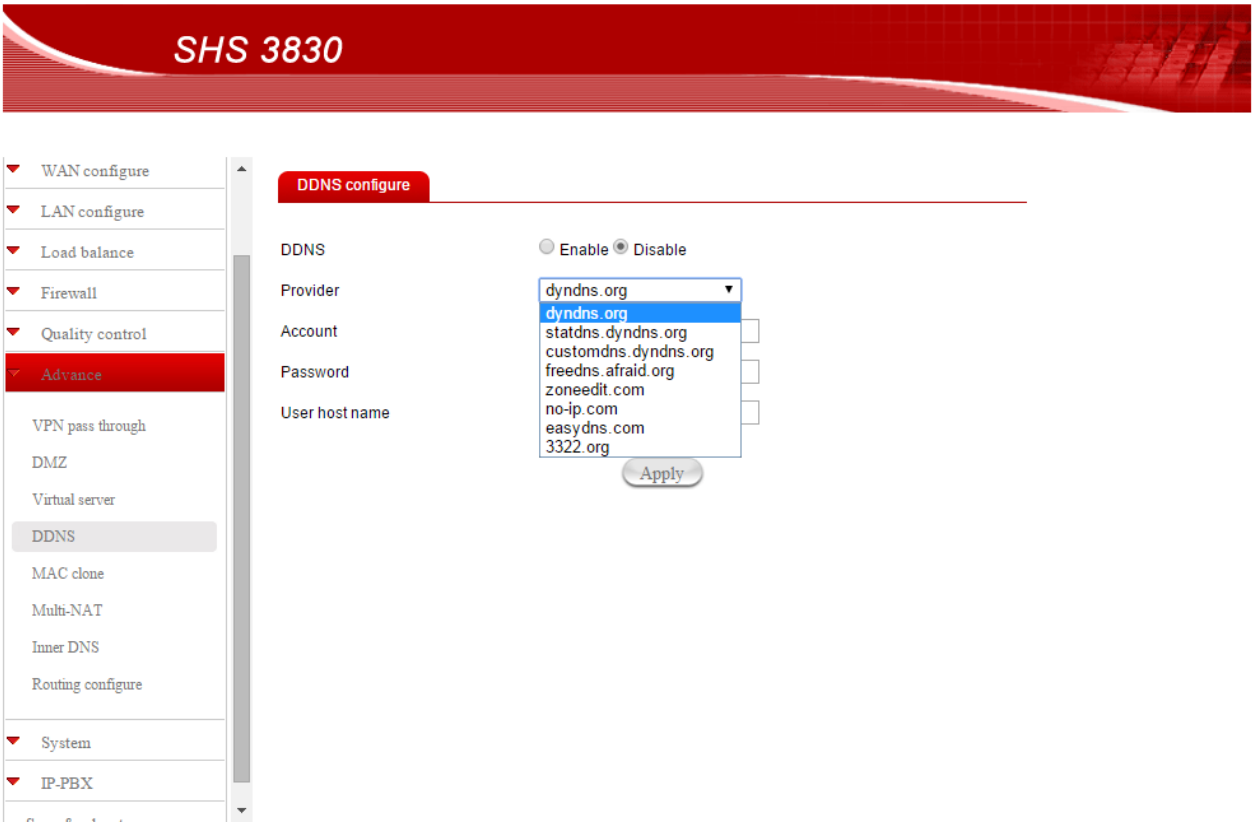
You need to apply for a free DNS domain name from DNS provider.

Example: dyndns.org. The SHS 3830 will update the WAN IP address to DDNS's

database once a WAN port was connected to Internet if DDNS function is enabled. And the users in Internet can find out the SHS 3830 via this domain name.

User Name: please apply from DNS provider.
Password: please apply from DNS provider.
User Hostname: please apply from DNS provider.

Advance – DDNS Configure



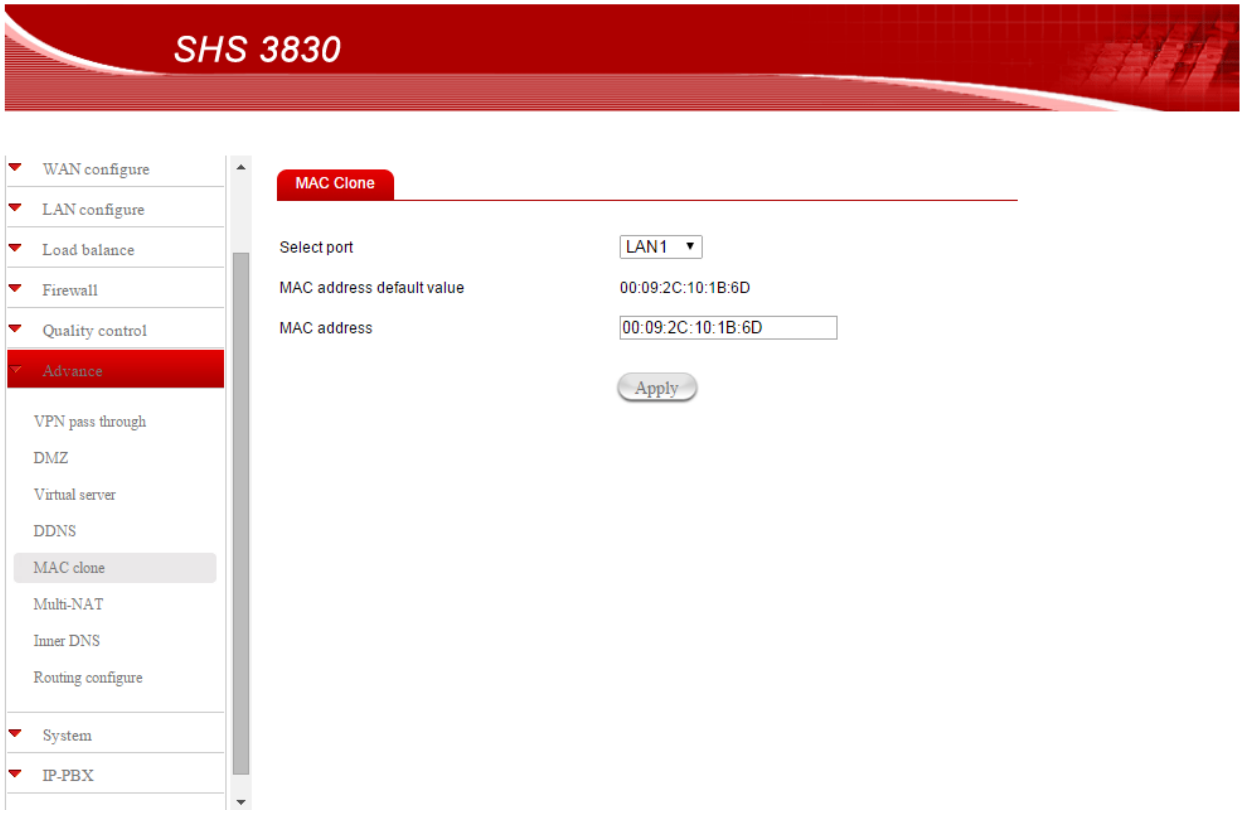
3.5.5 MAC clone

If your ISP blocked the MAC address of WAN port in router, you may use MAC Address Clone to duplicate the MAC address of PC in LAN to replace the Mac address in each WAN port.

Remove all Ethernet cable on Load Balance Router LAN port except for the PC you want to clone. Then press **Ok** when you ready.

Example: Select LAN or WAN1 or WAN2. Then fill a new MAC to MAC address

Advance – MAC Clone



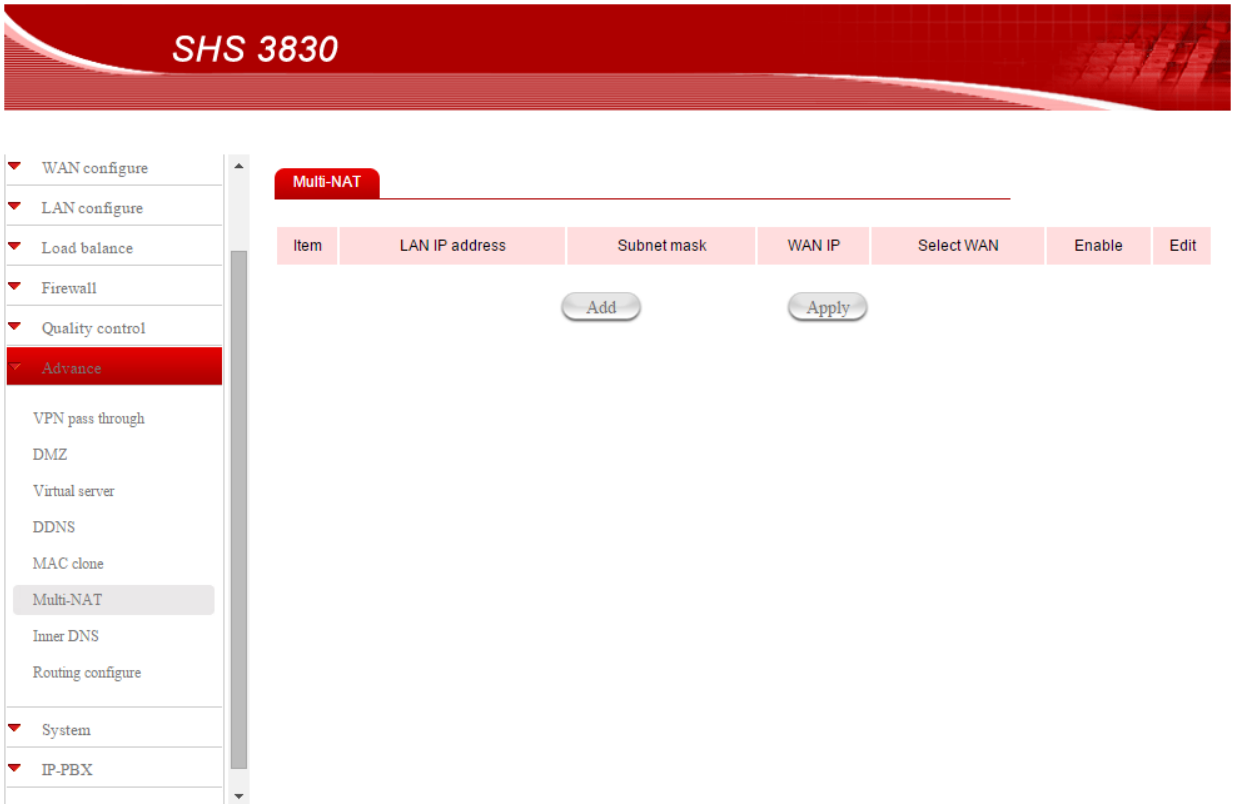
3.5.6 Multi-NAT

Multi-NAT function allow you to configure multiple LAN IP Domain to each WAN port, after configure multiple NAT function It will act like have virtual router connect to SHS 3830 LAN port, all traffic between each LAN IP domain , will send and receive through SHS 3830. SHS 3830 provides following benefit.

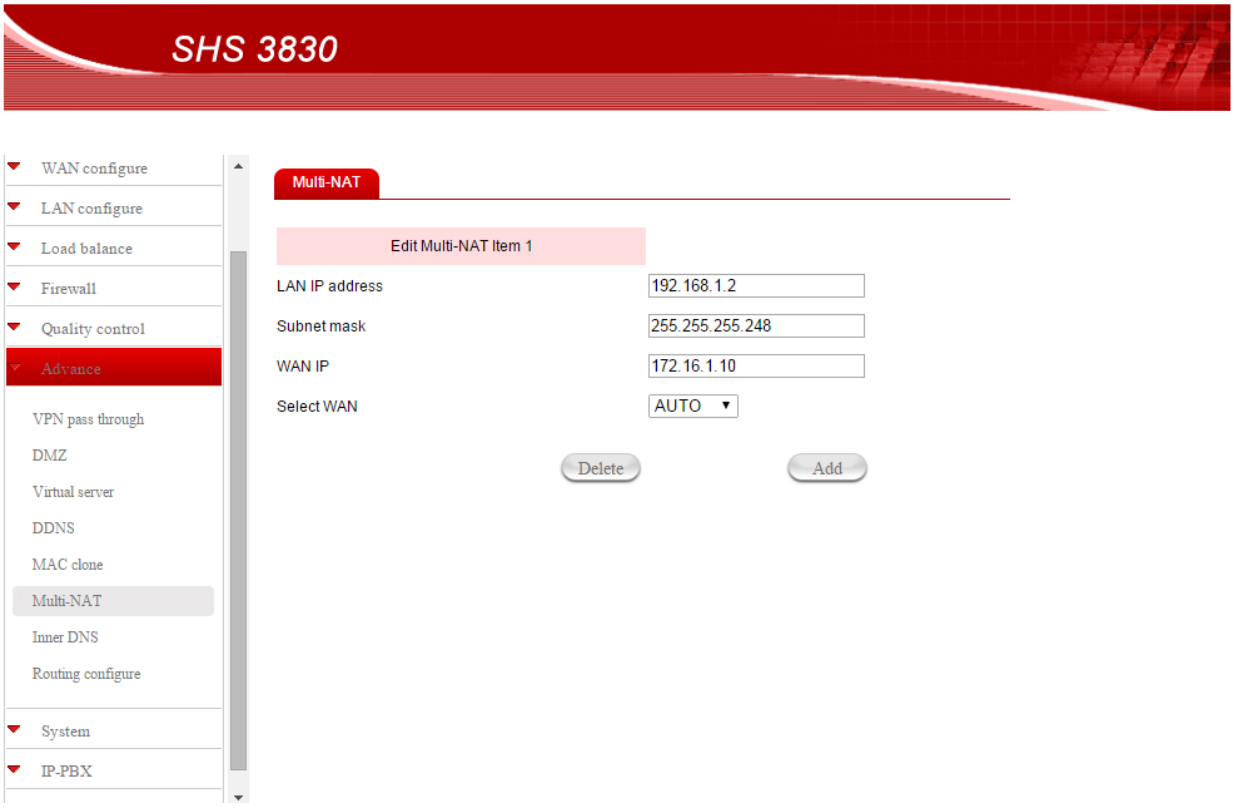
Example: Add a new item.

Step 1: Enter **Multi-NAT** web page. Then click “Add” to enter the added page.

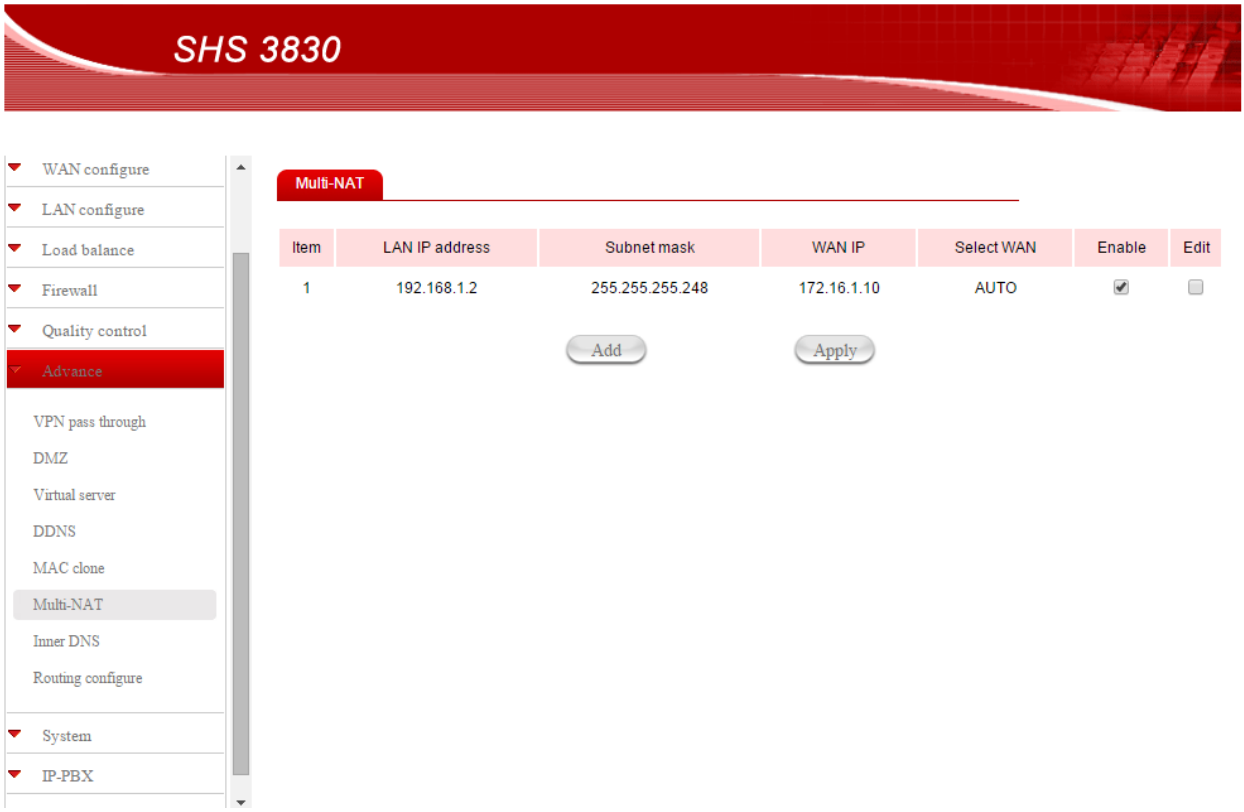
Advance – Multi-NAT



Step 2: Fill data to LAN IP address, Subnet mask, WAN IP and Select WAN. Then Click “Add” then router goes back to **Multi-NAT** list table.

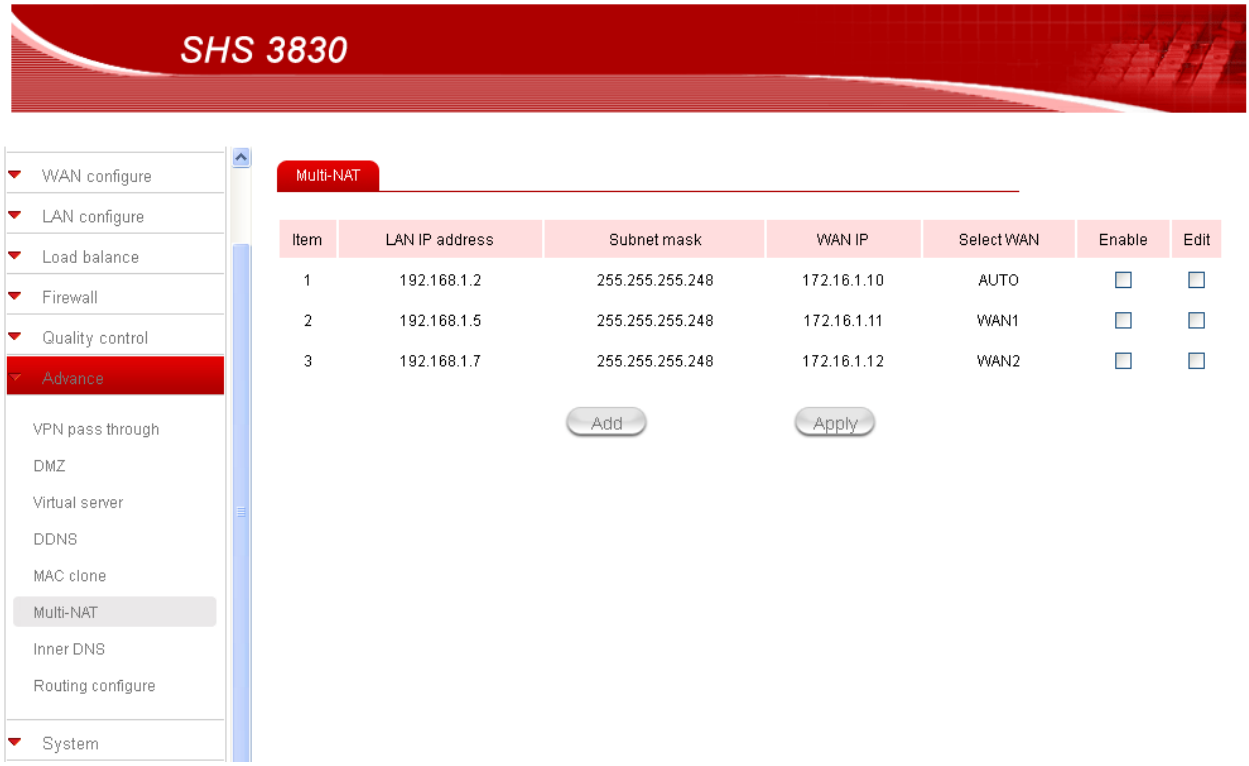


Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

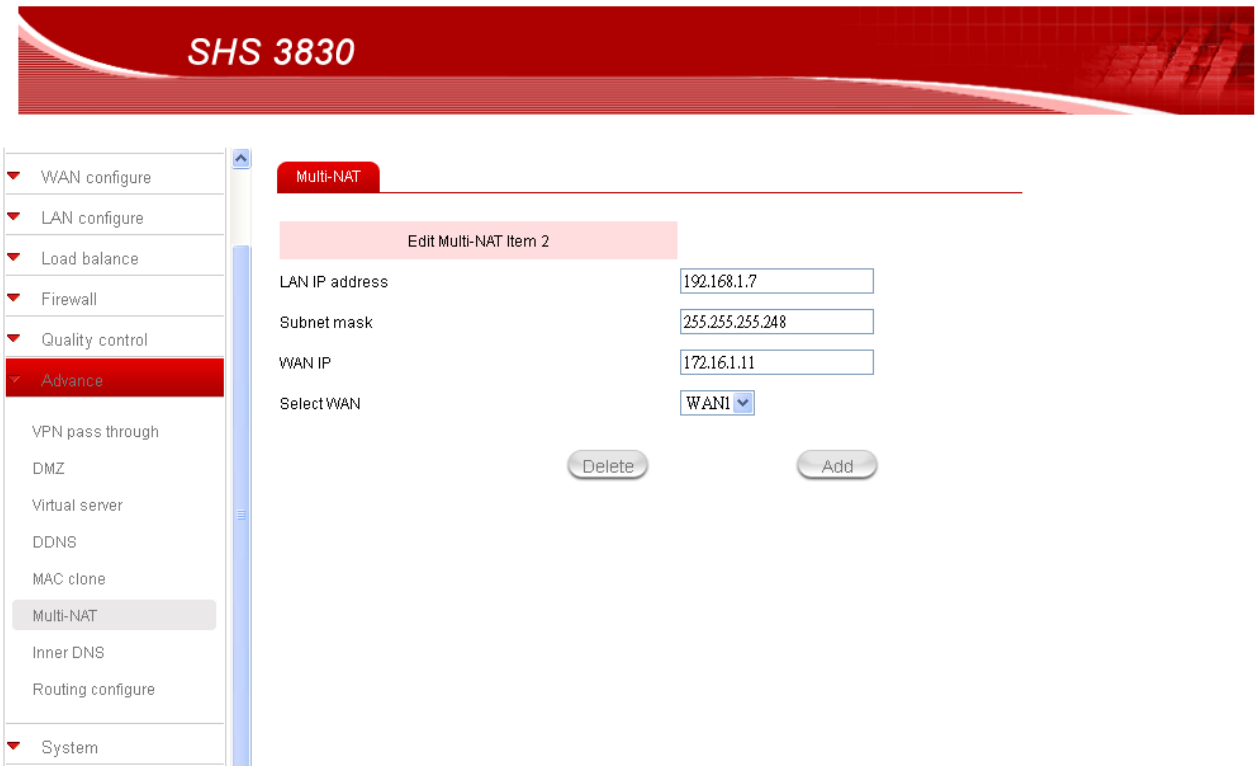


Example: Edit or Delete

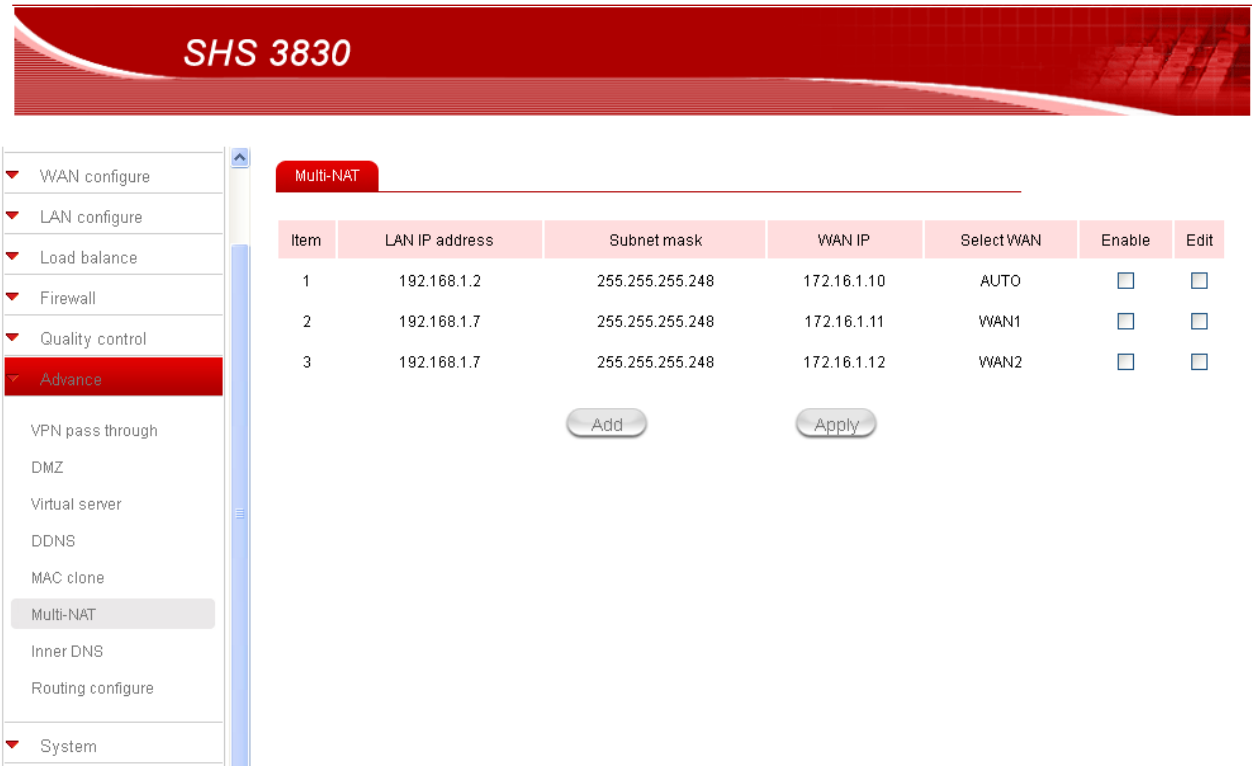
Step 1: Enter **Multi-NAT** web page. Then click “Edit” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Multi-NAT** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Multi-NAT** list table.



Step 3: Router go back to **Multi-NAT** list table.



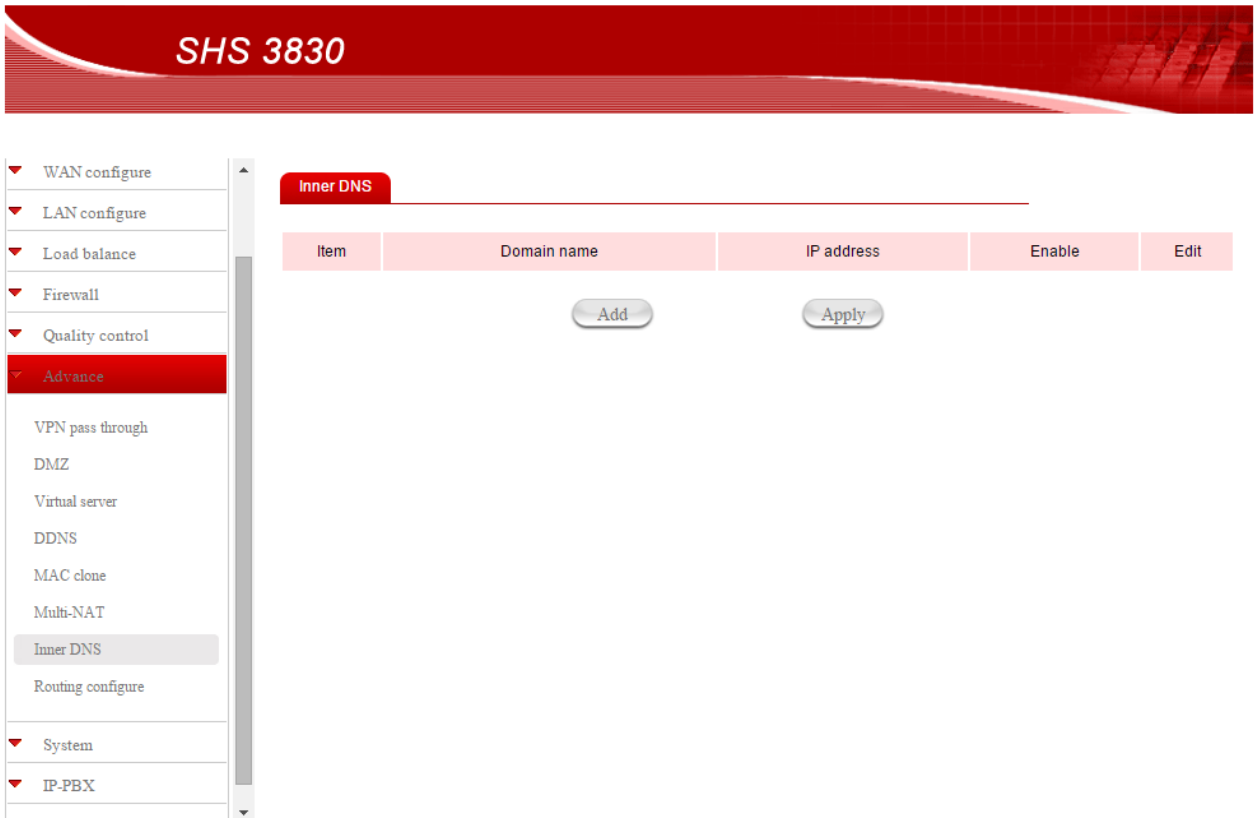
3.5.7 Inner DNS

In order to speed out DNS request process for quick surfing internet, Inner DNS works as a cache to retain DNS information for hosts DNS lookup.

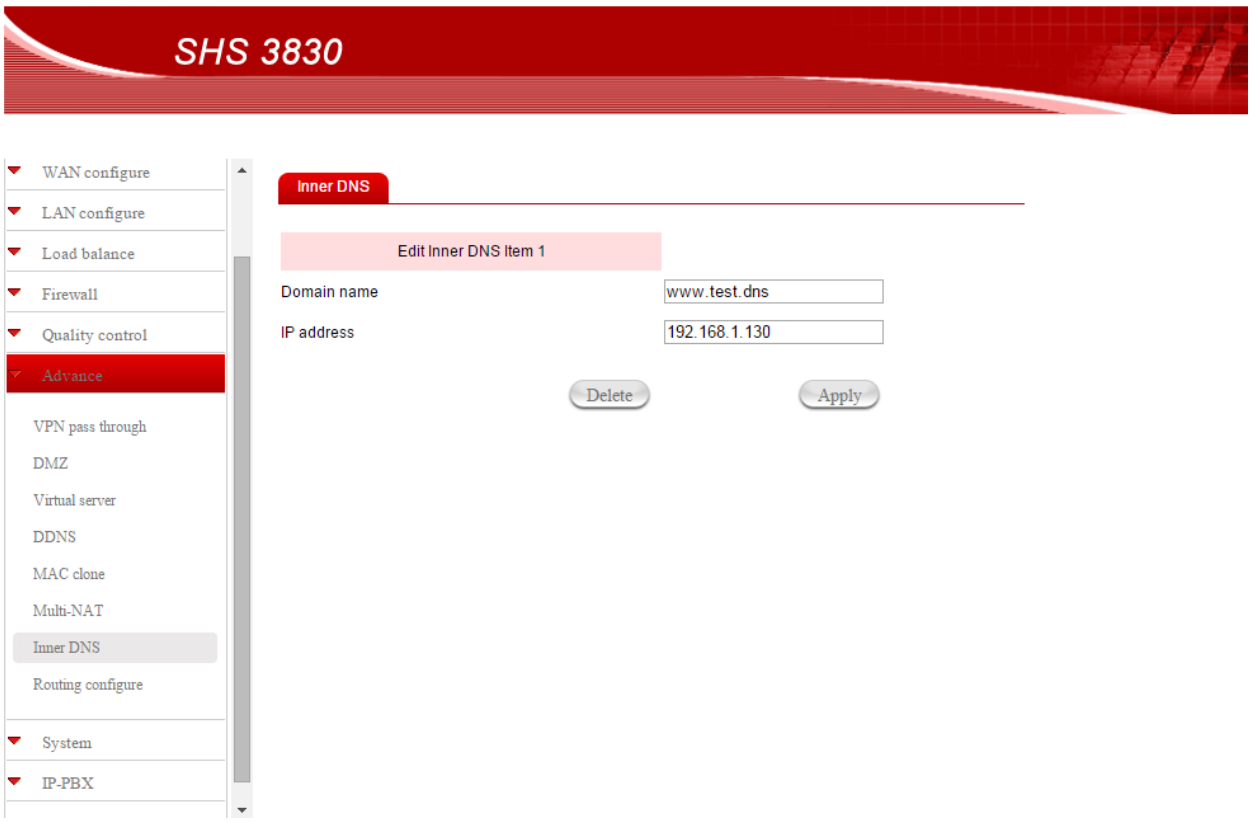
Example: Add a new item.

Step 1: Enter **Inner DNS** web page. Then click “Add” to enter the added page.

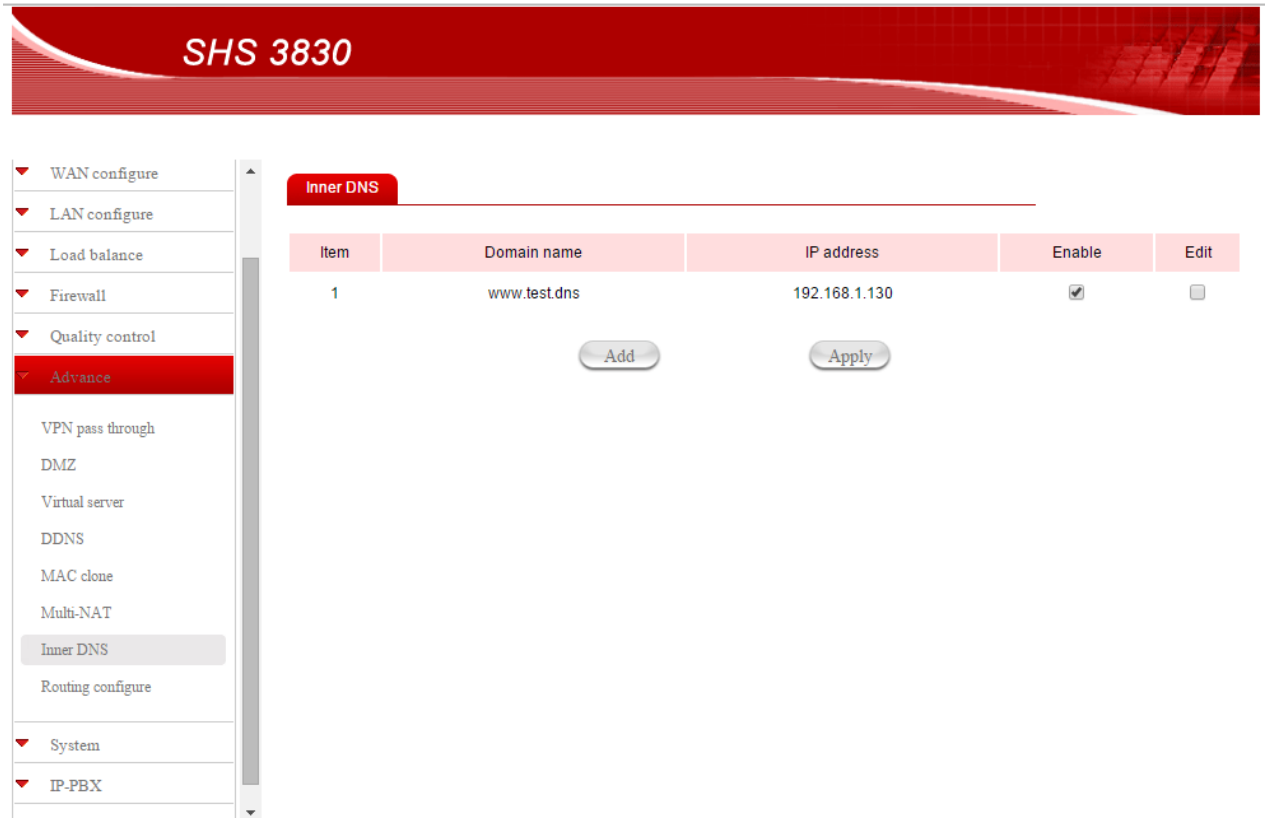
Advance – Inner DNS



Step 2: Fill data to Domain Name and its IP. Then Click “Add” then router goes back to **Inner DNS** list table.

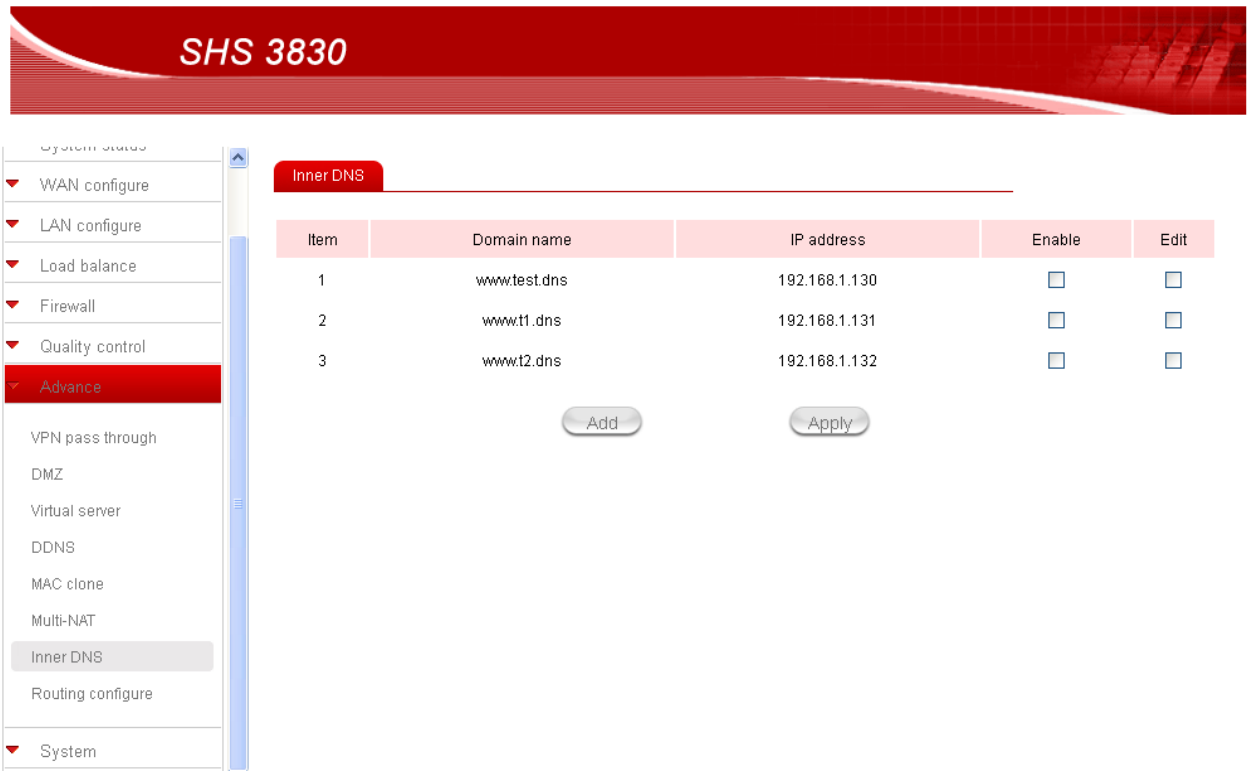


Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and enable.

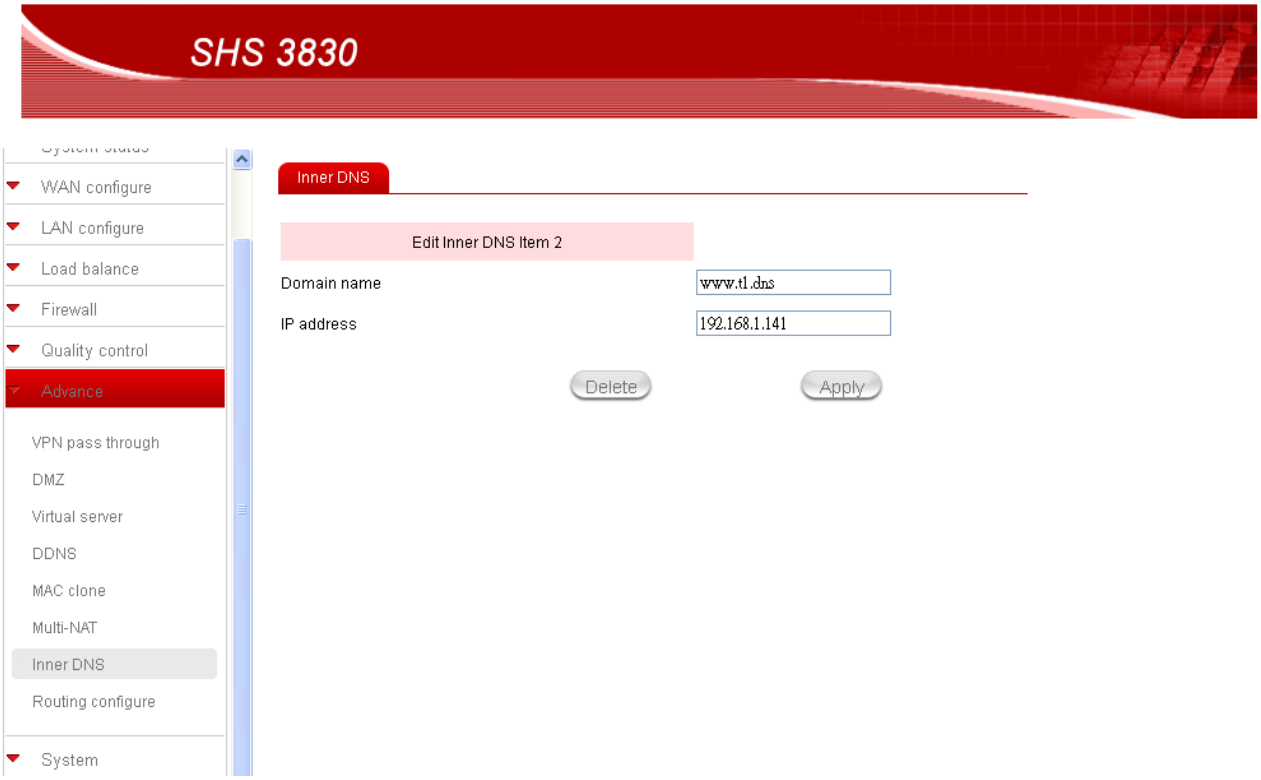


Example: Edit or Delete

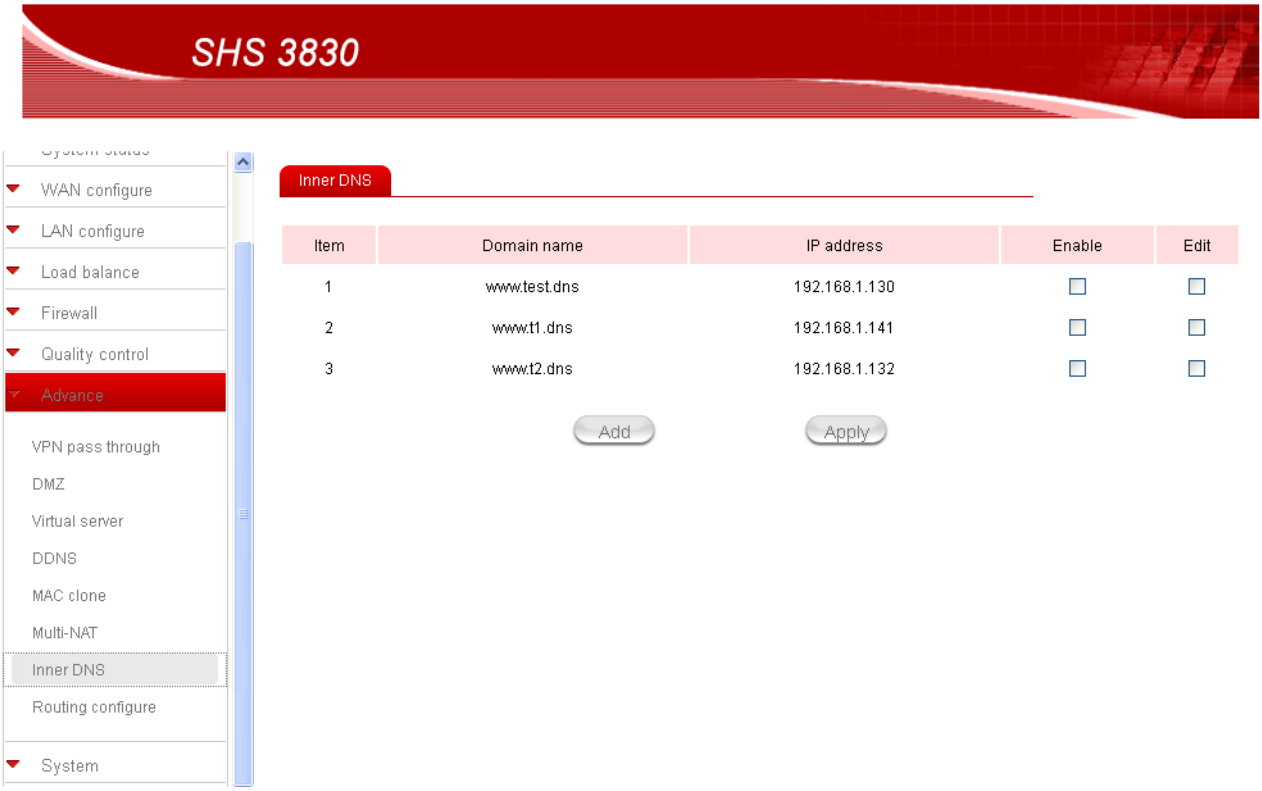
Step 1: Enter **Inner DNS** web page. Then click “Edit” check square of item 2 to enter the edited page.



Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Inner DNS** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Inner DNS** list table.



Step 3: Router go back to **Inner DNS** list table.



3.5.8 Routing configure

There are two routing methods can be applied in various network environments, so choose one of them (**Static routing**/**Dynamic routing**) for need.

Static routing

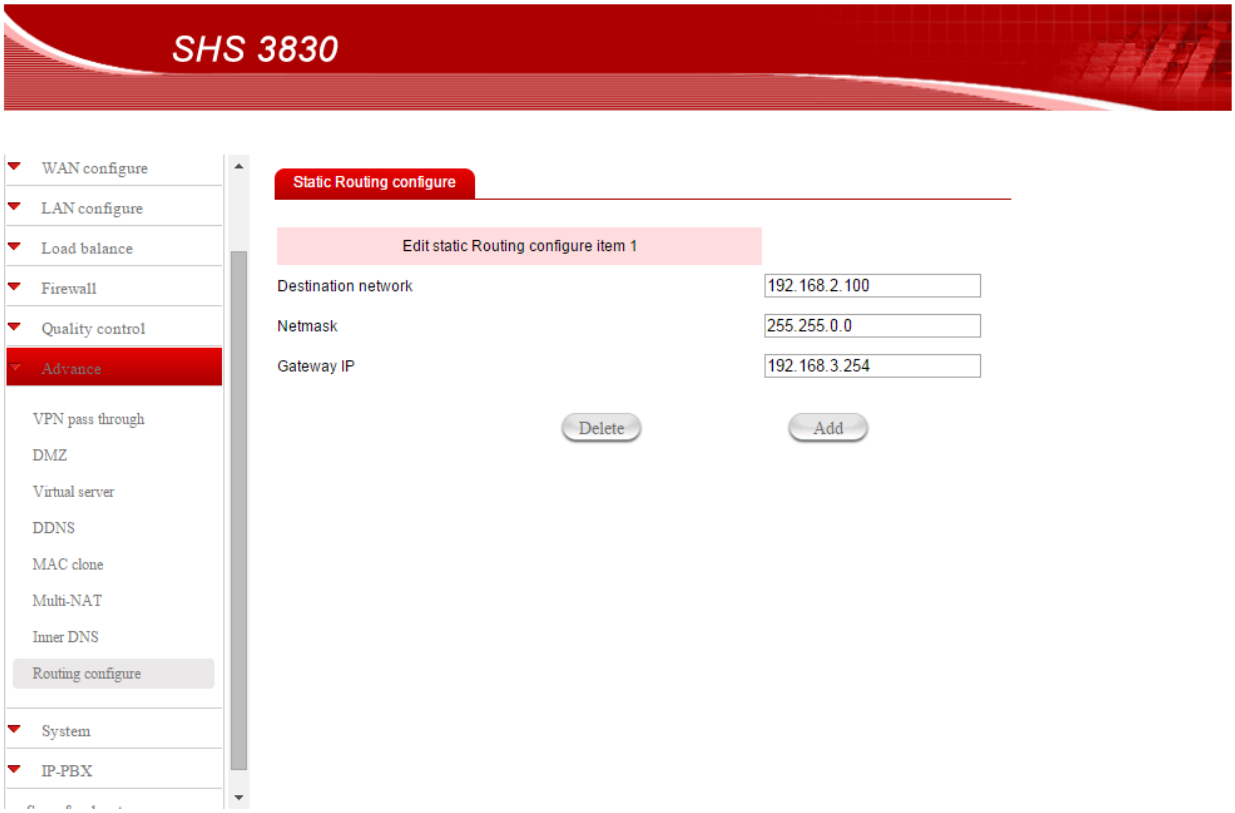
This function allows manually defined by users as the only path to the

destination. Users can configure the static routing path to Load Balance Router.

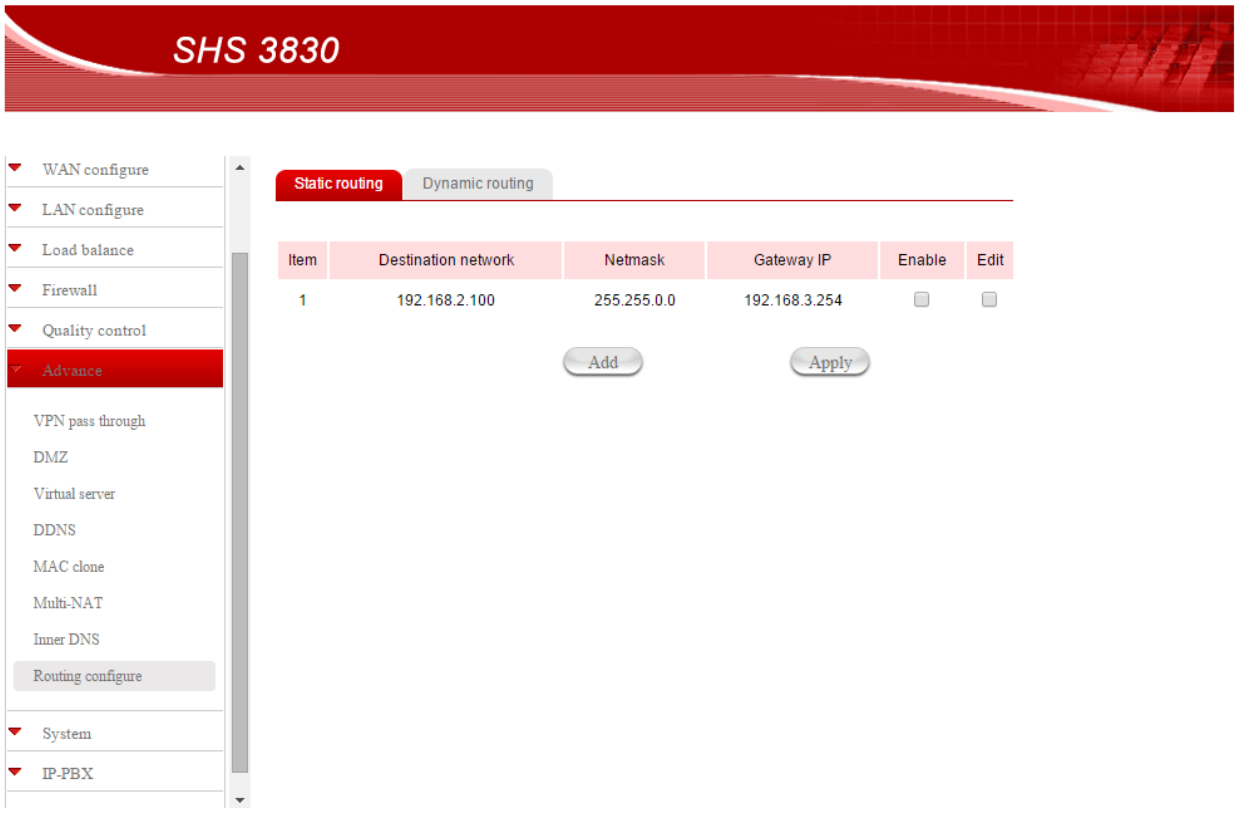
Example: Add a new item.

Step 1: Enter **Static routing** web page. Then click “Add” to enter the added page.

Advance – Static routing



Step 2: Fill data to Destination network, Netmask and Gateway IP. Then Click “Add” then router goes back to **Static routing** list table.



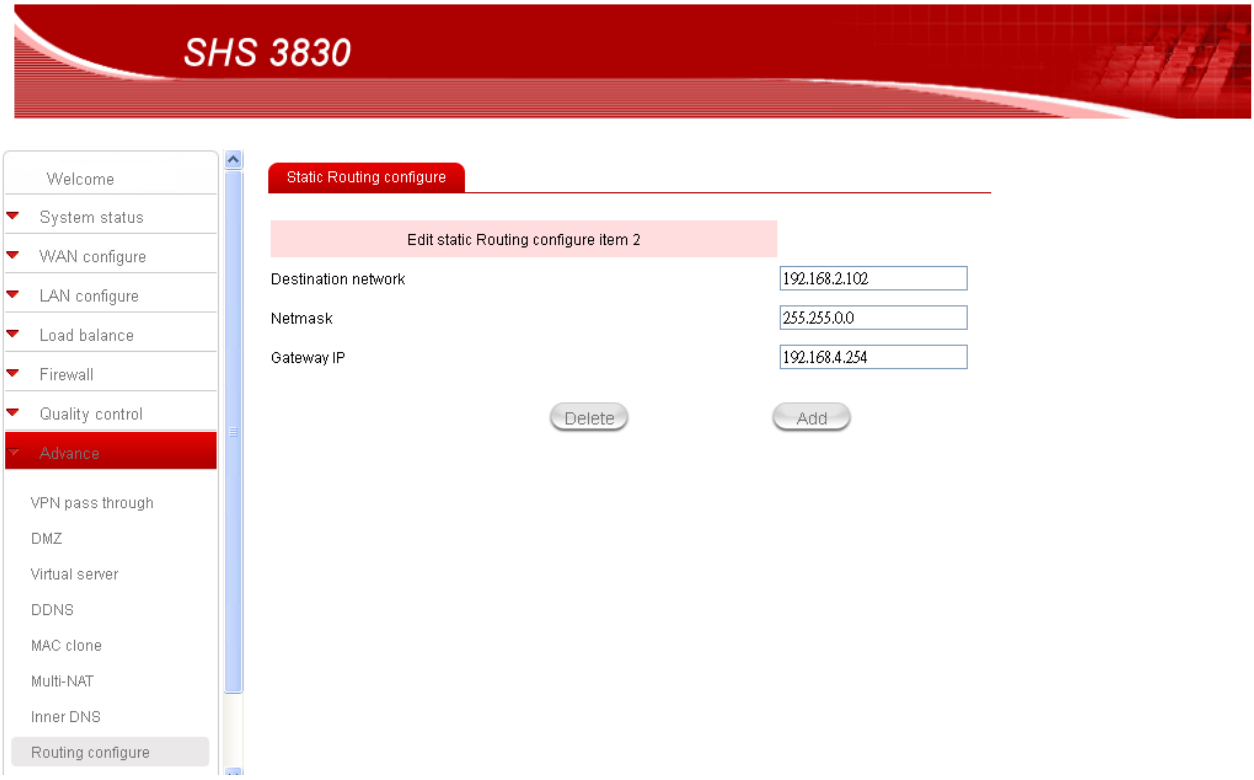
Step 3: Click the “Enable” check square of item 1. Then click “Apply” to save and

enable.

Example: Edit or Delete

Step 1: Enter **Static routing** web page. Then click “Edit” check square of item 2 to enter the edited page.

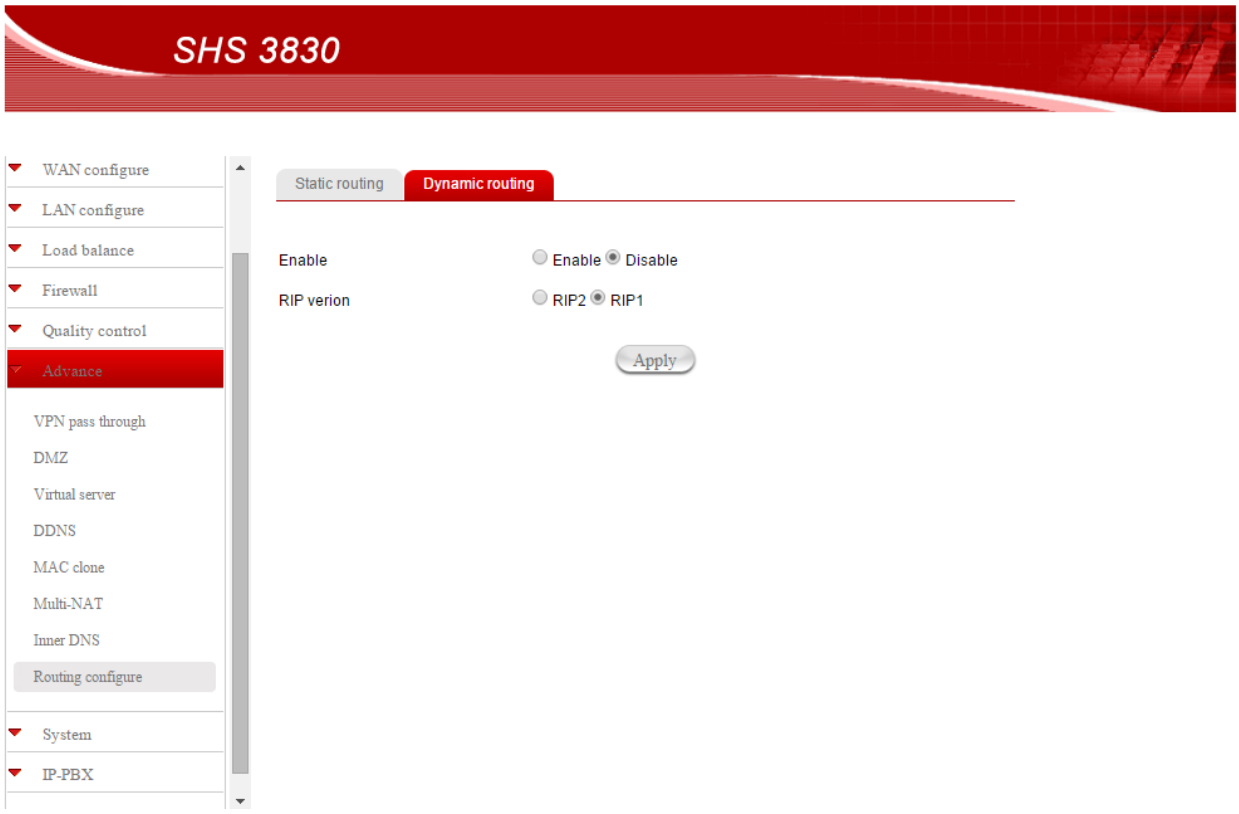
Step 2: User can edit or delete it. If user wants to delete it, click “Delete”. Then router goes back to **Static routing** list table. If users want to edit, click “add” when user finish editing job. Then router goes back to **Static routing** list table.



Dynamic routing

Dynamic routing allows router learns of path to destination by receiving periodic updates from others. The protocol used in communication between routers is RIP 1/2 (Routing Information Protocol). RIP1 supports only broadcast mode while RIP2 supports broadcast and multicast mode.

Advance – Dynamic routing



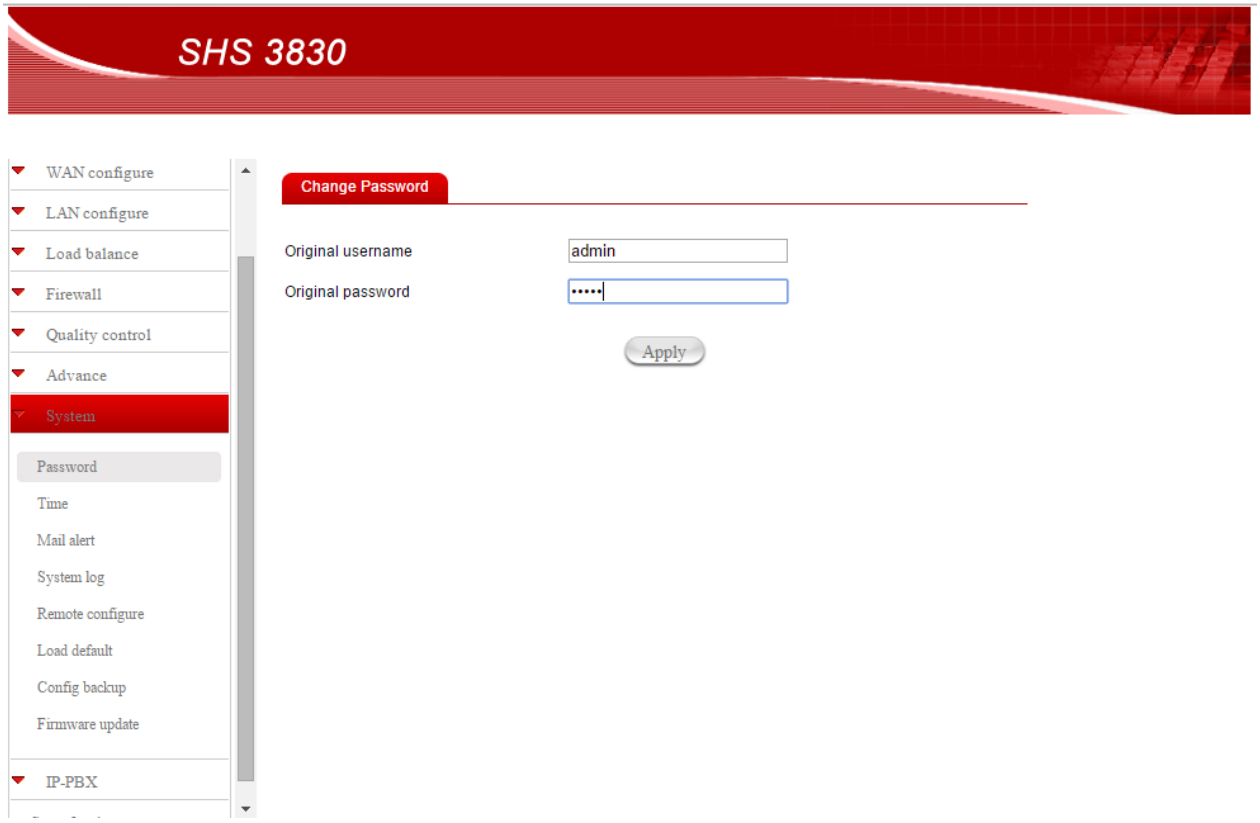
3.6 System

3.6.1 Password

Use this function to change the **Password** that is used for access the web configuration.

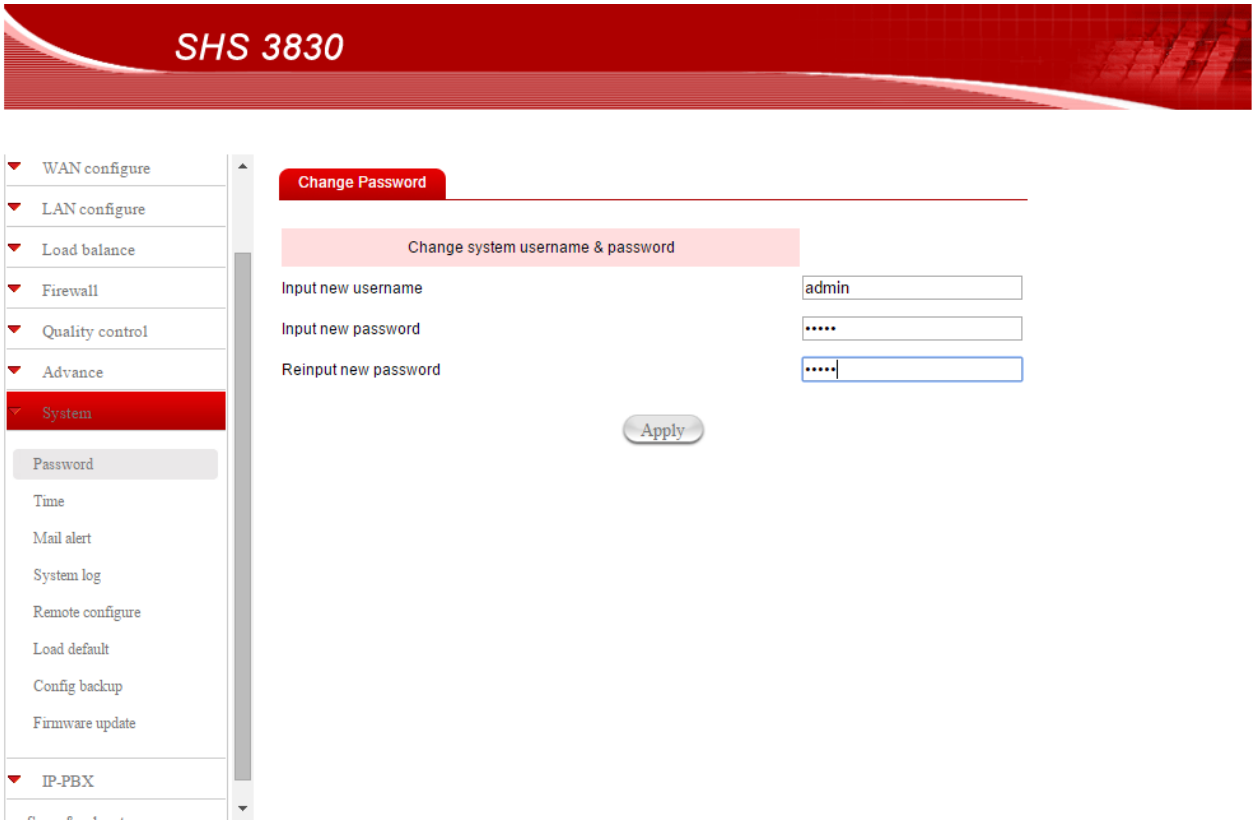
Step 1: Type in the **Original username** and **Original Password** then click “Apply” button. Router will display a change password web page.

System – password (1)



Step 2: Type in the **“Input new username”, “Input new Password”** and **Re-input new Password** in their respective fields and then click **Apply**, the password will be changed to new one after re-boot.

System – password (2)



"Password length can up to 30 alphanumeric characters with case sensitive"

WE SUGGESTED YOU TO CHANGE SHS 3830 PASSWORD AND KEEP IT IN SAFETY PLACE AFTER YOU RECEIVED SHS 3830 AND FINISH ALL ROUTER PARAMETER SETTING.

3.6.2 Time

The SHS 3830 will obtain the GMT (Greenwich Mean Time) after connected to Internet. You need to indicate the local time so that the system could show the correct time. For example, Taiwan's local time is GMT + 8 hours.

Select "Automatic adjust clock for daylight saving changes" will display the time one hour earlier than local time.

System – System time

3.6.3 Mail alert

Enter the **Receiver/ Sender** e-mail Address in the fields and check the items you want. System will send e-mails to **Receiver** address once the conditions meet the setting.

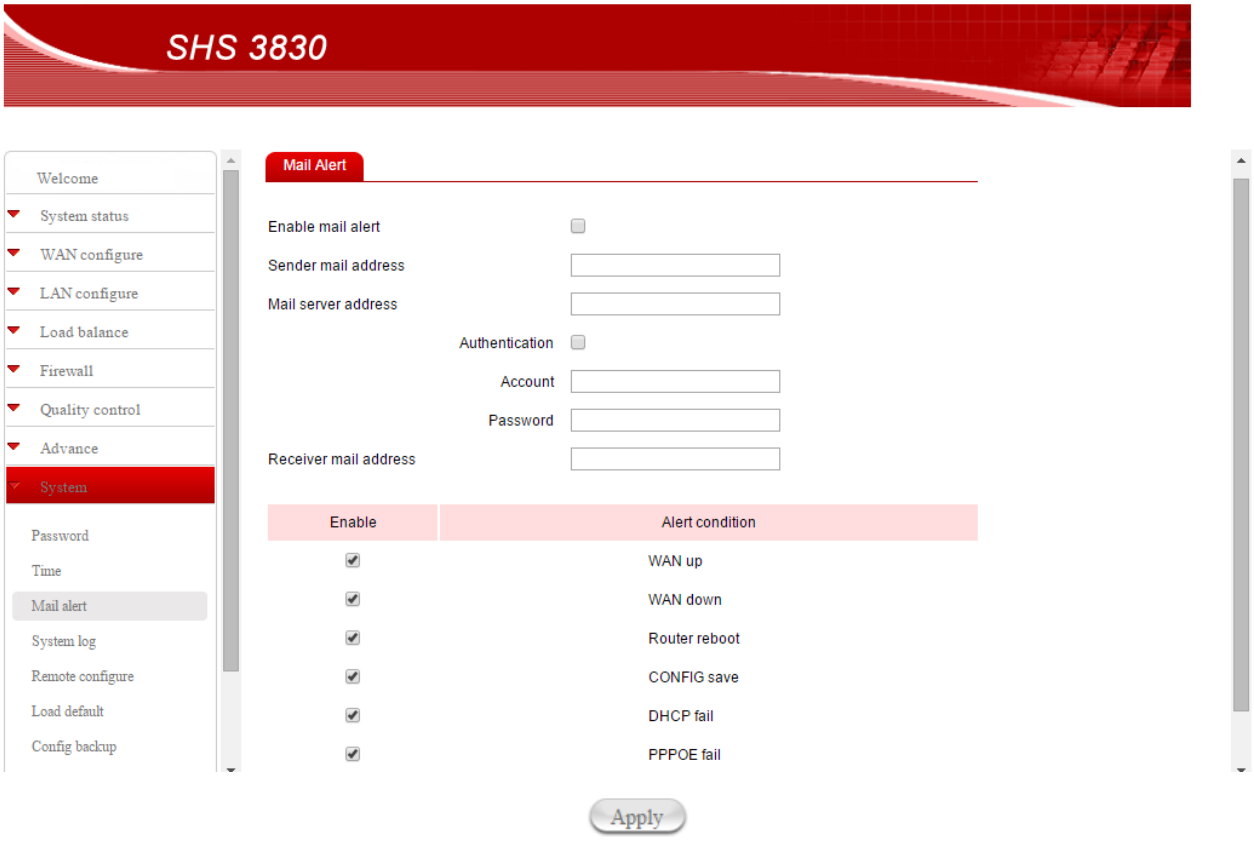
Receiver mail address: The mail address that will receive alert mail

Sender mail address: The mail address that send out alert mail, you should fill in a legal format address (ex. router@yahoo.com)

The SHS 3830 provides four condition selections:

WAN Up	System will send the mail, once WAN port(s) is connected to Internet.
WAN Down	System will send the mail, once WAN port(s) is disconnected from Internet.
Router Reboot	System will send the mail, once the router reboot.
CONFIG save	System will send the mail of log information, once the system configuration is saved.
DHCP Fail	System will send the mail of log information, once the WAN Port status is DCHP and it can't get an IP from DHCP server.
PPPoE Fail	System will send the mail of log information, once the WAN Port status is PPPoE and its connect is fail.

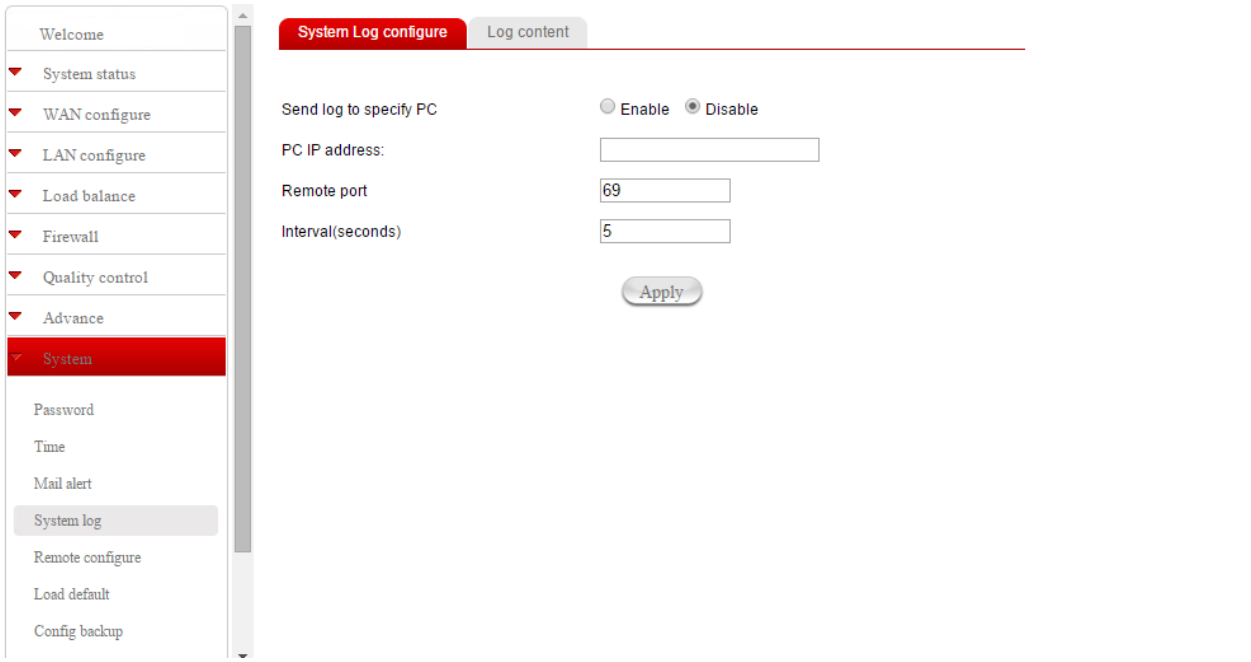
System – Mail alert



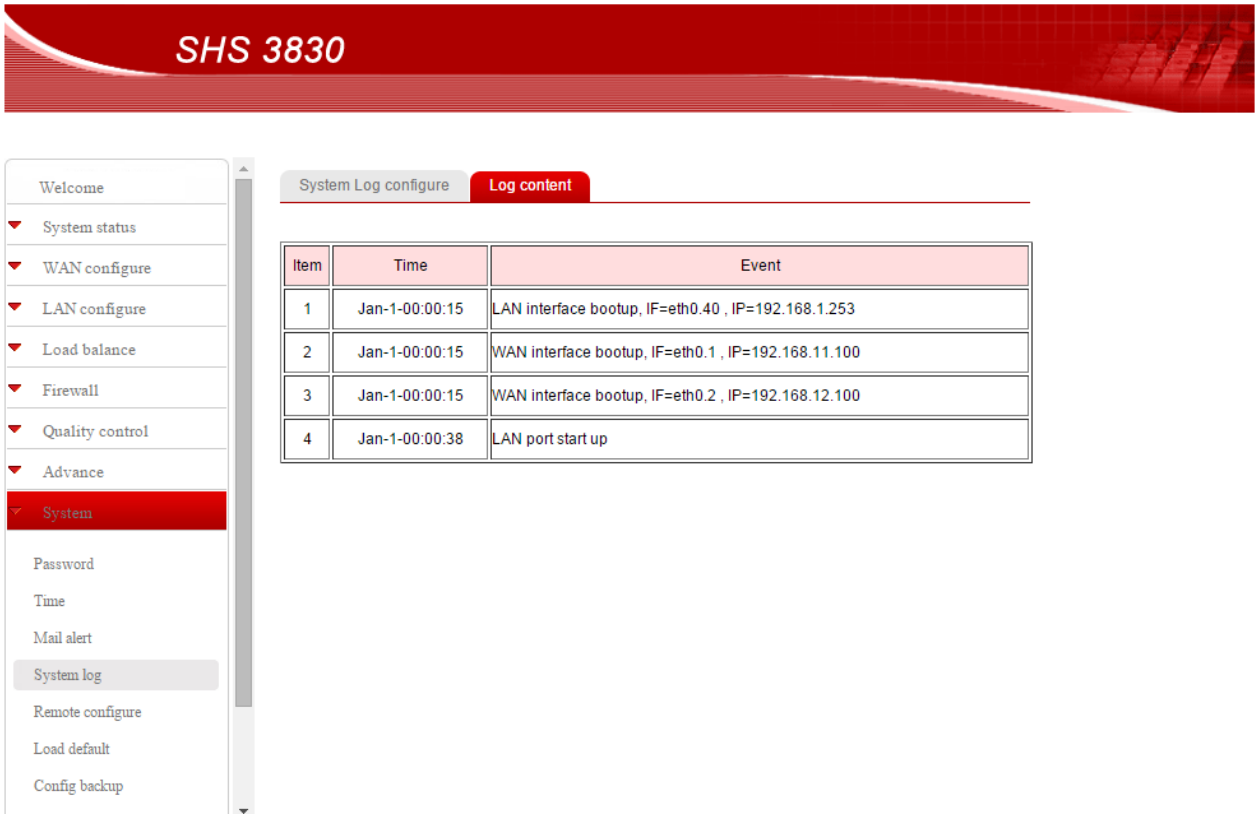
3.6.4 System log

Show all the records after SHS 3830 Power on, such as WAN port up/down, WAN IP address, the obtained time, DDNS current corresponding WAN IP address and so forth. You can also save these data to files.

System – System log configure



System – Log content



3.6.5 Remote Configure

The SHS 3830 can be managed from any PC from INTERNET. If enable **Remote configure** function in this display, access to the Web-based interface is available via the INTERNET, If not enabled, access is only available to PCs from LAN.

Access from LAN …… specific 192.168.1.254 in the URL field

Access from INTERNET …specific WAN port IP address in the URL field

ROUTER provide easy method to access from INTERNET via "Dynamic IP" & "Dynamic port"

Remote IP: specific dedicated PC can be remote access ROUTER

- Leaving these fields blank will allow access by all PCs.
- if enter specific IP address, only this address PC can access from remote
- The address must be Internet IP addresses.

Remote Port: The port number used when connecting remotely.

Example: If the local user

. Enable the **Remote configure** function

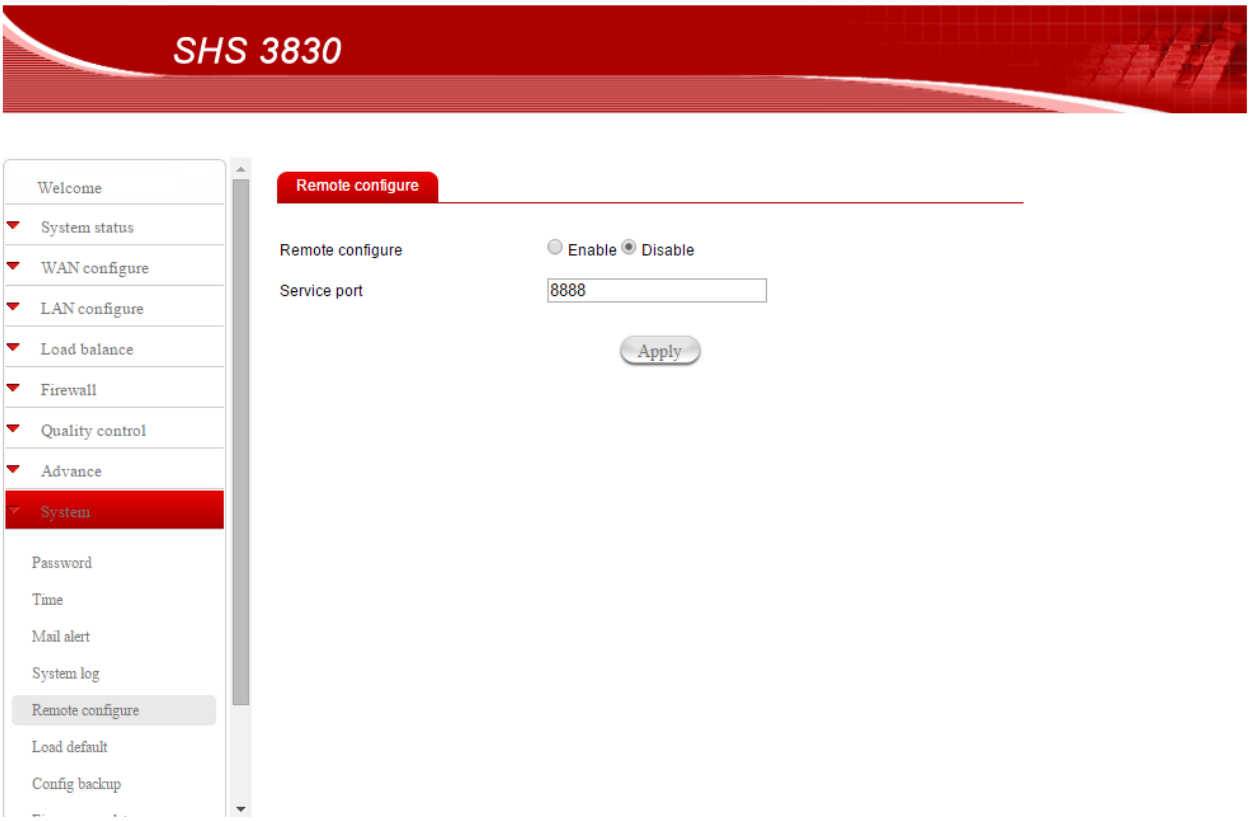
. Remote port is ***8888*** **(default is 8888, can be different port number)**

. Remote IP is blank.

. ROUTER WAN port IP is ***110.111.112.1***

When the user of remote side want to access the ROUTER web configure, the remote user only need to enter ***http:// 110.111.112.1:8888***

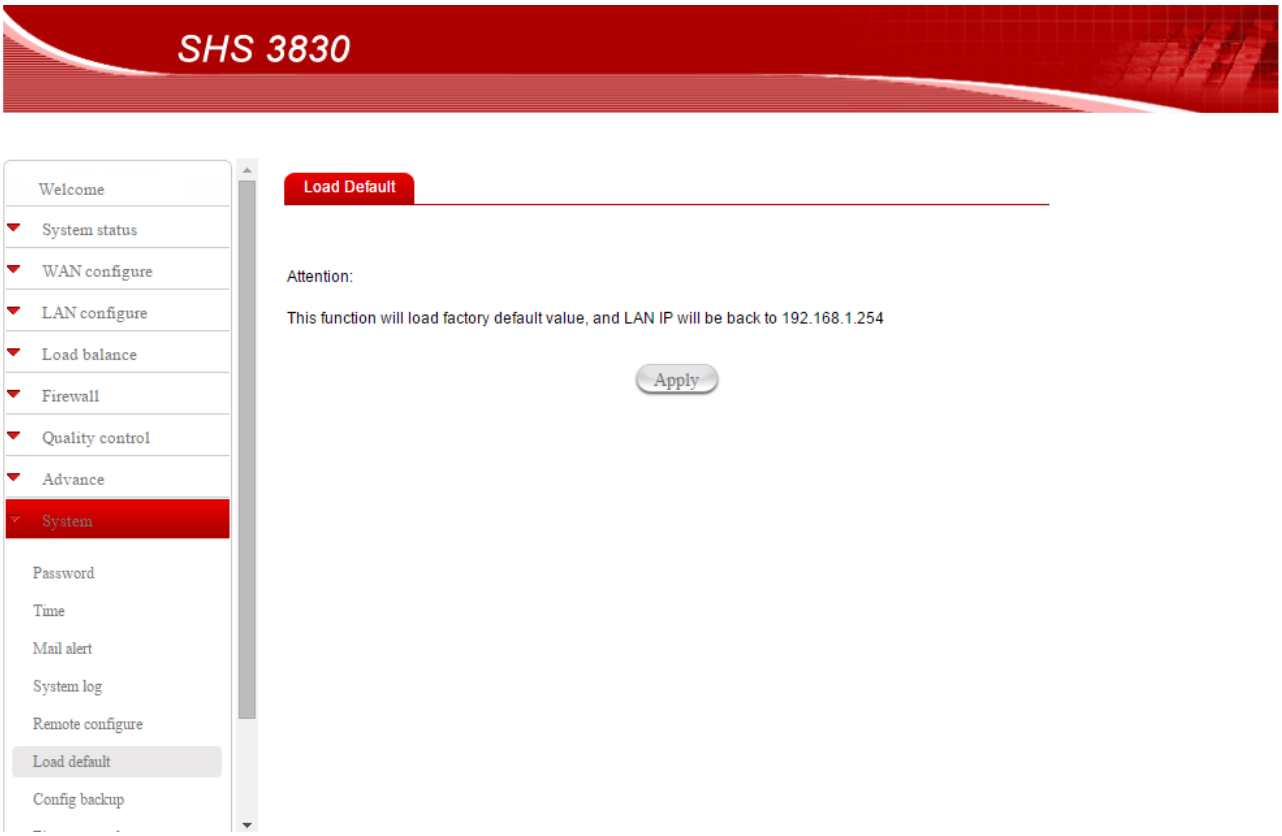
System – Remote configure



3.6.6 Load default

Use this function to reset all the settings to their factory default values or latest configuration file. Click **Apply** after selection, the ROUTER will restart automatically.

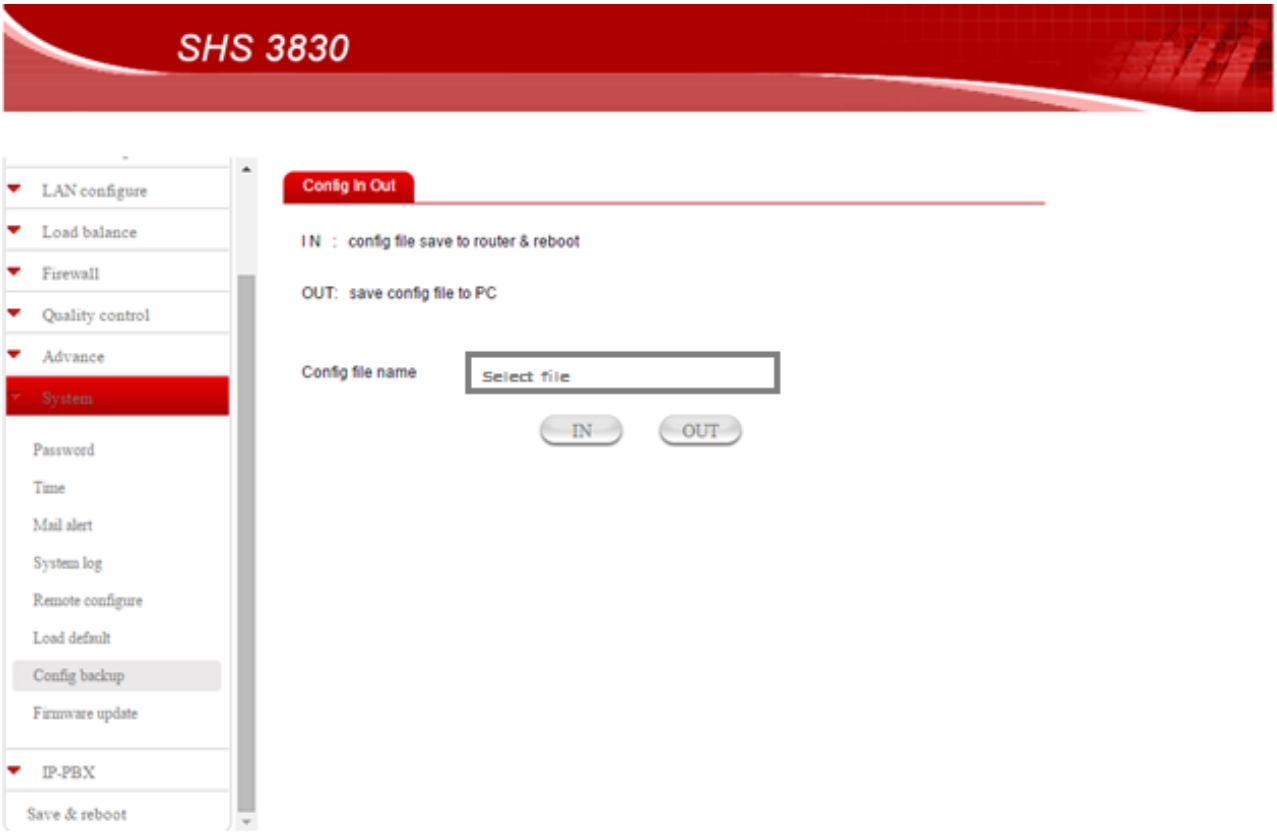
System – Load default



3.6.7 Configure backup

Use **Configure backup** function to save all the settings parameter to PC for safety issue, in order to avoid all parameters lose when system crush or SHS 3830 is loaded the default parameters.

System – Configure backup



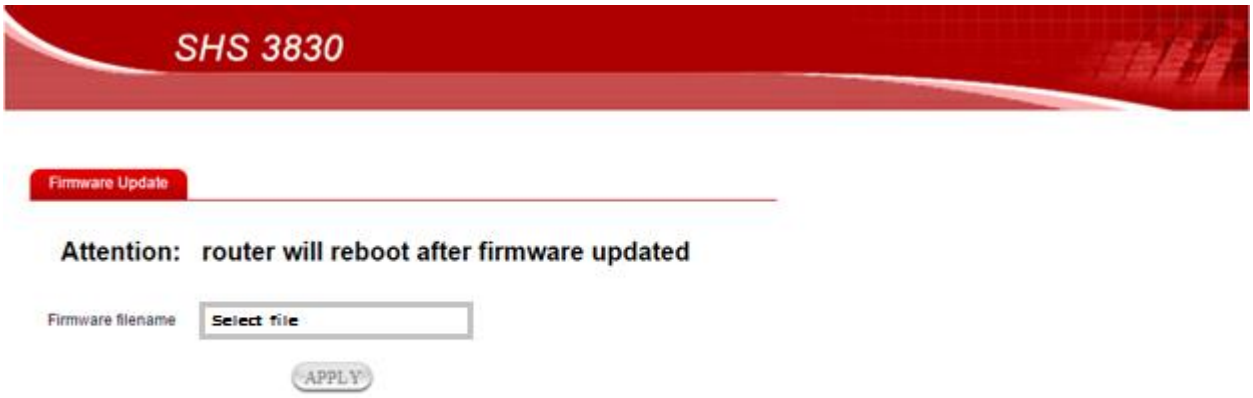
3.6.8 Firmware update

The SHS 3830 allows you to easily update the embedded firmware.

We will occasionally provide new firmware on the web site to help you updating the firmware of your SHS 3830.

Follow the procedure to update your firmware after downloaded the new code.

System – Firmware update

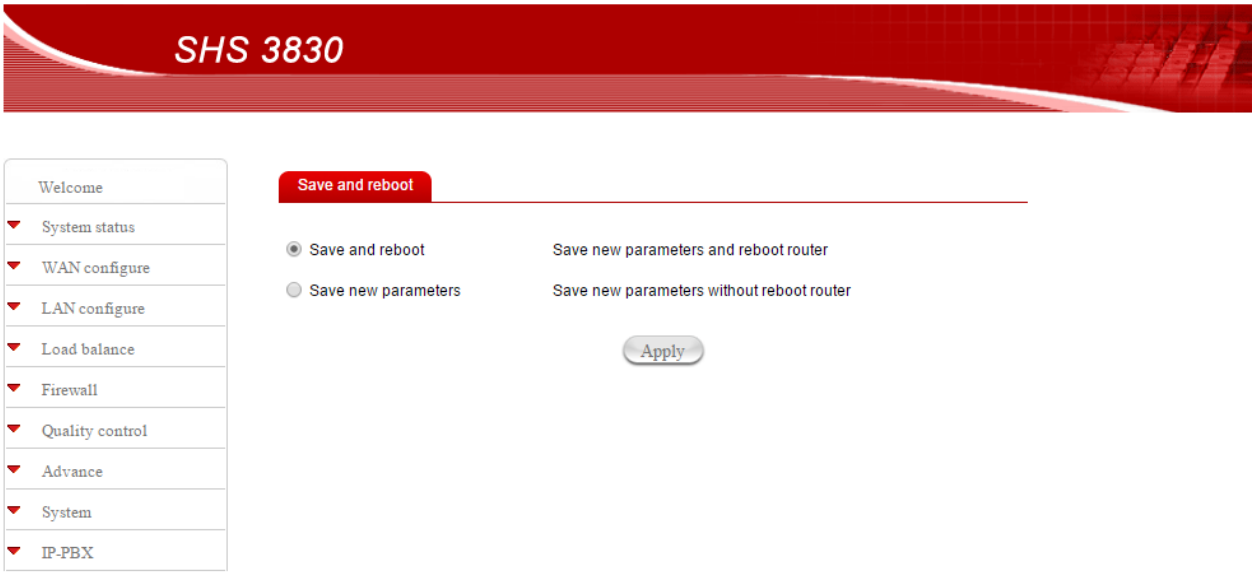


You will see the updating processing. After finishing update procedure, you must **reboot** SHS 3830 to run new code.

3.7 Save & Reboot

In order to save the configuration changes that have been made to the SHS 3830 you must save them to the SHS 3830's Flash memory. If you do not save the changes, the configuration settings will be lost in the event of a power loss or system reboot to the SHS 3830.

Save and reboot



Chapter 4 In-bound function

Authorities DNS is just a fancy term for the official IP address keeper/provider of particular Domain (or Internet) name, such as www.example.com is analogous to a telephone book where a person's name is associated with his telephone number. Wikipedia, the free encyclopedia has a good general discussion of DNS: http://en.wikipedia.org/wiki/Domain_Name_System

This IN-BOUND ROUTER DNS server contains the names and Internet addresses of servers that you wish to host. In order for all DNS requests for your domain names to be ultimately routed to your IN-BOUND ROUTER, it has to be setup at the registrar of your Internet name. In general, logon to your registrar site, and manage your domain name. For example, www.example.com Current is located at a WEBhosting company:

Domain servers in listed order: NS0.DNSMADEEASY.COM
NS1.DNSMADEEASY.COM NS2.DNSMADEEASY.COM
NS3.DNSMADEEASY.COM NS4.DNSMADEEASY.COM We need to change www.example .com to be hosted by IN-BOUND ROUTER; so we follow the registrar's instructions and delete: NS2, NS3, and NS4, and assign:
Domain servers as below

Name	IP address
NS0.EXAMPLE.COM	WAN1
NS1.EXAMPLE.COM	WAN2

The name is arbitrary; what are important are the IP addresses. It is absolutely necessary for WAN1 to be a static address, and for redundant, fault-tolerant accesses, WAN2 should also be a static address. It would take approximately 24 – 48 hours for this change to take effect throughout the Internet.

Chapter 5 Hardware load default

If you need to reset the settings of the SHS 3830 to factory default values or back to latest configuration file, please follow the description step by step to load the factory default settings or back to latest configuration file for the device. Please be careful. Do not press the **Factory Reset** button unless you want to clear the current data.

1. Plug in the power code and then press on the **Factory Reset** button **3 seconds**
2. Release the **Factory Reset** button.
3. The SHS 3830 will load the default settings or back to latest configuration file and do self-test
4. Complete the reset procedure.

Chapter 6 Appendix

6.1 TCP/IP Protocol Port Number List

Protocol Port No. List

Protocol	Service	Port no.	Protocol	Service	Port no.
TCP	FTP	21	TCP	LADP	389
TCP	SSH	22	TCP	HTTPS	443
TCP	TELNET	23	UDP	IKE	500
TCP	SMTP	25	TCP	RLOGIN	513
UDP	DNS	53	UDP	SYSLOG	514
UDP	TFTP	69	UDP	TALK	517,518
TCP	GOTHER	70	UDP	RIP	520
TCP	FINGER	79	TCP	AFPOWERTCP	548
TCP	HTTP	80	TCP	Net-Meeting	1503,1702
TCP	POP3	110	TCP	L2TP	1701
UDP	NFS	111	TCP	PPTP	1723
TCP	NNTP	119	TCP	AOL	5190~5194
UDP	NTP	123	UDP	PC Anywhere	5631~5632
TCP	IMAP	143	TCP	XWINDOW	6000-6063
UDP	SNMP	161	TCP	IRC	6660~6669
TCP	BGP	179	TCP	Real-Media	7070
TCP	WAIS	210	TCP		6000-6063